Security of Cyber-Physical Systems with Human Actors: Theoretical Foundations, Game Theory, and Bounded Rationality

Anibal Jean Sanjab

Dissertation submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Electrical Engineering

Walid Saad, Chair
Thomas C. Clancy
Harpreet S. Dhillon
Jaime De La Reelopez
Danfeng Yao

October 24, 2018
Blacksburg, Virginia

Keywords: Cyber-Physical Systems Security, Game Theory, Prospect Theory, Smart Grids, Unmanned Aerial Vehicles, Internet of Things.

Security of Cyber-Physical Systems with Human Actors: Theoretical Foundations, Game Theory, and Bounded Rationality

Anibal Jean Sanjab

ABSTRACT

Cyber-physical systems (CPSs) are large-scale systems that seamlessly integrate physical and human elements via a cyber layer that enables connectivity, sensing, and data processing. Key examples of CPSs include smart power systems, smart transportation systems, and the Internet of Things (IoT). This wide-scale cyber-physical interconnection introduces various operational benefits and promises to transform cities, infrastructure, and networked systems into more efficient, interactive, and interconnected smart systems. However, this ubiquitous connectivity leaves CPSs vulnerable to menacing security threats as evidenced by the recent discovery of the Stuxnet worm and the Mirai malware, as well as the latest reported security breaches in a number of CPS application domains such as the power grid and the IoT. Addressing these culminating security challenges requires a holistic analysis of CPS security which necessitates: 1) Determining the effects of possible attacks on a CPS and the effectiveness of any implemented defense mechanism, 2) Analyzing the multi-agent interactions – among humans and automated systems – that occur within CPSs and which have direct effects on the security state of the system, and 3) Recognizing the role that humans and their decision making processes play in the security of CPSs. Based on these three tenets, the central goal of this dissertation is to enhance the security of CPSs with human actors by developing fool-proof defense strategies founded on novel theoretical frameworks which integrate the engineering principles of CPSs with the mathematical concepts of game theory and human behavioral models.

Towards realizing this overarching goal, this dissertation presents a number of key contributions targeting two prominent CPS application domains: the smart electric grid and drone systems. In smart grids, first, a novel analytical framework is developed which generalizes the analysis of a wide set of security attacks targeting the state estimator of the power grid, including observability and data injection attacks. This framework provides a unified basis for solving a broad set of known smart grid security problems. Indeed, the developed tools allow a precise characterization of optimal observability and data injection attack strategies which can target the grid as well as the derivation of optimal defense strategies to thwart these attacks. For instance, the results show that the proposed framework provides an effective and tractable approach for the identification of the sparsest stealthy attacks as well as the minimum sets of measurements to defend for protecting the system. Second, a novel game-theoretic framework is developed to derive optimal defense strategies to thwart stealthy data injection attacks on the smart grid, launched by multiple adversaries, while accounting for the limited resources of the adversaries and the system operator. The analytical results show the existence of a diminishing effect of aggregated multiple attacks which can be leveraged to successfully secure the system; a novel result which leads to more efficiently and effectively protecting the system. Third, a novel analytical framework is developed to enhance the resilience of the smart grid against blackout-inducing cyber attacks by leveraging distributed storage capacity to meet the grid's critical load during emergency events. In this respect, the results demonstrate that the potential subjectivity of storage units' owners plays a key role in shaping their energy storage and trading strategies. As such, financial incentives must be carefully designed, while accounting for this subjectivity, in order to provide effective incentives for storage owners to commit the needed portions of their storage capacity for possible emergency events. Next, the security of time-critical drone-based CPSs is studied. In this regard, a stochastic network interdiction game is developed which addresses pertinent security problems in two prominent time-critical drone systems: drone delivery and anti-drone systems. Using the developed network interdiction framework, the optimal path selection policies for evading attacks and minimizing mission completion times, as well as the optimal interdiction strategies for effectively intercepting the paths of the drones, are analytically characterized. Using advanced notions from Nobel-prize winning prospect theory, the developed framework characterizes the direct impacts of humans' bounded rationality on their chosen strategies and the achieved mission completion times. For instance, the results show that this bounded rationality can lead to mission completion times that significantly surpass the desired target times. Such deviations from the desired target times can lead to detrimental consequences primarily in drone delivery systems used for the carriage of emergency medical products. Finally, a generic security model for CPSs with human actors is proposed to study the diffusion of threats across the cyber and physical realms. This proposed framework can capture several application domains and allows a precise characterization of optimal defense strategies to protect the critical physical components of the system from threats emanating from the cyber layer. The developed framework accounts for the presence of attackers that can have varying skill levels. The results show that considering such differing skills leads to defense strategies which can better protect the system.

In a nutshell, this dissertation presents new theoretical foundations for the security of large-scale CPSs, that tightly integrate cyber, physical, and human elements, thus paving the way towards the wide-scale adoption of CPSs in tomorrow's smart cities and critical infrastructure.

Security of Cyber-Physical Systems with Human Actors: Theoretical Foundations, Game Theory, and Bounded Rationality

Anibal Jean Sanjab

General Audience Abstract

Enhancing the efficiency, sustainability, and resilience of cities, infrastructure, and industrial systems is contingent on their transformation into more interactive and interconnected smart systems. This has led to the emergence of what is known as cyber-physical systems (CPSs). CPSs are wide-scale distributed and interconnected systems integrating physical components and humans via a cyber layer that enables sensing, connectivity, and data processing. Some of the most prominent examples of CPSs include the smart electric grid, smart cities, intelligent transportation systems, and the Internet of Things.

The seamless interconnectivity between the various elements of a CPS introduces a wealth of operational benefits. However, this wide-scale interconnectivity and ubiquitous integration of cyber technologies render CPSs vulnerable to a range of security threats as manifested by recently reported security breaches in a number of CPS application domains. Addressing these culminating security challenges requires the development and implementation of fool-proof defense strategies grounded in solid theoretical foundations.

To this end, the central goal of this dissertation is to enhance the security of CPSs by advancing novel analytical frameworks which tightly integrate the cyber, physical, and human elements of a CPS. The developed frameworks and tools enable the derivation of holistic defense strategies by: a) Characterizing the security interdependence between the various elements of a CPS, b) Quantifying the consequences of possible attacks on a CPS and the effectiveness of any implemented defense mechanism, c) Modeling the multi-agent interactions in CPSs, involving humans and automated systems, which have a direct effect on the security state of the system, and d) Capturing the role that human perceptions and decision making processes play in the security of CPSs. The developed tools and performed analyses integrate the engineering principles of CPSs with the mathematical concepts of game theory and human behavioral models and introduce key contributions to a number of CPS application domains such as the smart electric grid and drone systems. The introduced results enable strengthening the security of CPSs, thereby paving the way for their wide-scale adoption in smart cities and critical infrastructure.

To my wife, Hanna,
my parents, Afdokia and Jean,
and my brother, Adon.

Acknowledgments

I am ever grateful to the almighty God for all his blessings.

I would like to thank everyone who helped me during the course of this work. First and foremost, I owe my deepest gratitude to my Ph.D. advisor, Dr. Walid Saad, for his continuous support, guidance, and motivation which have made this dissertation[1] possible. I would like to thank him for always encouraging me and allowing me to benefit from his knowledge and expertise. His mentorship and energy have made my Ph.D. experience productive and stimulating. I would like to thank the members of my Ph.D. advisory committee, Dr. T. Charles Clancy, Dr. Harpreet Dhillon, Dr. Jaime De La Reelopez, and Dr. Danfeng Yao for their valuable comments and guidance which were tremendously helpful in improving the quality of this dissertation.

I would also like to express my sincere gratitude to Prof. Tamer Başar at the University of Illinois at Urbana-Champaign for his invaluable assistance and involvement. I am extremely grateful for his time and effort and for having the privilege to collaborate with him and benefit from his immense knowledge.

I am also grateful to all the notable researchers with whom I had the opportunity to work and interact during my Ph.D. studies. I would like to thank all my friends and colleagues at the NetSciWiS lab, Wireless@VT, and Virginia Tech. My time at Virginia Tech has been truly rewarding and enjoyable.

Words fail me to express my immense gratitude and appreciation to my wife, Hanna. Without her continuous love, support, and motivation, this dissertation would have never been possible. I owe her for always believing in me and for being my source of strength. I thank my beloved parents, Afdokia and Jean, and brother, Adon, for their unconditional love and never ceasing emotional support that have accompanied me in every step of my life. I am also heartily thankful to my parents-in-law, Doreen and Klaus, whose persistent support has been immensely helpful in every step of my Ph.D. studies.

[1] This research was supported by the U.S. National Science Foundation under Grants CNS-1446621 and ECCS-1549894

Contents

List of Figures

List of Tables

Chapter 1

Cyber-Physical Systems Security: Motivation, Background, and Contributions

In the era of the Internet of everything (IoE), cyber-physical systems (CPSs) have emerged as one of the most transformative technologies due to the key role they are expected to play in transforming traditional infrastructure, cities, and engineering systems into more sustainable, efficient, economic, resilient, and interactive systems. CPSs are networked systems comprising i) a *cyber layer* responsible for performing communication, data collection, processing, and exchange, ii) a *physical system* that encompasses physical components such as actuators and controllers, and iii) a *human layer* comprising users, operators, maintenance personnel, or any individual whose actions can have a direct impact on the system, in particular, administrators and hackers [1–6].

In a CPS, all physical components along with humans are interconnected via a cyber layer that provides a reliable and fast exchange of data as well as large data processing abilities enabling an efficient, accurate, and sustainable wide-area observability, controlability, and operation of CPSs. Indeed, accurately collected, exchanged, and processed data in CPSs will allow a continuous monitoring of their real-time state of operation which – alongside a wide reachability and control ability provided by the underlying communication layer – enables taking informed control decisions to ensure rejection of disturbances, optimal operation, and sustainable availability of these CPSs. For example, in the smart electric grid – a prominent example of such CPSs – the wide area synchronized data, collected and exchanged throughout the system, will potentially allow an accurate and quick identification and localization of the occurrence of faults and disturbances and enable taking optimal security and control actions (such as, line disconnection, and generation and load rescheduling/redistribution) which guarantees an efficient mitigation of the detected disturbances [7]. Along with the physical systems and cyber layer, *humans* represent a central component of CPSs. In this respect, humans can be passive agents, whose observations and collected data are used in the operation of CPSs, or active agents taking decisions which directly affect the operation and security of the CPS. Prominent examples of active human agents within CPSs security are hackers and system operators whose attack and defense strategies – relying on human intelligence in conjunction with software, mathematical, and engineering tools – naturally induce significant impacts on the operation and availability of a CPS. In addition, the decision of a user regarding whether to follow security recommendations and practices have a direct impact on securing or exposing a CPS to security threats.

In addition to the smart electric grid, leading examples of CPSs include the Internet of Things (IoT), unmanned aerial vehicle (UAV) systems, smart cities, intelligent transportation systems (ITS), smart water distribution systems, and smart medical systems, among others. Each of these CPS application domains is briefly introduced next.

- *The Smart Electric Grid:* as defined by the European Technology Platform for Smart Grids in their 2035 Strategic Research Agenda, a smart electric grid is "an electricity network that can intelligently integrate the actions of all users connected to it - generators, consumers and those that do both - in order to efficiently deliver sustainable, economic and secure electricity supplies" [8]. The smart grid is expected to play a key role in enhancing the efficiency, reliability, and availability of the power system due its underlying ability to provide wide-area protection, observability, and control of the system.

- *The Internet of Things:* The IoT will provide a large-scale interconnection of sensors, vehicles, electronics, and mundane objects that are endowed with cyber and computing capabilities. The IoT will create a world in which all used electronics, appliances, humans, and physical objects are interconnected, thus creating a massive CPS [9].

- *Unmanned Aerial Vehicles:* UAVs, commonly known as drones, are small-scale aircrafts piloted remotely or using on-board computers, with no human on board. UAVs were used, in the past few decades, exclusively for military applications. However, recently, advancements in their design and efficiency has promoted their potential use for civilian applications such as in disaster warning and rescue operations, delivery of medical supplies, and providing communication services [10–13]. Such UAV systems typically require constant UAV-UAV and UAV-ground base communications and continuous data collection and processing to insure the success of their missions.

- *Smart Cities:* Smart cities use crowd sensing (also known as citizen sensing)[1] as well as IoT and intelligent infrastructure systems' (electric grid, transportation systems, water and gas distribution systems), to i) create intelligent and interactive urban infrastructure, ii) efficiently manage cities' asset, and iii) coordinate response to emergency events [14, 15].

- *Intelligent Transportation Systems:* ITS enable the collection and exchange of data between vehicles and traffic control in transportation systems allowing an efficient and optimal traffic management [16, 17]. Such systems are based on the emerging integration of computing and

[1] Crowd sensing consists of the collection of large amount of data from a vast number users' computing devises such as smartphones, tablets, and wearables and use such data to extract certain features and learn about a certain process of interest [14].

communication technologies in every-day used automobiles and the collection, processing, and use of massive amounts of user and traffic data [16].

- *Smart Water Distribution Systems:* Smart water distribution and management systems use installed sensors (i.e. flow, temperature, and pressure sensors) and distributed computing devices to gain continuous monitoring and controllability of water distribution and water treatment systems [18].
- *Smart Medical Systems:* Smart medical systems will integrate wireless communication, sensing, and automation technologies to provide remote medical and health care services and monitoring. Such services range from diagnostic analyses and therapeutic decision making to robotic surgery [19].

All such CPSs rely on an interconnection of cutting edge data processing and communication technologies and novel intelligent physical components enabling a real-time reliable interaction between their various components as well as accurate and effective control and decision making.

However, despite the promising potential of CPSs, they are highly vulnerable to menacing security threats, known as cyber-physical attacks (CPAs), which are becoming increasingly common as evidenced by recent CPS security breaches [20–28].[2] Such security threats stem from the existence of various vulnerable points, in the physical and cyber systems, which can either be directly targeted – creating a cascading chain of failures – or can be used to infiltrate the system by leveraging the dense interconnectivity between the various CPSs elements. Indeed, such a dense interconnectivity and functional interdependence between the various components of a CPS, even though it introduces significant advantages to system operation and efficiency, it makes CPSs increasingly vulnerable to security breaches which can be detrimental to the system [29–32].

In this chapter, we investigate emerging security threats which can target CPSs in an effort to understand the unique challenges of security in CPSs and, then, propose effective security solutions. To this end, this chapter is organized as follows. Section 1.1 provides an overview of major recent CPS security breaches. Section 1.2 reviews the related research works pertaining to CPS security. Section 1.3 provides an analysis of the main challenges and difficulties which face the analysis of CPS security situation and the advancement of effective solutions. Section 1.3 also sheds light on the major differences between CPSs security and i) conventional network security, ii) conventional reliability analyses, and iii) robust control system design. Finally, Section 1.4 presents the main contributions of this dissertation.

1.1 Major CPS Security Breaches

Due to their critical role in the daily functionality of modern societies, CPSs have been the target of various recent security breaches which have led to damages and interruptions at various lev-

[2] Such breaches are surveyed in Section 1.1.

els of their operation. Indeed, many reports have discussed the vulnerability of critical CPSs to attacks [33–36] and the destructive effect that such attacks can have on a multitude of CPS application domains [34, 37]. Next, an overview of some of the recently reported major attacks on CPSs is provided; itemized with respect to the targeted CPS application. This overview exposes the vulnerabilities of CPSs to various types of attacks and enables learning from these security breaches to gain a better and deeper understanding of the security of CPSs, which allows devising appropriate security solutions.

- *Electric Power Grids:* Electric power systems are rapidly adopting new sensing, communication, and data processing technologies which enable accurate wide area protection, operation, and control of the power grid [7]. These technologies are incorporated at various levels of the grid, namely, at the generation, transmission and distribution components of the system. Such cyber-physical electric systems, are known as smart grids, and are a prominent example of CPSs. However, the security of smart grids is one of the most critical challenges facing its deployment [36,38–42]. In fact, smart grids are complex dynamic systems relying on accurate and synchronized data to control, operate, and protect the grid against potential disturbances. As a result, the manipulation or blockage of such transfered data – or using such interconnectivity to infiltrate into the control units of the grid – can have detrimental consequences as evidenced by the recent Ukrainian power grid security breach [20, 21] described next.

  The first recorded successful cyber-physical attack on a power system was the notorious attack which targeted the electric distribution system in Ukraine in December 2015 causing a large-scale blackout affecting 225,000 customers spanning several western Ukrainian cities [20, 21]. This cyber-physical attack is a coordinated attack which concurrently targeted three power distribution companies. The attack compromised a number of distribution companies' computers, through phishing e-mails and malware infiltration, to gain control of the supervisory control and data acquisition (SCADA) system to simultaneously disconnect 27 power substations while, at the same time, launching a denial-of-service attack against the power companies' call centers to prevent customers from reporting outages [20]. Similar cyber-physical attacks targeting the Ukrainian power grid have also taken place gain on December 2016 leading to a blackout in Ukraine's capital city Kiev [43].

  Physical attacks have also recently been launched on electric transformers and power substations. For example, remote physical attacks using rifles have been reported such as a sniper attack on a substation in California in 2013 [44] and a rifle attack that took place in 2005, in Florida, which led to the destruction of a power system transformer oil tank leading to a local blackout [45].

- *The Internet of Things:* The vast interconnectivity that the IoT brings in, introduces an unimaginable set of new services and applications. However, it poses various security challenges as recently evidenced by a malware labeled Mirai [22–24]. Mirai is a malware targeting IoT devices, which has recently infected IoT devices such as web cams, surveillance cameras, digital video recorders (DVRs), and other every-day-use IoT devices [22–24]. Mirai continuously searches for IoT connected devices, to infect the largest possible set of devices and, then, use this large set of infected devices as part of a *botnet* – a set of networked Internet connected devices controlled by one entity for, typically, malicious purposes – to launch a distributed denial-of-service (DDoS) attack. This DDoS, carried out by a huge number of infected devices, overwhelms the Internet infrastructure with massive traffic such that many providers of Internet services would not have any remaining capacity to provide services for benign users [22–24]. In this respect, Mirai has been responsible for a number of recent DDoS attacks around the globe, such as the attack on Deutsche Telekom (one of the largest telecommunications companies in Germany) in November 2016 [24] and the latest attack on Dyn (Internet performance management and domain name system provider) in October 2016 which has denied access to various prominent websites such as Twitter and Netflix in North America and Europe [22,23]. This attack on Dyn is the largest DDoS attack ever recorded with a throughput of 1.2 Tbps of data. Mirai is, hence, a real world example of how vulnerabilities in the physical system can be used to target the cyber layer in CPSs; unlike the other attacks listed here in which cyber vulnerabilities were used to penetrate and inflict damage to the physical system.

- *Industrial Systems:* One of the most recent major attacks on industrial CPSs was carried out using a computer worm known by the name of "Stuxnet" which was discovered in June of 2010 and which was responsible for infecting the cyber system of more than 14 industrial systems in Iran including a critical plant for uranium enrichment [25]. This computer worm typical targets the control of industrial systems – compromising their programmable logic controllers (PLC) – and giving the ability to the attacker to operate the control system the way it intends. As a result, the adversary may not only spy on the system but also cause self deterioration of large spinning centrifuges. This worm is known to be stealthy and has the ability to update and self-replicate [46].

  A malware that shows a high similarity to Stuxnet is a remote access Trojan (RTA) known by the name "Duqu" which was discovered in 2011 [47]. This malware does not have the capability to self-replicate or to trigger physical damage. It rather aims at collecting data to learn about a target industrial system which can help in future directed destructive attacks [48]. A high similarity exists between Duqu and Stuxnet [47,48]. Hence, this projects the continuous evolution of such attacks and anticipates their recurrence which may inflict even larger damage to CPSs.

- *Transportation Systems:* Transportation systems have also been subject to CPSs security breaches. In 2001, a denial-of-service attack disabled a ship assistance system at the Port of Houston, TX, USA. Various other reported CPS breaches have targeted railroad systems in Washington, DC in 2003 and Sydney, Australia in 2004 [28]. In addition, the increasing use of wireless systems, microprocessors, and Internet connectivity in new automobiles– such as, for instance, in self-driving cars – has raised various concerns regarding the security of such cars and their vulnerability to being remotely hacked. In fact, various real-time experiments [49,50] have shown that a hacker could launch attacks against such cars which can lead to disabling braking systems, denying control over the steering wheel, or even shutting down the engine.

- *Water Services:* One of the most famous attacks on water CPSs is the one which targeted Maroochy Water Services in Queensland, Australia in 2000 [26,27]. This attack was carried out by a former contractor of the victim company who was able to hack into the system using a laptop computer and a radio transmitter. As an act of revenge for not being offered a job with the Maroochy council, the identified attacker hacked into the system and successfully blocked communication links with wastewater pumping stations leading to the spill of around one million liters of sewage water mixing with water flowing to local waterways.

- *Medical Services:* CPS security threats also pose a concern to the medical sector. In fact, many implementable medical units, such as cardiac defibrillators, neurostimulators and drug pumps, among others, have underlying wireless communication features that enable them to be reprogrammed using wireless signals. Even though no major security-related incidents have been reported to date, multiple experiments on such devices showed the possibility of compromising such medical devices using wireless links, taking control of their functionality, which can be fatal to the targeted patients [28].

  Few reported health related breaches include the "Conficker" worm which was reported to target magnetic resonance imaging (MRI), X-ray machines, and other medical devices largely affecting their functionality [28].

This overview of the latest security breaches which have targeted CPSs shows the seriousness of the emerging threats and the need for the derivation of effective defense solutions. In fact, concentrated research efforts are needed to gain a deeper understanding of the vulnerabilities of CPSs and the threats with which they are faced. In this respect, next section overviews the CPS security threat models, the type of potential security solutions which can be implemented, and the challenges associated with gaining a full understanding of CPSs' security vulnerabilities and devising holistic security solutions.

1.2 Existing Research Efforts Focusing on CPS Security

Securing CPSs is indispensable to sustaining their availability and benefiting from the advantages that they introduce. To this end, a number of research efforts have focused, in the past few years, on studying the security of CPSs [9,29,51–113]. Indeed, researchers from multiple domains such as network and information security, wireless communications, control systems, power systems, and game theory have recently studied CPS security problems aiming at gaining a better and deeper understating of the security threats facing CPSs and proposing methods and solutions to thwart these threats. For analyzing the contributions made in this field, these contributions are categorized next based on the type of the studied security vulnerability, purpose of the work (i.e. aspect of the proposed security solution), and CPS domain area. A review of these contribution is provided next.

1.2.1 Threat Models in CPSs

Given their interconnected cyber-physical nature, CPSs will inherit physical and dynamic system threats as well as well-known communication and network threats such as those targeting their integrity, availability, and privacy. However, the goals of such attacks will significantly differ from those sought by adversaries targeting classical cyber systems, such as communication networks. Indeed, an attack on a CPS will primarily seek to disturb the operation of the underlying physical systems by exploiting their reliance on the cyber layer (e.g. the Internet and underlying communication infrastructure). The main differences between CPS security analyses and conventional network security analyses are further highlighted in Section 1.3. Next, the key CPSs security threats are discussed, in detail.

Integrity:

Integrity refers to the credibility of the data collected and transferred over the CPS. Targeting this integrity through what is known as deception attacks of the transfered data, used for instance in a feedback control, can have detrimental effects on the system. Attacks that target this integrity can cause a false visualization of the real-time state of operation of the system as well as lead to the unobservability or even dynamic instability of the system. Two of the most studied types of integrity attacks are data injection attacks (DIAs) [69, 75, 81] and time-synchronization attacks [114, 115]. DIAs consist of an adversary manipulating exchanged data such as sensor readings and feedback control signals. DIAs have a detrimental effect on the capacity to correctly monitor the real-time state of operation of the system which can lead to false control decisions. In addition, manipulating feedback control signals using DIAs can have serious consequences which can range from a suboptimal operation of the CPS to completely destabilizing the system. Time synchnronization attacks correspond to manipulating the time tags at which measurements have been collected. Such manipulation can cause inaccurate perception of the real-time state of operation of the system and, hence, leads to false control and operational actions.

Availability:

Availability, on the other hand, represents the accessibility of every component of the system as well as to the information transmitted and collected when needed. Attacks compromising this availability are known as denial-of-service (DoS) attacks. Given that the dynamic stability of dynamic CPSs – CPSs incorporating dynamic control systems – is dependent on feedback control signals, DoS attacks blocking such feedback control signals can lead to the instability of these CPSs. Such instability causes large-scale components disconnection and failures, loss of service, as well as physical damage to a wide-range of dynamic physical components. For example, blocking control signals in a power system (a dynamic CPS) can lead to a generation-load mismatch which causes significant rises or drops in system frequency requiring protection systems (i.e. over and under-frequency relays) to disconnect generation units or shed loads. If such protection relays'

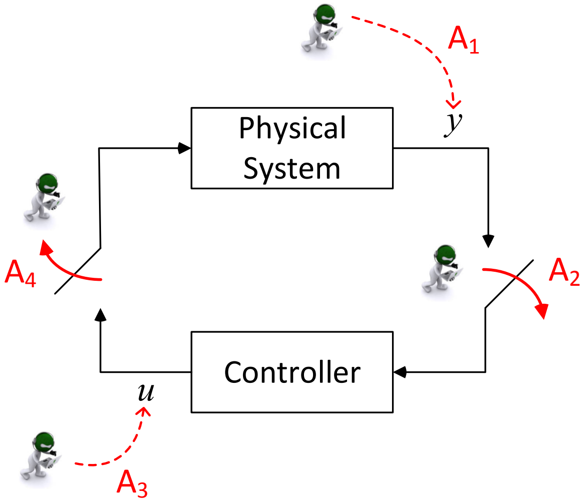

Figure 1.1: Illustration of Integrity and Availability Attacks Against CPSs [117].

actions are not performed in a timely manner, the resulting swings in frequency can cause detrimental damage to the generation, transmission, and even the distribution systems [116]. Moreover, the observability and monitoring of such systems is often dependent on a set of collected system-wide measurements which are fed to a data acquisition system responsible for estimating the real-time operating state of the CPS. As such, disrupting the communication links that carry these measurements may lead to the unobservability of the system. This, in turn, will deprive the CPS operator from accurately monitoring the operation of the CPS which can lead to taking inappropriate control and operational actions. Hence, compromising availably can thus destabilize a cyber-physical system as opposed to the case of conventional networked systems in which a temporary DoS may not, in most cases, lead to the collapse of the whole system [117].

Fig. 1.1, based on the work in [117], helps illustrating such integrity and availability attacks with can target CPSs. In this regard, Fig. 1.1 presents a simple CPS consisting of a physical dynamic system and a controller with targeted attacks launched by CPS adversaries [117]. In Fig. 1.1, attacks A_1 and A_3 correspond to deception attacks in which the attacker corrupts the sensors' and controllers' outputs y and u, respectively, and sends instead false data $\hat{y}$ and $\hat{u}$ such that $\hat{y} \neq y$ and $\hat{u} \neq u$. The adversary can perform these attacks by, for example, compromising measurement devices or controllers (e.g. PLCs [46]) or intercepting the associated communication channels [81] and can, for instance, send false data [81], false transmitters' identification [117], or false timestamps corresponding to the time at which the measurements were taken. On the other hand, attacks A_2 and A_4 in Fig. 1.1 correspond to DoS attacks in which the adversary blocks sensor measurements from reaching the controller and/or block the control signals from reaching the physical system, namely, the actuator [118]. Such DoS attacks can be achieved, for example, by jamming or disrupting the communication channels [118], or by compromising the measurement devices [117].

Dynamic System Attacks:

As a dynamic control system, various dynamic system attacks (DSAs) can target CPSs. One well investigated type of such attacks is known as *replay attacks* (RAs) which can have serious effects on system stability [119]. In RAs, the adversary injects input data in the system without causing changes to the measurable outputs. To launch this attack, an adversary compromises sensors, monitors their outputs, learns from them, and repeats them while injecting its attack signal. Another type of DSAs is known as *dynamic data injection attacks* (D-DIAs) which uses knowledge of the system's dynamic model to inject data that causes unobservability of unstable poles [120]. As a result, a successful D-DIA prevents the CPS's operator from detecting instability which, in turn, can lead to a system collapse. In addition, *stealthy data injection attacks* (S-DIAs) are a type of data injection attacks which leverage an acquired knowledge of the system dynamic model to launch an attack that is undetectable [120]. A *covert attack* is one other type of DSAs that is basically a closed loop version of a replay attack [120].

Physical Attacks:

Given the wide footprint over which CPSs are physically spread and the presence of unprotected physical components, the danger of physical attacks in which an adversary physically attacks system components is prominent [44, 45]. Such attacks encompass tampering with the physical environment, physical destruction of a component, or manipulating the component's circuitry to output corrupt data.

The threats of physical attacks targeting the physical environment of a CPS is most pronounced in IoT critical applications (for example, forest monitoring for fire hazards) in which an attack-induced physical environment manipulation of certain sensors leads to sending corrupt data (such as, for example, false fire alarm data) which cannot be identified to be malicious using conventional authentication techniques since such data is actually sent by an authenticated component. IoT systems are the most vulnerable to such types of physical attacks since, in the IoT, the physical environment is more accessible to an attacker, as compared to other CPS applications, whose components and physical environment might be physically inaccessible or might be within secured perimeters. Nevertheless, physical environment manipulation attacks can also target other CPSs such as transportation systems, as explored in [81], which studied non-invasive attacks directly targeting antilock braking system (ABS) speed sensors and highly affecting the vehicle's operation and safety. In addition, physical attacks can consist of physically destroying some components of a CPSs. Well-known examples of such attacks include the recent rifle attacks which targeted power substations in California, USA in 2013 [44] and in Florida, USA in 2005 [45]. Moreover, physical attacks can take the form of physical manipulation of the electric circuits of CPS components to interfere and modify their functionality. Such types of attacks are common in smart grid applications for energy theft purposes [38, 121]. In this regard, electric energy suppliers have long studied the energy theft problem and identified various physical manipulation techniques which are the most used for theft purposes including: meter bypass (or bridging) as well as tampering with the meter's software, and memory, among others [121].

Coordinated Attacks:

Coordinated attacks (CAs) are a type of cyber-physical attacks in which several types of attacks are concurrently used; simultaneously targeting various parts of a CPS eventually leading to its collapse. CAs are the most challenging type of CPS attacks since they can surpass traditional redundancy and robustness design solutions, by entailing very unlikely simultaneous failures which are not accounted for in robustness measures. For instance, CPSs typically incorporate robustness measures (based, for example, on added redundancy) which help them survive potential failures [122, 123]. Due to these measures, under typical system conditions, an attack leading to the failure of one or few components might not always have significant effects on the system's operation. However, since CAs lead to a large number of naturally unlikely simultaneous failures, such robustness techniques based on added redundancy will no longer be able to thwart such attacks and maintain the system operational. For example, the power system follows the so-called "$N-1$" security criterion [122] which instills redundancies in the system design allowing the preservation of the system's state of normal operation even after the loss of one of its N components. However, a coordinated attack leading to the simultaneous failure of various components may not be prevented by the $N-1$ security criterion. In this respect, the recent attack-induced blackout of the Ukrainian grid – including malware infiltration and control of the SCADA along with a DoS attack targeting the power system customers (i.e. targeting the human layer of the CPS) – is a real-world example of the detrimental effect that CAs can inflict on a power system.

Advanced Persistent Threats:

Advanced persistent threats (APTs) are, by design, a type of targeted attacks that specifically target a certain user or group of users (or a certain node in a CPS) considered to be a valued target, and employ all available resources for such attacks, rather than being concerned with attacking a certain network as a whole (which is typically the case for viruses and worms) [124, 125]. Such attacks are persistent in the way that they focus on a specific target rather than searching for weak alternative targets. The value of the target can reflect its essentialness to a whole CPS, in which compromising such target opens access to various parts of the CPS or enables inflicting a broad damage to the system. The value of the target can also reflect the importance of the target itself, regardless of its interconnected network (for example, acquiring confidential information about a prominent figure, learning about certain features of a CPS, among others). A prominent example of APTs which targeted cyber-physical systems is Stuxnet [25, 124]. In fact, Stuxnet has specifically targeted a brand of programmable logic controllers used in the SCADA network of a targeted industrial system. Due to their nature, such attacks comprise long intelligence gathering and attack modeling phases to be able to design an effective attack. APTs are considered to be an emerging type of attacks. Hence, research efforts in this field are quickly rising with the goal to devise appropriate solutions which are, primarily, user-centric rather than network centric [124, 125].

Privacy:

Due to the human participation in CPSs – as users, customers, and operators – privacy naturally remains a primary concern. This concern directly stem from the private data that users transmit as part of cyber-physical interactive systems such as in the IoT (home automation and application usage data), smart grid (customers' electricity usage), and smart cities (users' movement and location). A mere access to such users' data may lead to a broader breach of user's privacy. For example, various studies [38, 40, 126] have focused on analyzing privacy concerns when it comes to readings of smart meters and energy consumption patterns. In fact, from smart meters' readings, private information such as which appliances are being used at which time, whether an individual is present in its dwelling or not, and the type of activities that a person is performing can be extracted [38,40,42,126]. With regard to IoT and smart cities [126], the nature of the data transmitted itself contains various private information which must be kept confidential.

A number of research works [29, 30, 68–70, 74, 75, 81, 90, 114, 115, 118–120, 124, 125, 127, 128] have studied these types of attacks with the purpose of analyzing and understanding these emerging threats as well as deriving adequate security solutions. In this respect, Table 1.1 provides a listing of some of these research works grouped by the type of threats studied.

Table 1.1: CPS Security Research Efforts

Type of Attacks	**Relevant Work**
Denial-of-Service	[118, 127]
Data Injection Attacks	[69, 75, 81]
Time Synchronization Attacks	[114, 115]
Stealthy Dynamic Data Injection	[29, 30, 68, 70, 74, 128]
Dynamic Data Injection Attacks	[120]
Replay and Covert Attacks	[90, 119]
Advanced Persistent Threats	[124, 125]
CPS Privacy Attacks	[38, 40, 42, 126]

Facing such security threats, a number of security solutions can be advanced to prevent such attacks from targeting CPSs, detect their presence, and mitigate their effects. These security solutions are explored next.

1.2.2 Security Solutions: Prevention, Detection, Mitigation, and Restoration

To address the various types of CPS threats explored in the previous subsection, a number of research efforts have focused on devising CPS-centric security solutions that can maintain the integrity, availability, and operation of CPSs, under such diverse threats. The existing security solutions can be categorized based on their central security objective, namely: i) prevention, ii) detection, as well as iii) mitigation and restoration. In fact, the reviewed literature includes various security solutions which are specific to the treated application. Hence, rather then going through each of these specific solutions, this subsection aims at introducing the guidelines of each of these defense solutions, by categorizing them in terms of their primary security objective, i.e., either to thwart potential future threats (prevention), detect the presence of stealthy threats (detection), or mitigate the potential damage that an attack can inflict on the system (mitigation).

These categorized security objectives and the major research works which have focused on each of these objectives are presented next.

- **Prevention – Vulnerability Assessment and Security Reinforcement:** Attack prevention consists of reinforcing the security of the CPS to prevent any attack from successfully intruding and intervening in its operation. Attack prevention necessitates vulnerability assessment and risk management. The vulnerability analysis phase consists of analyzing which CPS components are vulnerable to what type of threats as well as the security interdependence between the various system components (in an analogous manner to vulnerability assessment and security hardening in network security [129–131]). In addition, risk management corresponds to assessing the effect that the loss of a CPS component can have on the system and identifying the cascading chain of failures that such a component loss can trigger. Once these threats are identified and their effects are traced, a security reinforcement phase must be implemented in which security solutions to thwart the attacks targeting the previously identified vulnerable components are implemented. Such security solutions include measures such as encrypting sensor readings, implementing new security protocols, replacing outdated components with more secure ones, setting up security perimeters, or incorporating additional redundant components, among others. Hence, this prevention phase aims at implementing preventive security solutions to secure the CPS against a range of potential threats. A number of research works have recently focused on devising preventive security solutions to thwart potential attacks on CPSs such as the works in [64–68]. For example, the work in [64] developed a testbed to assess the security threats which can target supervisory control and data acquisition systems of CPSs, based on which defense solutions can be implemented. Similarly, the work in [67] provides a discussion of the threats which can target data acquisition systems of the power grid. The authors in [65] focused on the implementation of preventive techniques to protect advanced metering infrastructure (AMI)[3] from potential attacks. Such preventive techniques are based on a continuous monitoring of the AMI traffic. In addition, the work in [66] discusses security standards which can be implemented to prevent attacks on smart electric grids. These standard must surpass the traditional concepts of security by obscurity which relies on the confidentiality of the designs and system models as the system's primary way to prevent attacks. The authors in [68] propose a framework based on which measurement units in a power system can be made more secure

[3] Infrastructure which enables a reliable communication between electric utilities and customers.

to prevent potential data injection attacks.

- **Detection:** Vulnerability assessment, risk management, and security reinforcement constitute preventive measures to thwart potential attacks which can target CPSs. However, such preventive security reinforcement techniques may fail to thwart some type of stealthy attacks and advanced threats. This is mainly due to the fact that malware designers continuously develop their malwares to penetrate already existing security solutions. As such, the CPS operator must continuously scan the system to detect new threats which have passed the attack prevention defense lines. This is crucial for stealthy attacks which penetrate the system (or continuously and repeatedly attempt to target a certain part of the CPS) and run long-term attacks that cannot be identified using the security solutions already in place. To this end, a number of algorithms and strategies to detect the presence of such stealthy attacks have been presented in the literature [69–71,88,89]. For instance, the works in [88] and [89] introduce detection techniques to detect attacks which can target water supply systems. The work in [69] proposes a framework to identify measurement corruption, dynamic data injection attacks, and replay attacks in a power system. Moreover, the authors in [70] leverage system's parameter estimation techniques to detect data injection attacks on the power grid. In addition, the work in [71] advances intrusion detections techniques which can detect real-time malicious attacks on CPSs.

- **Mitigation – Resilience and Robustness:** To mitigate the effect of attacks on CPSs, two major characteristics of the system are studied: its robustness and resilience to potential attacks. A robust system is designed to withstand attacks or exogenous disturbances without deviating from its normal state of operation. Complete robustness is not always achievable or feasible. The resilience of a system, on the other hand, reflects the flexibility of the system and its ability to temporarily deviate from the defined normal state of operation, to prevent the overall failure of the system, and to restore normal operation after the attack/contingency has been eliminated [51, 73, 132]. In this regard, a number of research efforts have focused on designing defense strategies to mitigate the effects of potential attacks on the system using robust or resilient designs, such as the works in [51, 82, 91, 92]. In this regard, the work in [82] presents a study aiming at enhancing the resilience of state estimation in CPSs against potential attacks; while the work in [51] focuses on the design of a resilient control for CPSs. In addition the works in [91] and [92] introduce a hybrid robust-resilient approach to mitigate the effect of physical disturbances and cyber attacks on the operation of a cyber-physical system. Robustness can be considered to be a pre-attack mitigation strategy while resilience can be considered to be a mitigating post-attack measure.

After exploring the potential security threats which can target CPSs and the guidelines governing possible defense methodologies, the next subsection reviews research works which have aimed at characterizing the threats and advancing solutions for specific CPS applications.

1.2.3 CPS Security: State-of-the-art in Various CPS Application Domains

The previous subsections have introduced and analyzed the various types of security threats which can target CPSs as well as the general types of defense methodologies which can be implemented to face these threats. This subsection provides a review of the CPSs security works based on each application area.

- **Smart Grid:** The security of the smart grid has been the main focus of a profusion of research efforts due to the necessity of the continuous availability of electric power for the functioning of modern societies. These contributions have focused on the two main constituents of the grid: the physical side, with its corresponding control system, and the cyber supporting infrastructure necessary for the successful and efficient operation of the grid. In fact, the work in [79] provides a survey of the security threats which can target the smart grid's control infrastructure and which are due to the underlying cyber-physical interconnection within the smart grid. In addition, the work in [52] reviews the emerging cyber threats which can target the smart grid. A large number of works have considered stealthy data injection attacks on the state estimator of the smart grid – which is responsible for providing the system operator with an estimation of the real time operating states of the power system – and analyzed ways of preventing and detecting such attacks as well as their potential economic and operational effects such as the works in [29, 68, 70, 74–76, 78, 93] and the references therein. In this regard, the works in [75] and [76] have derived a set of stealthy data injection attacks which can affect the state estimation outcome of the power system without being detected by traditional bad data detectors. In addition, the works in [29, 68, 70, 74, 78, 93] have focused on the characterization of a subset of measurement units which must be defended to thwart or mitigate the effect of potential attacks on the power system's operation [29, 68, 70, 75, 76, 78, 93] or electricity pricing [74]. Moreover, vulnerability assessment of SCADA systems of the electric power grid is also the main focus of a number of research works such as in [64,67,77]. The work in [64] has implemented a testbed which can be used to characterize the security vulnerabilities of SCADA systems. In addition, the works in [67] and [77] advance a comprehensive vulnerability assessment of SCADA systems quantifying the extent up to which attacks on the SCADA can affect its effective functionality. This vulnerability assessment can be used in the design of defense solutions which can reinforce the security of the SCADA and mitigate the effects of potential attacks.

- **UAVs:** The proliferation of the use of unmanned aerial vehicles for various applications – such as ad-hoc networks, communication in emergency situations, as well as parcel delivery and time-critical applications – have raised concerns about their security and robustness facing cyber-physical attacks. In this regard, a number of works have focused on analyzing and understanding the security of UAVs and UAV-systems within various applications as explored in [57, 83–87]. In this regard, the works in [83] and [84] provide a comprehensive overview of security threats which can target UAV systems while the authors in [57] introduce an extensive risk assessment scheme which enables assessing the risks facing UAVs.

Moreover, the work in [85] provides a demonstration in which a UAV – typically used for critical operations – was compromised and was subject to the injection of malicious control commands to manipulate its operation. The authors in [86] investigates the security of state estimation in UAV systems aiming at detecting attacks which can target the state estimation process. Furthermore, the authors in [87] introduce a simulation testbed which can emulate security scenarios that can face UAV systems and allow the derivation of important insights which can be used in the design of security solutions. In addition, those developments in UAV technologies have also raised concerns regarding their possible use for malicious activities such as intruding into secured military perimeters or smuggling illicit products [133, 134]. As such, a number of research works [133, 134] have focused on exploiting UAVs' vulnerabilities to cyber-physical attacks to develop anti-drone defense systems to interdict UAVs suspected to carry out malicious activities or intruding into secure perimeters. These anti-drone systems are surveyed in [133, 134].

- **IoT:** the Internet of Things provides vast interconnectivity between various components used in critical applications, urban settings, as well as in automation. Even though such interconnectivity provides vast monitoring and operational abilities, it introduces broad security risks as evidenced by the Mirai malware. As such, various works have focused on studying the security aspect of the IoT with the goal of understanding the risks of such interconnectivity, identifying potential vulnerabilities, and devising appropriate security solutions as surveyed in [9, 53, 54, 80] and the references therein. For instance, the works in [9] and [53] provide a comprehensive survey of the security risks facing the implementation of the IoT. These work review existing communications protocols which can be implemented to enhance the security of IoT interconnected devices while highlighting their potential shortcomings when implemented in the context of IoT applications. In addition, the work in [54] discusses security protocols which can be implemented for IoT security while taking into consideration the significantly limited resources that some IoT devices may possess. In this regard, small cryptographic key sizes are proposed for securing data exchange between IoT devices while minimizing the cryptographic computational processing requirements that an IoT devise must perform. As such, this work also highlights the trade-off between the processing capacity of an IoT devise and the required time span for privacy protection. In addition, in the wake of the discovery of the Mirai malware, the use of IoT devices as part of a Botnet of distributed DoS attacks is investigated in [80] while highlighting the need for security solutions optimized for IoT applications.

- **Transportation Systems:** Transportation systems have been subject to various security breaches as reported in [28]. Hence, their security has been the subject of various research studies such as in [55, 56, 81, 82], among others, focusing on different types of transportation such as ground transportation [81, 82] and air transportation [55, 56], among others. For instance, the work in [81] investigates a physical manipulation type of attacks against antiblock braking systems of cars. The investigated type of attacks manipulates the environment of the wheel speed sensors and inject data in the breaking system computer to tamper with its normal functionality causing life-threatening consequences. In addition, the work in [82] proposes a robust defense mechanism for thwarting attacks which can target the state estimators of unmanned ground vehicles. Moreover, the authors in [55] and [56] study the security of automatic dependent surveillance broadcast (ADS-B) systems. The ADS-B is a system which collects aircraft related information such as location and speed – while in flight – and uses such information for flight management. However, this system uses unencrypted communication which poses various security threats. In this regard, the works in [55] and [56] investigate the vulnerabilities of this system and the security threats it introduces to the aviation field. Moreover, the work in [56] proposes the implementation of what is known as format-preserving encryption to enhance the security of such systems.

- **Water Distribution:** A surge in security studies of water distribution systems has occurred following the security breaches exposing the vulnerability of such systems [26, 27]. These research efforts have ranged from proposing attack detection techniques [88] to proposing security frameworks of water systems [89] and analyzing security threats and protection strategies to irrigation systems' SCADA [135].

- **Smart Cities:** With the advancements in IoT technologies, smart cities applications have come closer to potential wide implementation. Accordingly, security threats targeting smart cities have attracted particular interest in literature. The scope of the works focused on the privacy, integrity, and availability of information flow as well as on the risk of propagation of security threats due to the vast number of underlying interconnected systems [58–63].

As discussed in this section, CPSs in their various applications face various types of cyber-physical threats. As such, devising appropriate and effective security solutions to thwart these threats and mitigate their effects is necessary for the successful implementation and operation of CPSs. However, security analyses of CPSs face a number of challenges. Understanding these challenges is necessary for carrying out a well-informed and effective security analysis. These challenges are addressed next.

1.3 Challenges of CPS Security Analyses

For numerous years, researchers in the fields of network and information security have been working on creating secure systems and devising security solutions to prevent or mitigate the effects of potential cyber attacks [136]. Namely, security protocols, cryptography, risk management, and information security and privacy have been the center of the research efforts of network security professionals. On the other hand, researchers in the field of control systems, have also developed secure, robust, and resilient systems that can withstand exogenous perturbations while preserving the stability of the system as well as a high level of operation quality [136]. Such cyber security analyses and robust control designs are at the center of the security analyses of cyber-physical systems. However, due to the tight cyber-physical coupling in CPSs, such previous analyses, even though essential, need to be transformed, updated, and developed, to account for the unique nature of CPSs. In fact, this cyber-physical interconnection introduces a myriad of challenges which hinder performing accurate security analyses and devising effective security solutions for CPSs. These challenges are discussed next.

1.3.1 The Human Layer

Humans play an essential role in cyber-physical systems and their decisions – as operators, users, or administrators and cyber-physical adversaries – are crucial for the operation, protection, and security of CPSs [1–6, 137]. The role of humans in CPSs is has become more pronounced – as compared to the case of conventional network security – due to the spread, distributed, and interactive nature of CPSs in which humans continuously interact with these CPSs and make active decisions with direct effects not only on the operation of CPSs but also on their security [5]. For example, in transportation systems, a vulnerable vehicle as part of a vehicular platoon [138], if compromised, can put the whole platoon and the humans involved at risk [139]. Another example of the human role in securing CPSs is directly relevant to IoT connected systems. Indeed, an IoT system contains millions of components which are operated or maintained by a large number of humans. These humans routinely perform security tasks such as changing the standard factory passwords of newly bought components, or securing their smart phones or computing devices which directly interact with their IoT devices. Not doing so puts the whole system at risk; a crucial lesson learned based on the latest Mirai IoT malware [22–24]. The increasing number of components in CPSs, and the increasing levels of active user involvement, increases the chance of occurrence of security mistakes whose consequences can have significant effects on the whole system. As such, the understanding and heavy integration of the behavioral aspects of humans in CPS security pose additional challenges to the task of securing CPSs. Indeed, humans and computer systems observe, reason, make decisions, and report observations differently [5]. Understanding these differences, and incorporating them in security analyses, are challenging tasks which are indispensable to advancing the security of CPSs.

1.3.2 Limitation of Conventional Network Security Solutions

The scope of CPS security analyses and solutions greatly differ from conventional network security due to various aspects as summarized next.

- **The physical system:** The physical system constitutes the principal part of a CPS, which typically comprises a dynamic system that must be controlled, stabilized, and optimized [1–4]. This layer does not, normally, exist in conventional networks and, hence, introduces new challenges to the security studies of CPSs. For example, a small-scale denial-of-service attack in a cyber system might not be considered catastrophic while blocking a feedback control signal from reaching the controlled plant can lead to destabilizing the system. In addition, the presence of a largely spread physical realm in cyber-physical systems makes CPSs vulnerable to a broad range of physical attacks and physical environment manipulations. Such attacks and threats most exclusively target CPSs. Hence, CPSs security analyses must account for physical threats through which adversaries directly target the physical environment or physical components of the system to affect its operation. Hence, even though conventional cyber security solutions may provide valuable tools for the protection of CPSs, these solutions needs to be reshaped and developed when applied as part of a security solution to CPSs.

- **Risk management and risk diffusion:** The analysis of the propagation of attacks and threats in a cyber-physical system is different than that corresponding to conventional network systems. For instance, the study of how computer worms and viruses propagate in a cyber system is different than the analysis of the cascading chain of events that the loss of a physical component, due to a cyber attack, can cause. Hence, security solutions to CPS security threats must typically account for the potential cascading failures which can occur within interconnected CPSs.

1.3.3 Limitation of Conventional Reliability Evaluation and Control-Theoretic Solutions

Security analysis in the physical realm typically represents achieving robustness against physical failures and exogenous disturbances. Such robustness is achieved using reliability enhancement as well as robust control system designs.

Reliability and availability [123] evaluation of physical systems is based on the analysis of the probability of failure of their components (focusing, mainly, on natural failures) and their expected availability. The goal of such analyses is then to devise techniques and designs to improve the overall reliability and availability of the system. Such availability improvement techniques include adding redundancies, improving maintenance processes, and testing for hidden failures. Indeed, a primary area of focus in reliability analyses comprises devising schemes for optimal addition of redundancies, to the system, to face stochastic failure events which may occur following defined stochastic processes. However, due to budgetary constraints, such added redundancies cannot account for events that are very unlikely to naturally occur. On the other hand, due to the vast interconnectivity provided by CPSs, an attacker may trigger the occurrence of simultaneous failures which are very unlikely to naturally take place and, hence, are not accounted for in traditional redundancy addition schemes and reliability measures. This is corroborated by the latest attack-induced blackout of the Ukrainian power grid which was caused by simultaneous disconnection of a large number of substations (an event that is highly unlikely to occur due to natural events) which have caused a large-scale blackout. As such, since designing a system that is 100% reliable is practically impossible, and since the increasing number of interconnected, non-redundant, components leads to reduced overall reliability levels, enhancing the availability of such tightly interconnected cyber-physical systems, which face menacing security threats, is highly challenging.

Robust control designs [140] also provide fundamental techniques to preserve the operation of dynamic systems subject to exogenous inputs and disturbances. However, these conventional control-theoretic solutions do not explicitly account for the presence of a cyber layer and its underlying cyber threats that it can introduce to a CPS. In other words, accounting for the communication layer security while considering sensors' output, state estimation, and control inputs, is highly challenging and has not been typically included in conventional robust control designs. That is, indeed, of practical importance for CPSs when considering multiple interconnected dynamic systems whose operation and control require continuous exchange of data using a common communication layer.

1.3.4 Security and Performance Tradeoff

CPS security solutions must be inherently cognizant of the performance of the system. In particular, these solutions must seamlessly integrate with the CPS with minimal disruption to its operation and performance. This trade-off between security and performance is very challenging since the advantages brought-in by CPSs stem from the vast interconnectivity that they introduce between a very large number of users and components. Hence, insuring the availability of this interconnectivity is essential to achieving the sought CPSs performance. However, insuring the security of the CPS against attacks, while preserving this interconnectivity, is a significantly challenging task.

Following the overview of CPS security – including reported breaches, studied threats, solutions, and challenges – which was provided in the previous subsections, we next introduce the limitations of previous CPS security works and introduce the contributions of our work.

1.4 Contributions

As detailed in the previous sections, CPSs are expected to be central to modern cities, advanced infrastructure, and interconnected engineering systems. However, as evidenced by recent security breaches, they are vulnerable to emerging threats targeting their physical and cyber realms. Hence, there is a growing need to devise security strategies to thwart these threats and mitigate their effects. These security strategies, to be effective, must account for all aspects of CPSs security. Indeed, devising security strategies to enhance the security of CPSs with human actors must focus on the engineering designs of CPSs, highlighting the functional and security interdependence between their various layers and elements, as well as focus on their underlying multi-agent decision making processes and human subjective behavior.

1.4.1 Summary of the Shortcomings of Previous Works

The existing body of work [9, 29, 51–113, 141–144] has provided key initial steps towards advancing methods to thwart emerging CPSs threats. However, this prior art is still lacking at multiple fronts. For instance, a large set of these works [51–63] treat the underlying CPS problem as a typical network security problem without specific regard to the existence of the physical system and its interconnection with the cyber layer. Hence, the derived solutions and analyses might not directly apply to CPS security settings as discussed in Section 1.3. Meanwhile, a subset of the works which do consider the interconnected cyber-physical nature of CPSs [9, 29, 64–89] focus on the control, reliability, and derivation of specific security solutions without focusing on the optimality of the provided solutions nor on modeling the multi-agent strategic interactions that arise within the CPS. Moreover, even though a subset of works [90–98, 98–113] study this multi-agent optimal decision-making, typically using game-theoretic techniques, the vast majority of these works [90–98, 98–104] is restricted to zero-sum games which significantly limits the scope of the analyses and derived solutions. Moreover, zero-sum games do not factor in the heterogeneity of the objective functions that can exist between the involved agents. Nonetheless, a subset of works [105–113] propose more general games' representations which model and analyze this complex multi-agent strategic behavior within CPSs security. However, the major drawback of these works is their underlying assumption that the agents involved always act with full rationality which include considering that the agents always choose optimal strategies, have an objective perception of their environment, and an objective perception of their skill levels. However, since CPSs security relies in many cases on humans who can deviate from this full rationality, such provided analyses may fail to analyze cyber-physical security with human actors since they do not account for the role of humans and their potential subjective behavior. A number of recent works [141–144] incorporate the human layer in their CPS security analyses and account to some extent for their potential bounded rationality. However, these works significantly abstract either the cyber layers or the physical systems of the considered CPSs. As a result, these works do not provide a comprehensive security to the entire cyber-physical-human loop.

1.4.2 Summary of Contributions

The main contribution of this dissertation is to provide an in-depth understanding and analyses of the security of CPSs with human actors and develop novel mechanisms and defense strategies for securing CPSs in their various application domains. Towards achieving this goal, this dissertation will develop new mathematical frameworks that allow precise characterization of the threats facing CPSs and derivation of fundamental security strategies and solutions to thwart such threats and mitigate their effects; while explicitly incorporating the multi-agent interactions that occur across a CPS and factoring in the human role in the security analyses.

In this respect, our work brings forward a theoretical foundation of CPSs security with human factors focusing on the following three tenets:

- **Theoretical models for CPS security:** Since CPSs are densely interconnected systems, devising a fundamental understanding of the functional and security interdependence between their various components is essential to quantify the effects of any security breach and assess the merit of any proposed defense strategy. As such, a primary objective of this dissertation constitutes understanding such security interdependence to be able to assess emerging threats or value potential solutions.

To this end, based on the engineering principles of *power systems*, *communications systems*, and *control systems* as well as novel mathematical principles of *graph theory* [145], this dissertation introduces mathematical CPS security frameworks capable of quantifying i) the effects of a certain security breach on the system, ii) the effectiveness of a certain implemented defense policy, iii) the security interdependence between the various CPS elements, iv) the propagation of threats throughout a CPS, and v) the interdependence between the actions of the agents involved in CPS security and their collective effects on the security state of the system.

- **Multi-agent interaction:** CPSs are vastly distributed systems in which various agents (automated and humans) interact and whose actions, learning, and decisions have direct impacts on the security and availability of CPSs. As such, understanding the collective interaction and decision making processes of such multitude of agents as well as characterizing the role that each agent plays in securing and/or exposing CPSs to security threats are indispensable to characterizing the security risks facing CPSs and attempting to defend these systems against such threats.

  Capturing, understanding, and incorporating multi-agent interactions in a security analysis requires a mathematical framework with the capability of modeling the optimal decision making of each agent – with respect to other agents – and collectively quantifying the effect of their distributed behavior – being competitive or cooperative – on the security and operation of the system. To this end, this dissertation advances new notions from *game theory* [136, 146, 147] to model this multi-agent interaction. For instance, clearly, in CPS security settings, the effectiveness of a defense solution is in its ability to anticipate the potential attacks which can target the system. Hence, the security and availability of a CPS is subject to the multi-agent interaction between the system defender(s), attacker(s), and, at instances, users. Our developed game-theoretic frameworks enable an in-deep modeling, understanding, and analysis of such interactions. As such, this dissertation develops a suite of new game-theoretic tools, advance novel game-theoretic concepts, and derive specific results for securing CPSs. The proposed game-theoretic models are, hence, central to our derived security analyses enabling the advancement of strategies for enhancing the security of CPSs with human actors.

- **Role of the human layer:** Humans constitute one of the most prominent components of CPSs. As users, customers, operators, defenders, and hackers, their behavior and perceptions have a direct impact on the security and availability of CPSs. As such, a fundamental understanding of the way humans behave, make decisions, perceive risks, value outcomes, build beliefs, and interact in the presence of risk, uncertainty, and complexity – as is the case in CPS security settings – is vital for devising an in-depth understanding of the threats facing CPSs and for quantifying the impact of any proposed defense strategy.

  Modeling the behavior of humans involved in CPS security settings requires an understanding of i) the way humans subjectively make decisions, perceive risks, and value outcomes, ii) the way humans value their skills and cognitive abilities with respect to their peers and opponents, iii) the way humans make decisions under minimal knowledge of their environment, and iv) the way in which humans' beliefs and psychology affect their decision making processes. In this respect, this dissertation advances and incorporates notions from psychology and behavioral game-theory in the CPS security mathematical formulations to capture the impact of humans' behavior and decision making on the security of CPSs. In this regard, the introduced mathematical frameworks for CPS security capture the following aspects of human behavior and decision making.

– **Subjective perception of risks and outcomes:** Humans' perception of the likelihood of occurrence of events (such as the risk of a successful security breach) and subjective valuation of their outcomes (i.e. subjective assessment of the consequences that a breach may trigger) can affect their behavior and decision making processes. For example, a CPS administrator (or an adversary) may over-weight or under-weight the level of vulnerability of the CPS to a certain type of attacks as well as have a misled assessment of the effects that such attacks may have. This, as a result, will have a direct impact on any implemented security policies (or attempted attacks). Hence, modeling this subjective assessment of attackers and defenders is essential to gain an advanced understanding of the decision making processes of the humans involved in CPS security settings. This modeling requires mathematical tools with the ability to quantify this subjective perception of risks and personal valuation of outcomes. As such, this dissertation incorporates a psychological theory of decision making under risk capable of modeling this subjective behavior based on a large set of psychological experiments and empirical observations known as *prospect theory* [148, 149].

– **Subjective perception of skills and qualifications:** In a complex decision making environment faced with large uncertainties, stringent time constraints, and demanding computational needs, such in CPS security settings, the behavior of humans is highly affected by the way they perceive their skill levels and cognitive abilities with respect to the skill levels and abilities of their opponents. In other words, an overconfident defender can assume that its system is robust/secure enough and that its implemented defense policies cannot be bypassed or penetrated. This overconfident behavior represented by this defender's perception of the superiority of its skills and knowledge over those of potential attackers can be detrimental to a CPS since it leads to a misconception of the robustness and security level of the CPS. Hence, understanding the way humans value their skills with respect to others is essential for anticipating the way they behave in security settings and hence assess the robustness of the CPS to potential attacks. As such, this dissertation advances and includes notions from *cognitive hierarchy theory* [150] in the developed mathematical security frameworks. Such mathematical modeling enables a further understanding of human behavior within CPS security analyses.

– **Subjective behavior under information scarcity:** The humans involved in CPS se-

> curity – attackers and defenders – must implement their attack and defense strategies while faced with a significant lack of information due to the confidentiality involved in security settings. Hence, due to this lack of information, attackers and defenders may not always aim at choosing optimal strategies but rather at meeting a specific security or operational goal or requirement. In this regard, this dissertation captures two notions of decisions making: satisfaction-based decision making and greedy decision making. In satisfaction-based decision making, agents aim at meeting a certain preset requirement; while in greedy decision making, agents always aim at optimizing their objective function. Under scarcity of information, satisfaction-based decision making can more practically model and emulate the decision making processes of the humans involved. As such, in addition to focusing on the greedy approach for decision making, this dissertation also captures satisfaction-based decision making using the behavioral framework of *satisfaction equilibrium* [151, 152] which enables anticipating human behavior seeking to meet a predetermined target requirement.

Based on the introduced analytical frameworks, this dissertation addresses various emerging CPS security problems pertaining to general CPSs as well as to specific CPSs application domains such as the smart electric grid, and IoT and UAV applications. In this respect, the dissertation's major contributions addressing these challenges along with the corresponding results are detailed next. The game-theoretic background needed for the devised analytical frameworks is reviewed in Chapter 2.

1.4.3 Unified Analysis of Observability and Data Injection Attacks in the Smart Grid

State estimation is a fundamental process needed for the effective operation of the smart grid. As such, cyber-physical attacks such as denial-of-service and data injection attacks, which often target the availability and the integrity of the collected state estimation measurements, can have detrimental consequences on the operation of the system.

In Chapter 3, a novel graph-theoretic framework is proposed to generalize the analysis of a broad set of security attacks, including observability and data injection attacks, that target the state estimator of a smart grid. First, the notion of observability attacks – denial–of–service attacks on measurement units which render the system unobservable – is defined based on a proposed graph-theoretic construct. In this respect, a novel algorithm is proposed to characterize the critical set of measurements which must be removed along with a certain measurement to make the system unobservable. It is then shown that, for the system to be observable, these critical sets must be part of a maximum matching over a proposed bipartite graph. In addition, it is shown that stealthy data injection attacks are a special case of these observability attacks. Then, various attack strategies and defense policies, for observability and data injection attacks, are shown to be amenable to analysis using variations of the formulated maximum-matching problem over a bipartite graph. The proposed framework is then shown to provide a unified basis for exact analysis of four key security problems (among others), pertaining to the characterization of: 1) The sparsest stealthy attack, 2) The sparsest stealthy attack including a certain specific measurement, 3) A set of measurements which must be defended to thwart all potential stealthy attacks, and 4) The set of measurements, which when protected, can thwart any attack whose cardinality is below a certain threshold. A case study using the IEEE 14-bus system containing a set of 17 distributed measurement units is used to corroborate the theoretical findings. In this case analysis, stealthy attacks of lowest cardinality are characterized and shown to have a cardinality equal to 2. In addition, it is shown, for example, that defending only 3 out of the 17 measurements is enough to thwart any stealthy attack with cardinality lower than 3, while defending a minimum of 13 measurements is needed to thwart all possible stealthy attacks.

1.4.4 Data Injection Attacks on Smart Grids with Multiple Adversaries

The stable operation of the smart grid is contingent upon the availability and accuracy of a set of collected system-wide measurements which enable the estimation of the real-time operating state of the system. Hence, manipulating the collected data entails distorted automated control actions which could cause a large-scale blackout. In this respect, data injection attacks have emerged as a significant threat to the smart power grid [29, 76, 78]. By launching data injection attacks, an adversary can manipulate the estimation of the real-time state of operation of the system yielding incorrect operational and control decisions. The goal of such attacks ranges from merely causing damage to the system to reaping financial benefit from manipulating electricity prices.

Despite the surge of existing literature on data injection [29, 74, 76, 78, 93], all such works assume the presence of a single attacker and assume no cost for attack or defense. In contrast, in Chapter 4, a framework for the analysis of data injection attacks with multiple adversaries and a smart grid defender is introduced, while explicitly factoring in the limited resources that the attackers and defender might have. To study the interactions between the defender and the attackers, two game models are considered. In the first, a hierarchical game model is proposed in which the defender acts as a leader that can anticipate the actions of the adversaries, that act as followers, before deciding on which measurements to protect. The existence and properties of the solution (i.e. equilibrium) of this game are studied. To find the equilibrium, a distributed learning algorithm that operates under limited system information is proposed and shown to converge to the game solution. In the second proposed game model, it is considered that the defender cannot anticipate the actions of the adversaries. To this end, a hybrid satisfaction equilibrium - Nash equilibrium game is proposed. To find the equilibrium of this hybrid game, a search-based algorithm is introduced. Numerical results using the IEEE 30-bus system are used to illustrate and analyze the strategic interactions between the attackers and defender. The results show that by defending a very small set of measurements, the grid operator can achieve an equilibrium through which the optimal attacks have no effect on the system. Moreover, the results also show how, at equilibrium, multiple attackers can play a destructive role toward each other by choosing to carry out attacks that cancel each other out, leaving the system unaffected. In addition, the obtained equilibrium strategies under both game models are compared while characterizing the amount of loss that the defender endures due to its inability to anticipate the attackers' actions.

1.4.5 Time-critical Network Interdiction Games for Cyber-Physical Security of UAV Systems

Unmanned aerial vehicles, popularly known as drones, will play a major role in many smart city applications such as delivery systems. This role includes delivering consumer goods as well as time-critical items such as medical supplies to remote areas. Despite this promising outlook, the effective deployment of such drone-based systems hinges on securing them against cyber-physical attacks that can jeopardize their mission or use them to intrude into secured perimeters.

In Chapter 5, a novel mathematical framework is introduced for modeling and analyzing the cyber-physical security of time-critical UAV applications, such as drone delivery. In this regard, a general UAV security network interdiction game is formulated to model interactions between a UAV operator and an interdictor, each of which can be benign or malicious. In this game, the interdictor chooses an optimal interdiction strategy specifying the location(s) from which to jeopardize the drone system by interdicting the potential paths of the UAVs. Meanwhile, the UAV operator responds by finding an optimal path selection policy that enables its UAVs to evade attacks and minimize their mission travel time. New notions from cumulative prospect theory (PT) are incorporated into the game to capture the operator's and interdictor's personal valuations of a certain achieved mission completion time relative to a defined target time and their disparate subjective assessment of the cyber-physical risk levels facing the UAVs. The equilibrium of the game, with and without PT, is then analytically characterized and studied. Novel algorithms are then proposed to reach the game's equilibria under both PT and classical game theory. Simulation results show that the operator's and interdictor's bounded rationality will significantly impact their equilibrium strategies and the expected mission completion times. In this regard, the results show that the bounded rationality of the players is more likely to be disadvantageous to the UAV operator. Indeed, the results show that the more distorted the perceptions and valuations of the operator are, the higher its achieved expected mission completion time. For example, under full rationality, the operator can achieve an expected mission completion time that is up to 30% lower than the one achieved under subjective probability perceptions.

1.4.6 Diffusion of Threats in Cyber-Physical Systems

Due to the interconnectivity between the cyber and physical components of a CPS, threats can propagate from the cyber layer to the physical system components. In fact, entry points in the cyber layer can be leverage by a malicious attacker to inflict damage to the physical system. For instance, the likelihood of a cyber node being compromised by an attacker induces a probabilistic risk of failure on all physical components connected to this compromised cyber node. As such, understanding the propagation and diffusion of such threats – from the cyber to the physical side, and vice versa – is indispensable to quantifying the effects of potential security breaches and devising accurate defense solutions which factor in such probabilistic diffusion of risks.

To this end, Chapter 6 presents a general model for CPSs that captures the diffusion of threats from the cyber layer to the physical system using graph-theoretic techniques. In addition, a game-theoretic approach is proposed to capture the strategic decision making of a defender and an attacker within this interconnected CPS. In this game, the attacker launches cyber attacks on a number of cyber components of the CPS to maximize the potential harm to the physical system while the system operator chooses to defend a number of cyber nodes to thwart the attacks and minimize potential damage to the physical side. The proposed game explicitly accounts for the fact that both attacker and defender can have different computational capabilities and disparate levels of knowledge of the system which can limit their rational decision making behavior. To capture such bounded rationality of the attacker and defender, a novel approach inspired from the behavioral framework of *cognitive hierarchy theory* is developed. In this framework, the defender is assumed to be faced with an attacker that can have different possible “skill levels” reflecting its knowledge of the system and computational capabilities. To solve the game, the optimal strategies of each attacker type are characterized and the optimal response of the defender facing these different types is computed. This general approach is applied to smart grid security considering wide area protection with energy markets implications. Numerical results show that a deviation from the rational equilibrium (i.e. the Nash equilibrium defined in Chapter 2) strategy is beneficial when the bounded rationality of the attacker is considered. Moreover, the results show that the defender’s incentive to deviate from the Nash equilibrium decreases when faced with an attacker that has a high computational capability.

1.4.7 Distributed Storage for Enhanced Smart Grid Resilience

The proliferation of distributed generation and storage units is leading to the development of local, small-scale distribution grids, known as microgrids (MGs). In this regard, in the event of a loss of generation capacity due, for example, to cyber-physical attacks or other emergency events, there is a potential in using the distributed stored energy in the MGs to compensate for this loss in generation by supplying the power grid’s most critical loads. As such, each MG operator (MGO) must devise an energy management and energy trading strategy aiming at deciding their optimal level of power to be stored for emergency events and the level of power which could be routinely traded under non-emergency operating conditions.

In Chapter 7, the problem of optimizing the energy trading decisions of MGOs is studied using game theory. In the formulated game, each MGO chooses the amount of energy that must be sold immediately or stored for future emergencies, given the prospective market prices which are influenced by other MGOs’ decisions. The problem is modeled using a Bayesian game to account for the incomplete information that MGOs have about each others’ levels of surplus. The proposed game explicitly accounts for each MGO’s subjective decision when faced with the uncertainty of its opponents’ energy surplus. In particular, the framing effect of prospect theory is used to account for each MGO's valuation of its gains and losses with respect to an individual utility reference point. The reference point is typically different for each individual and originates from its past experiences and future aspirations. A closed-form expression for the Bayesian Nash equilibrium is derived for the standard game formulation. Under prospect theory, a best response dynamics algorithm is proposed to find the equilibrium. Simulation results show that, depending on their individual reference points, MGOs can tend to store more or less energy under prospect-theoretic valuations compared to classical game theory. In addition, the impact of the reference point is found to be more prominent as the emergency price set by the power company increases.

1.4.8 Chapters Outline

These studied research topics and advanced contributions are extensively explained and detailed in their corresponding chapters in the body of the dissertation. In this regard, this dissertation is organized as follows. Chapter 2 introduces the fundamentals of game theory highlighting its valuable impact to CPS security analyses. Chapter 3 provides a unified graph-theoretic framework for the analysis of observability and data injection attacks which can target the smart grid. Chapter 4 focuses on stealthy data injection attacks on the smart grid which with the potential presence of multiple adversaries. Chapter 5 introduces a novel framework for the analysis of cyber-physical security of time-critical UAv applications. In addition, Chapter 6 introduces an analytical framework for analyzing and modeling the diffusion of threats in CPSs as well as enabling the derivation of optimal defense strategies. Moreover, Chapter 7 introduces a game-theoretic framework in which distributed energy storage is leveraged to enhance the resilience of the smart grid against emergency events. Finally, Chapter 8 provides a summary of these contributions and concludes the dissertation. Moreover, it provides an outlook on a number of open problems and research directions which can be taken to further expand the current contributions.

Prior to providing an in-depth analysis of each of these research topics, we provide, in the next chapter, an overview of game theory highlighting the advantages that it brings to CPSs security analyses.

Here, we note that the notations used in the subsequent chapters are specific to the chapter in which they are introduced and are not shared with other chapters.

1.5 List of Publications

As a byproduct of the above contributions, thus far, this dissertation has made the following key contributions:

Book Chapter:

- A. Sanjab and W. Saad, “Power System Analysis: Competitive Markets, Demand Management, and Security”, in *Handbook of Dynamic Game Theory* (eds. G. Zaccour and T. Başar), Springer, 2017.

Journal Publications:

- A. Sanjab, W. Saad, and T. Başar, “A Game of Drones: Cyber-Physical Security of Time-Critical UAV Applications with Cumulative Prospect Theory Perceptions and Valuations”, submitted, 2018.
- A. Sanjab, W. Saad, and T. Başar, “Graph-Theoretic Framework for Unified Analysis of Observability and Data Injection Attacks in the Smart Grid”, submitted, 2018.
- Y. Hu, A. Sanjab, and W. Saad, “Dynamic Psychological Game Theory for Secure Internet of Battlefield Things (IoBT) Systems”, submitted, 2018.
- A. Sanjab, W. Saad, I. Guvenc, A. Sarwat, and S. Biswas, “Smart Grid Security: Threats, Challenges, and Solutions”, submitted, 2018.
- W. Saad, A. Sanjab, Y. Wang, C. Kamhoua, and K. Kwiat, “Hardware Trojan Detection Game: A Prospect-Theoretic Approach”, in *IEEE Transactions on Vehicular Technology*, vol. 66, no. 9, pp. 7697-7710, Sept. 2017.
- A. Sanjab and W. Saad, “Data Injection Attacks on Smart Grids With Multiple Adversaries: A Game-Theoretic Perspective”, in *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 2038-2049, July 2016.

Conference Publications:

- A. Ferdowsi, A. Sanjab, W. Saad and T. Başar, “Generalized Colonel Blotto Game”, in *Proc. of the Annual American Control Conference (ACC)*, Milwaukee, WI, USA, 2018, pp. 5744-5749 [the first two authors have equally contributed to this paper].
- A. Ferdowsi, A. Sanjab, W. Saad and N. B. Mandayam, “Game theory for secure critical interdependent gas-power-water infrastructure”, in *Proc. of Resilience Week (RWS)*, Wilmington, DE, 2017, pp. 184-190.
- A. Sanjab, W. Saad, and T. Başar, “Prospect Theory for Enhanced Cyber-Physical Security of Drone Delivery Systems: A Network Interdiction Game”, in *Proc. of the IEEE International Conference on Communications (ICC), Communication and Information Systems Symposium*, Paris, France, May 2017.

- G. El Rahi, A. Sanjab, W. Saad, N. B. Mandayam, and H. V. Poor, “Prospect Theory for Enhanced Smart Grid Resilience Using Distributed Energy Storage”, in *Proc. of the 54th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, September 2016.

- A. Sanjab and W. Saad, “On Bounded Rationality in Cyber-Physical Systems Security: Game-Theoretic Analysis and Application to Smart Grid Protection”, in *Proc. of the IEEE /ACM CPS Week, Workshop on Cyber-Physical Security and Resilience in Smart Grids*, Vienna, Austria, April 2016.

- A. Sanjab and W. Saad, “Smart grid data injection attacks: To defend or not?” in *Proc. of the IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Miami, FL, USA, Nov. 2015, pp. 380-385 **This paper received the Best Student Paper Award at IEEE SmartGridComm’15.**

Chapter 2

Game Theory for CPS Security

Securing CPSs against emerging threats requires not only an in-depth knowledge of the system, its vulnerabilities, and its interdependencies, but also an understanding of the interactions, learning, and decision making processes of the agents involved, such as attackers and defenders, which can be automated systems or humans. In fact, attacks are typically carried out by intelligent adversaries who learn from their experience and adapt to their environments. Indeed, adversaries engage in a continuously evolving dynamic decision making process [153] to actively design a certain cyber-physical attack. As such, an attack mechanism, that has a forceful impact, is one that is designed to consider potential defense mechanisms, that it may face, while devising the best possible attack strategy. Similarly, an effective defense strategy is one that accounts for potential attack strategies that it can face when devising corresponding defense mechanisms, developing security software tools, or reinforcing the security infrastructure of the CPS. Indeed, defense mechanisms must consider potential types of threats that they may face, possible infiltration points, as well as potential attack strategies in their design of defense strategies and mechanisms.

Hence, a comprehensive modeling of the interactive multi-agent decision making processes, in a CPS security settings, is indispensable to understanding the security state of a CPS and devising effective defense mechanisms. To this end, as corroborated by its successful applications in various engineering fields [147], such as wireless communication, power systems, and transportation systems, as well as various non-engineering fields, such as economics, political science, psychology, and biology, *game theory* [136, 146] provides powerful analytical tools and quantitative frameworks for the modeling and analysis of complex distributed multi-agent decision making processes in CPS security settings, which allow anticipating possible attacks strategies and developing fool-proof defense mechanisms and algorithms.

In this regard, in a typical CPS security setting, an operator (defender) aims at choosing a defense strategy, while typically constrained by limited resources, to minimize the potential damage to the system that a possible attack may cause. Mathematically, the defender must, hence, solve an optimization problem in which the objective function captures the damage that an attack can cause to the system while the constraints depend on the system model, operating conditions, and defense budget. However, in this case, the value function (i.e. value of the objective function) is not only dependent on decision variables controlled by the defender itself, but also on decision variables controlled by the attackers; since the achieved security level of a system is not only dependent on the implemented defense policy but also on the attack carried out. Similarly, an attacker typically aims at choosing the optimal attack strategy to maximize the inflicted damage to the system or a certain profit made from this attack (which can be financial, political...). However, as in the case of the defender, the level of the caused damage to the system is not only dependent on the attack strategy but also on the defense decisions. As such, an intelligent active attacker is one that investigates and learns potential defense mechanisms that it can face and incorporates such knowledge in the design of its optimal attack strategies. In this regard, game theory provides the necessary mathematical tools which enable the modeling and analysis of such multi-player CPS security optimization problems and allow the characterization and the enhancement of the security state of the CPS. Hence, this provides a distinct advantage over one-player optimization analyses of CPS defense strategies since it enables accounting for and predicting the attacker's behavior as part of the game-theoretic CPS security analyses. Such game-theoretic models enable, hence, an effective design of defense policies which explicitly factor in intelligent attack mechanisms. Indeed, a game-theoretic defense (attack) "strategy" is one that designs the best defense solution (attack policy) to each possible attack (defense mechanism) that it might face.

Therefore, game theory enables the modeling and anticipation of the decision making processes of the agents involved in CPSs security settings. Such agents can correspond to purely automated mechanisms or to humans. In this regard, classical game theory assumes that the players involved are fully rational. In other words, it is assumed that the players are fully objective and always choose the strategies that maximize their payoffs. This would mostly hold for automated mechanisms. However, CPS security settings incorporate a large number of humans such as operators, engineers, administrators, users, and hackers. In this regard, as has been observed in a number of empirical analyses and psychological experiments, when faced with risk, uncertainty, limited information, and extreme complexity – as is the case in CPS security settings – humans tend to act with bounded rationality; relying on subjective perceptions and assessments rather than on objective analyses. Hence, this bounded rationality must be incorporated in the developed security games to capture the way in which humans behave and make decisions in a CPS security setting. This subjective behavior modeling and incorporation in CPS security analyses is one of the major contributions of this dissertation.

As such, this chapter focuses on introducing the fundamentals of game theory, their potential use in CPS security settings, as well as on introducing psychological mathematical models which can be used to account for the subjective behavior of humans in CPSs security analyses. As such, this chapter is organized as follows. Section 2.1 provides an overview of the fundamentals of game theory. Section 2.2 introduces the concept of CPS security games motivating the use of game theory in CPS security settings. Moreover, Section 2.3 and Section 2.4 introduce various types of games which are of main interest to this dissertation and provide an overview of recent research works which have implemented these types of games for CPS security analyses. In addition, Section 2.5 introduces mathematical models which enable modeling the potential subjective behavior of humans in CPS security analyses.

2.1 Game Theory - A Brief Overview

Game theory provides a set of mathematical tools and quantitative frameworks used to analyze interdependent decision making between entities, referred to as players, with interconnected, conflicting or aligned, interests [146, 154]. A game in its standard form consists of the following elements:

1. *Players:* The players are the entities participating in the game who make decisions and whose decisions affect the outcome of the game.
2. *Strategy space:* A strategy space of a player is the set of alternatives that this player has and from which it must choose a certain strategy. Here, a strategy is a decision rule that each player seeks to develop.
3. *Utility functions:* The utility function of a player is the objective function of this player which depends on its own chosen strategy and on the strategies chosen by the other players.

Hence, in a game, each player chooses a strategy, from a number of alternatives, aiming at maximizing a benefit or minimizing a loss that is generally captured by a utility function which not only depends on the player's own strategy but also on the strategies chosen by the opponents.

Various game types have been introduced and studied since the first contributions in the field of game theory and strategic decision making. Some of the game types which are of particular interest to the work in this dissertation are summarized next [146, 154].

- **Noncooperative vs. cooperative:** In an noncooperative game, players are assumed not to have the ability to communicate and potentially cooperate. Noncooperative games typically model competitive interactions in which the interests of the set of players are fully or partially conflicting. In noncooperative games, players are assumed not to have the ability to coordinate and communicate. Hence, if a cooperation is beneficial for the players, this cooperation must be self-enforcing without the need or the existence of any coordination between these players. On the other hand, in a cooperative game, players can communicate, cooperate, and form coalitions. As such, in a cooperative game framework, players have the ability to form agreements which can affect their strategic choices as well as their resulting achieved utility.
- **Static vs. dynamic:** In static games, the players typically choose their actions simultaneously, or equivalently, without observing each others' current or previous actions. In this respect, in static games, the players typically play once and independently of each other; without being influenced by actions and game outcomes which occurred at previous time periods. Hence, the notion of time, or game history, is absent in static games. On the other

hand, dynamic games are games in which players make decisions in a sequence over time and in which the decision taken by a player, at a time period, depends on its acquired information of the game in its current and previous time stages (which can include a player's own previous actions, opponents' previous decisions, and previous states of the game itself). Hence, in dynamic games, each player must choose a decision rule (i.e. a strategy) which specifies the action to be taken depending on quantities that are not fully controlled by the player itself. This leads to a clear distinction between a strategy (which is a decision rule) and an action.

- **Zero-sum vs. nonzero-sum:** Zero-sum games typically consider two players whose objectives are completely conflicting. A profit for a player causes an equal loss to its opponent. Thus, under zero-sum games, the summation of the utility functions of the players is identically zero. If the summation of the utility functions is equal to a constant value, the game is known as a constant-sum game. A constant-sum game can typically be transformed to a zero-sum game. In zero-sum games, one player is typically a maximizer – whose goal is to maximize its gain – and the other player is a minimizer – whose goal is to minimize its loss. Games which do not have the zero-sum (or constant-sum) property are known as nonzero-sum games.

- **Complete vs. incomplete information:** Complete information implies that the players have a complete knowledge of the structure of the game (such as the game rules, the set of players, and the strategy spaces and utility functions of the players). Otherwise, the game is of incomplete information.

- **Deterministic vs. stochastic games:** A game is deterministic if its outcome is solely dictated by the strategies chosen by the players. A stochastic game is one in which the outcome depends on the player's strategies as well as the "state" of the game, which is probabilistically influenced by the players' decisions. In stochastic games, based on the players' actions, the game transitions probabilistically from one state to the other. As such, a player's strategy typically seeks to specify an action to be taken at each possible state of the game.

Classical game theory assumes that the players involved are *fully rational*. Rationality of the players typically reflects that the players are purposeful, which indicates that each of them always seeks to optimize a given utility function, without making mistakes, based on objective observations of the game environment and structure. When players deviate from this full rationality assumptions, they are known to act with *bounded rationality*.

These various types of games can be used in CPS security analyses based on the security settings and the entities involved. In the next section, the use of game theory for CPS security analyses is explored.

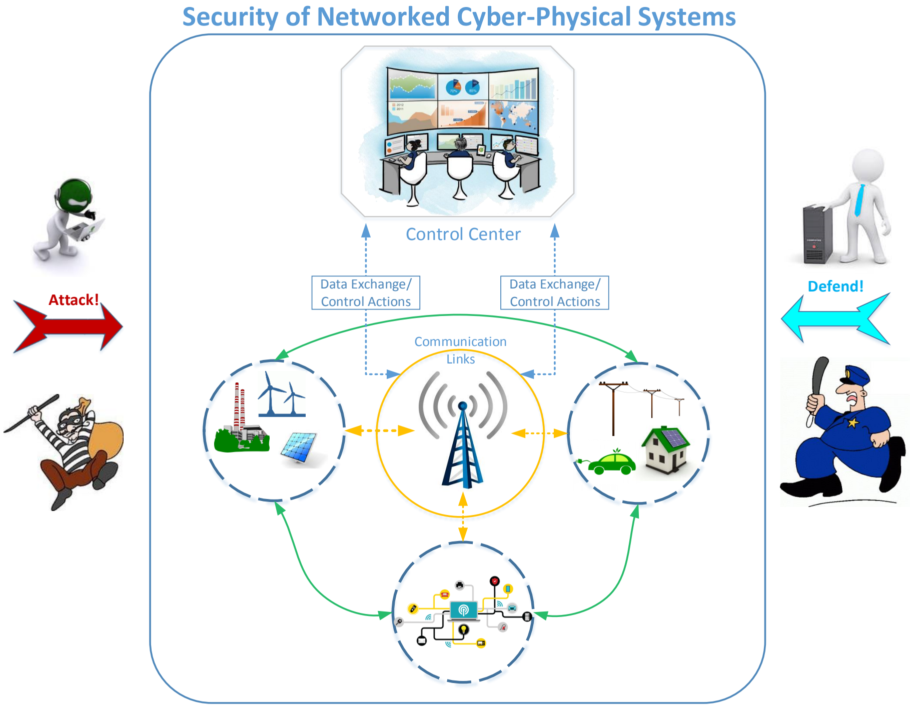
Security of Networked Cyber-Physical Systems
Control Center
Data Exchange/ Control Actions
Data Exchange/ Control Actions
Communication Links
Attack!
Defend!

Figure 2.1: Illustrative representation of defense vs. attack in CPS security settings.

2.2 Security Games: Securing Cyber-Physical Systems

A number of research works have used game theory to model the decision making processes of defenders and adversaries in conventional network security applications as surveyed in [155] and the references therein. However, the coupling between the physical and cyber layers in CPSs, as well as the more pronounced presence of the human layer, pose new challenges that game-theoretic models must consider. In this section the concept of CPS security games is introduced.

In this respect, CPS security games model the interdependent decision making processes and strategic interaction between attackers, aiming at attacking a given CPS, and defenders aiming at defending that system. An illustration of such interaction is provided in Fig. 2.1.

In a CPS security game, the players constitute attackers and defenders while the strategy spaces constitute the potential attack or defense strategies that can be, respectively, carried out or implemented. Such possible attack and defense strategies depend on the underlying CPS. The utility function of the attacker typically captures a level of damage than can be caused to the system or a certain financial, strategic, or political benefit that the attacker can reap from such attacks. As for the defender, the utility function typically reflects the level of damage that an attack can inflict on the system or deviations from normal operating state of the system, due to an attack, that must be minimized (in this case the utility function is a cost function).

In such CPS security games, the attack and defense strategies are subject to a number of constraints. Two of the main constraints can be summarized as follows:

- **Practicality constraints:** A CPS defender's goal must not exclusively be to protect the system from potential threats. It must also meet the CPS's performance requirements. Indeed, a maximum cyber-physical security can be potentially achieved using a complete disconnection of all forms of wireless communication and Internet connectivity from the physical system. However, even though such a strategy can enhance the security of the CPS, it deprives it from the operational and economic advantages that such communication systems provides. Equivalently, designing a robust control system against an extremely wide range of possible disturbances can make the system unable to meet all the performance requirements of its intended application [92]. Therefore, security solutions must ensure the security of CPSs while meeting their performance requirements and offering a high quality of operational service.

- **Feasibility restrictions:** The attackers and defenders have limited resources which they can use to implement their attack or defense strategies. These resources can comprise monetary resources, skills, computational capacity, and time, among others. Thus, the attackers' and defenders' strategies must abide by their corresponding recourse limits.

The nature of the strategic interactions between the various attackers and defenders depends on the application domain in which they are interacting, the amount of information that each has, the objective of each, and their respective constraints.

Next, various types of games of complete and incomplete information, which are fundamental for CPS security games and which are of particular interest to the current work, are introduced along with a survey of some of the research works in literature which have focused on these types of games.

2.3 Complete Information CPS Security Games

In this section, CPS security research contributions are considered in which deterministic games of complete information are considered. These games can be static or dynamic. However, next, the static type of such games is explored since it provides the needed insights.

2.3.1 Static Noncooperative Games

Zero-sum Games

Given that an attacker and defender have, typically, opposing objectives, a number of research works [93, 103, 104] have modeled their strategic behavior as a zero-sum game. Letting s^a denote a strategy chosen by the attacker from a strategy set $\mathcal{S}^A$ and s^d denote a strategy chosen by the defender from a strategy set $\mathcal{S}^D$, the utility functions of the attacker, $U^A(s^a, s^d)$, and the utility function of the defender, $U^D(s^a, s^d)$, are such that:

$$U^D(s^a, s^d) = -U^A(s^a, s^d). \tag{2.1}$$

Since, when optimizing its payoff, an attacker causes a worst payoff for the defender, and vice versa, each of the two may seek to choose the best worst-case payoff that the opponent may cause. This is known as a *minimax* strategy, *security strategy*, or *prudent strategy*. In this respect, an attacker aiming at maximizing a damage, $U^A(s^a, s^d)$, to the system and a defender minimizing that damage have the following respective objectives:

$$s_a^* = \max_{s^a} \min_{s^d} U^A(s^a, s^d), \quad s_d^* = \min_{s^d} \max_{s^a} U^A(s^a, s^d). \tag{2.2}$$

Zero-sum games have been used to model CPS security problems in a variety of applications such as in [91, 93–104, 104]. For instance, the work in [93] considers data injection attacks on a power system state estimation using a zero-sum game in which the attacker aims at increasing a power flow estimate over a transmission line while the defender (i.e. smart grid operator) aims at decreasing that estimate. In addition, the authors in [104] consider jamming attacks on CPS state estimators in which a sensor and the attacker play a zero-sum game where the attacker aims a maximizing a cost function related to estimation quality while the defender aims at minimizing this cost function. The work in [103] introduces a defense framework against Stuxnet-like malware in which a zero-sum game is used to model the interaction between the attacker and the network. In this zero-sum game, the adversary aims at maximizing the impact of its data injection on the system performance while the network aims at decreasing this effect.

Nonzero-sum Games

In addition to zero-sum games, general (nonzero-sum) static noncooperative games modeling the strategic interaction between attackers and defenders have also been used in literature such as in [106, 108, 156, 157], among others. In such games, even though their objectives are conflicting, the attackers' and defenders' utilities are not limited to the case in which they are perfectly opposing. For example, a defender's objective can correspond to minimizing the potential damage to the system that the attacker may cause while the attacker's objective can correspond to maximizing a financial profit that it can reap from this attack. In this case, the utility function of the defender reflects the damage to the system while the utility function of the attacker reflects its financial benefit. Hence, even though these objectives are conflicting, the utilities of the attacker and defender do not necessarily sum to zero.

Various research works have modeled CPS security problems using static noncooperative games. In [156], a static noncooperative game between an attacker and a defender over a CPS is introduced in which the attacker aims at compromising a number of system resources, in the cyber and physical systems, aiming at causing a system collapse while the defender aims a keeping the number of uncompromised resources over a given threshold to insure the operation and survival of the system. In addition, the work in [106] studies advanced persistent threats while simultaneously considering stealthy attacks and insider threats. In this regard, a noncooperative game is proposed to model the strategic interaction of three players – an attacker, a defender, and an insider which can choose to help either the attacker or defender. In [157], security risk management of a smart grid with interconnected communication and power systems is considered. In this regard, a noncooperative game between an attacker and a defender is formulated in which the defender aims at protecting a set of communication equipment while the attacker aims at compromising a set of communication devices to inflict the highest possible damage to the grid. The work in [157] also considers a Stackelberg game. This type of games is introduced in Section 2.3.2.

Equilibrium Analysis

In such games, each of the attacker and defender aims at choosing its best response strategy given the strategies chosen by the opponent. The best response strategy, $s^{a^*} \in \mathcal{S}^A$, of an attacker to strategy $s^d \in \mathcal{S}^D$ by the defender is one that satisfies the following relation; assuming the attacker maximizes a utility function given by $U^A(s^a, s^d)$:

$$U^A(s^{a^*}, s^d) \geqslant U^A(s^a, s^d) \ \ \forall s^a \in \mathcal{S}^A. \tag{2.3}$$

On the other hand, the best response strategy, $s^{d^*} \in \mathcal{S}^D$, of a defender to a strategy $s^a \in \mathcal{S}^A$ by the attacker satisfies the following relation; assuming the defender minimizes a cost function given by $U^D(s^a, s^d)$:

$$U^D(s^a, s^{d^*}) \leqslant U^D(s^a, s^d) \ \ \forall s^d \in \mathcal{S}^D. \tag{2.4}$$

An equilibrium of the game is achieved when the attacker's and defender's best response strategies intersect. In that situation, given that each is playing a best response, none of the attacker or defender have any incentive to deviate from this best-possible strategy. Such an equilibrium state is known as a *Nash equilibrium* and is defined as follows:

Definition 1. *An attack strategy, s^{a^*}, and a defense strategy, s^{d^*}, constitute a Nash equilibrium if:*

$$U^A(s^{a^*}, s^{d^*}) \geqslant U^A(s^a, s^{d^*}) \ \ \forall s^a \in \mathcal{S}^A, \tag{2.5}$$

$$U^D(s^{a^*}, s^{d^*}) \leqslant U^D(s^{a^*}, s^d) \ \ \forall s^d \in \mathcal{S}^D, \tag{2.6}$$

while considering the attacker to be a maximizer and the defender to be a minimizer.

Given that under such a Nash equilibrium strategy profile each of the attacker and defender choose an optimal strategy with respect to the strategy of the opponent, any unilateral deviation from this Nash equilibrium, by any of the attacker and defender, will not lead to an improve in its achieved utility. As such, none of the attacker nor defender has any incentive to unilaterally deviate; hence, the game is at equilibrium.

Attackers and defenders may choose to pick their strategies based on a realization of a probability distribution over their decision (i.e. action) spaces. In this case, rather than choosing a certain action deterministically, a player's strategy would correspond to choosing a probability distribution over its set of possible actions. Such a probability distribution specifies the likelihood of choosing each of the actions in its action space. Such probabilistic strategies are known as *mixed strategies*; while deterministic strategies are known as *pure strategies*. Let $\boldsymbol{\sigma}^a \in \mathit{\Gamma}^A$ and $\boldsymbol{\sigma}^d \in \mathit{\Gamma}^D$ denote the probability distributions, i.e. mixed strategies, over the action spaces $\mathcal{S}^A$ and $\mathcal{S}^D$ of, respectively, the attacker and defender – where $\mathit{\Gamma}^A$ and $\mathit{\Gamma}^D$ are the set of such possible distributions – the concept of best response can be extended to mixed strategies as follows. Let E_u^A denote the expected utility of the attacker (to be maximized), the attacker's best response mixed strategy, $\boldsymbol{\sigma}^{a^*}$, to a defender's mixed strategy, $\boldsymbol{\sigma}^d$, satisfies:

$$E_u^A(\boldsymbol{\sigma}^{a^*}, \boldsymbol{\sigma}^d) \geqslant E_u^A(\boldsymbol{\sigma}^a, \boldsymbol{\sigma}^d) \ \ \forall \boldsymbol{\sigma}^a \in \mathit{\Gamma}^A. \tag{2.7}$$

Similarly, let E_u^D denote the expected cost of the defender (to be minimized). Then, the defender's best response mixed strategy, $\boldsymbol{\sigma}^{d^*}$, to an attacker's mixed strategy, $\boldsymbol{\sigma}^a$, satisfies:

$$E_u^D(\boldsymbol{\sigma}^a, \boldsymbol{\sigma}^{d^*}) \leqslant E_u^D(\boldsymbol{\sigma}^a, \boldsymbol{\sigma}^d) \ \ \forall \boldsymbol{\sigma}^d \in \mathit{\Gamma}^D. \tag{2.8}$$

The notion of Nash equilibrium can be also extended to incorporate mixed strategies. In this regard, the game is at equilibrium when each of the players, attacker and defender, chooses a best response mixed strategy with respect to the best response strategy of the opponent. In that case, the game is at equilibrium since none of the attacker nor defender has any incentive to deviate from these mixed strategies. Such an equilibrium under mixed strategies is known as a *mixed strategy Nash equilibrium* and is formally defined as follows:

Definition 2. *An attack mixed strategy, $\boldsymbol{\sigma}^{a^*}$, and a defense mixed strategy, $\boldsymbol{\sigma}^{d^*}$, constitute a mixed strategy Nash equilibrium if:*

$$E_u^A(\boldsymbol{\sigma}^{a^*}, \boldsymbol{\sigma}^{d^*}) \geqslant E_u^A(\boldsymbol{\sigma}^a, \boldsymbol{\sigma}^{d^*}) \ \ \forall \boldsymbol{\sigma}^a \in \mathit{\Gamma}^A, \tag{2.9}$$

$$E_u^D(\boldsymbol{\sigma}^{a^*}, \boldsymbol{\sigma}^{d^*}) \leqslant E_u^D(\boldsymbol{\sigma}^{a^*}, \boldsymbol{\sigma}^d) \ \ \forall \boldsymbol{\sigma}^d \in \mathit{\Gamma}^D, \tag{2.10}$$

while considering the attacker to be a maximizer and the defender to be a minimizer.

2.3.2 Stackelberg Games

A Stackelberg game is a type of games involving hierarchy between the players, i.e. leader(s) and follower(s). In this regard, a leader chooses its strategy and the follower(s) respond to the leader's strategy [146]. Accordingly, the leader should have the capacity to anticipate the potential response of the followers before choosing its strategy.

In a CPS security context, an attacker can be modeled as a leader targeting a component of the CPS while the defender can observe that an attack has targeted the system and respond accordingly. Thus, in this application, the defender can be modeled as a follower. It is important here to note that the attacker should be able to anticipate the way in which the defender will respond to this attack and takes this anticipation into consideration when choosing its attack strategy. In other applications, a defender can be modeled as a leader while the attacker can be a follower. In this regard, the defender can choose to enhance the robustness of its system by implementing new security measures. An attacker can observe the occurrence of such security reinforcements and respond accordingly.

We consider a game in which the defender is a leader and the attacker acts as a follower. In addition, consider that the defender aims at minimizing a cost function, $U^d(s^a, s^d)$, and the attacker aims at maximizing a cost function $U^a(s^a, s^d)$. In this regard, the optimal reaction set, $\mathcal{R}^a(s^d) \subset \mathcal{S}^A$, of the attacker to a chosen strategy s^d by the defender is the set of optimal attack strategies that the attacker can implement when the defender chooses a defense strategy s^d. This optimal reaction set is, hence, defined as follows:

$$\mathcal{R}^a(s^d) = \{\zeta^a \in \mathcal{S}^A : U^a(\zeta^a, s^d) \geq U^a(s^a, s^d), \forall s^a \in \mathcal{S}^A\}. \tag{2.11}$$

Based on the definition of this optimal reaction set, the *Stackelberg equilibrium* of the game is defined as follows:

Definition 3. *The strategy pair (s^{a^*}, s^{d^*}) in which the defender is a leader and the attacker is a follower is a* Stackelberg equilibrium *of the game if:*

$$U^D(\mathcal{R}^a(s^{d^*}), s^{d^*}) \leqslant U^D(\mathcal{R}^a(s^d), s^d) \ \ \forall s^d \in \mathcal{S}^D. \tag{2.12}$$

and

$$s^{a^*} \in R^a(s^{d^*}), \tag{2.13}$$

while considering the attacker to be a maximizer and the defender to be a minimizer.

One should note that some games involve multiple leaders and/or multiple followers. In this regard, the group of followers can play, for example, a static noncooperative game in response to the static noncooperative game played by the group of leaders. This case is studied, for instance, in [158].

Multiple research works have used Stackelberg games to study CPS security problems such as in [110, 113, 157], among others. For instance, the authors in [157] consider a model in which the attacker reacts to security measures implemented by the defender and, hence, model the attacker as a follower and the defender as a leader in a Stackelberg model. Moreover, the work in [110] considers a CPS in which state measurements and control signals are subject to coordinated jamming by adversaries. A two-level Stackelberg game is considered in which the control jammer is a follower of the system operator which in turn is a follower of the measurement jammer. In [113], the authors study the security of networked 3D printers using a Stackelberg game model. This work considers that the control design of the printing process is subject to physical disturbances while the cyber layer – connecting users to 3D printers – are subject to cyber attacks. In this regard, the integrity of the commands sent to the 3D printers is based on the outcome of the attacker vs. defender game at the cyber layer. As such, in the Stackelberg game formulation, given that the physical system receives commands from the cyber layer, the physical system is modeled as a follower to the attacker vs. defender cyber game.

This section has explored a number of complete information CPS security games. Next section will focus on games of incomplete information in which each of the attacker and defender might have a limited knowledge about its opponent.

2.4 Incomplete Information CPS Security Games

In security settings, each player may not have complete information about the properties of other players. The strategic interactions between the players in such settings can be captured using *Bayesian games*. In Bayesian games, each player i is assumed to have a "type", t_i, from a number of possible types $\mathcal{T}_i$, and the realizations of the types of each player follow a joint probability distribution which is usually known by all the players. When the game is played, each player i knows its own type, t_i. Given its type, each player chooses a strategy that optimizes its payoff given its belief over the distributions of the types of all other players [136,154]. A player's strategy, s^i, is one that associates an action with every one of its possible types, t_i. An optimal strategy s^{i^*} is such that each $s^{i^*}(t_i)$ maximizes the player's expected payoff given the beliefs over the types of all other players. For example, consider one defender and one attacker (this example can be readily generalized to multiple defenders and multiple adversaries) and consider that the defender's type is t_d, the set of possible types of the attacker is denoted by $\mathcal{T}^A$, and the joint probability density function of the defender's and attacker's types is given by $\text{Pr}(t_d, t_a)$. The defender's optimal defense strategy, $s^{d^*}(t_d)$, is one that solves (assuming the defender aims at minimizing an expected cost):

$$\min_{s^d \in \mathcal{S}^d} \sum_{t_a \in \mathcal{T}^A} \text{Pr}(t_a|t_d) U^D((s^{a^*}(t_a), s^d), (t_a, t_d)), \tag{2.14}$$

where $\text{Pr}(t_a|t_d)$ denotes the probability of the attacker being of type t_a given that the defender is of type t_d and follows from Bayes' rule:

$$\text{Pr}(t_a|t_d) = \frac{\text{Pr}(t_d, t_a)}{\sum_{t'_a \in \mathcal{T}_a} \text{Pr}(t_d, t'_a)}. \tag{2.15}$$

The game is at equilibrium when all the players play their optimal strategies (specifying each player's optimal action for each one of its possible types) with respect to each other following (2.14) [154]. This equilibrium is known as a *Bayesian Nash equilibrium*.

Different versions of Bayesian-based games can also be used in the case of dynamic games with imperfect information, i.e. dynamic games in which a player does not have a perfect observation of the previous sequence of play and game states. In such games, the beliefs are built over the potential histories of the games (i.e. over the sequence of actions which could have been chosen by the players in past time periods). Such beliefs typically follow from Bayes' rule.

One of the most famous applications of Bayesian games to CPS security problems is the popular Bayesian Stackelberg security model implemented at the Los Angeles international airport [159]. In this model, the defender acts as leader and aims to choose a scheduling strategy for security checkpoints and canine patrols while facing many types of adversaries which act as followers. An additional application of Bayesian games to CPS security is presented in [160] in which the interaction between a service provider and clients, who can be of the benign or attacker types, is modeled using a Bayesian game model. In a nutshell, the advantages of using Bayesian games consist in their ability to capture the incomplete information that the attacker or defender can have about the properties of its opponents.

The assumption of rationality of the players, attackers and defenders, is essential to all the previously presented game-theoretic models. This underlying assumption can be accurate in the case where the agents involved in the CPS games are automated systems. However, many humans are, in fact, involved in CPS security settings such as operators, hackers, users and engineerings. The strategic behavior of these humans is highly affected by their environment, their perceptions, and the uncertainty and risk they face in CPS security settings. Such factors may lead humans to deviate from the notion of full rationality. As such, the underlying assumption of full rationality constitute the main limitation of the the CPS security game models surveyed so far in this chapter. Indeed, such bounded rationality should be carefully studied and incorporated in the security analyses model to improve the accuracy and the applicability of the obtained solutions.

Therefore, next section introduces various quantitative mathematical frameworks which allow capturing human decision making under uncertainty (using prospect theory and cumulative prospect theory), human subjective perception of skills levels (using cognitive hierarchy theory), and human decision making under scarcity of information (using the concept of satisfaction equilibrium), and proposes and motivates the need for the incorporation of such behavioral frameworks in security analyses. Indeed, one of the contributions of this work consists in bringing notions from psychology and behavioral decision making into the analyses of CPS security to allow the derivation of effective security solutions which explicitly account for the prominent human layer in cyber-physical systems.

2.5 Game-Theoretic Techniques with Bounded Rationality

When faced with risk, incomplete information, extreme complexity, and tight constraints (such as time and computational capacity) humans tend to act with bounded rationality [148, 149, 161]. Hence, the behavioral aspect of humans involved in CPS security settings must be incorporated in the decision making models within CPSs security analyses. This section introduces a number of fundamental mathematical principles, which are based on psychological experiments and empirical observations, and which can be used to model the bounded rationality and subjectivity of players in CPSs security.

2.5.1 Prospect Theory

Classical Prospect Theory

In their seminal work [148], Kahneman and Tversky noted that – when faced with risk and uncertainty – humans' decision making processes drift from full rationality assumed by the conventionally used principles of expected utility theory (EUT) (used for example in the derivation of mixed best response strategies as in (2.3) and (2.4) and hence deviate from the full rationality assumed in classical game-theoretic models. To this end, they proposed an alternative theory of choice which they labeled *prospect theory* (PT) and which can predict, more closely, the decisions that humans would make when faced with different probabilistic alternatives (i.e. gambles). Prospect theory is a Nobel prize-winning theory (Nobel prize in economic sciences in 2002) which has gained wide acknowledgment and is considered to have drastically advanced the field of behavioral economics.

A prospect is a gamble $g_1 \triangleq (x_1, p_1; ...; x_n, p_n)$ with n possible outcomes, where each outcome x_i can occur with a probability p_i. Decision making analysis aims at predicting the choice that humans would make when faced with different prospects. EUT is a conventionally used theory to model such decision making under uncertainty whose tenets can be summarized as follows:

- *Expectation*: the main principle behind EUT is assuming that a prospect is valued based on its expected value; and hence, a decision maker would choose the prospect which yields the highest expected outcome. The expected value of a prospect g_1 is denoted by $U(g_1)$ and is defined as follows:

$$U_{g_1} \triangleq U(x_1, p_1; ...; x_n, p_n) = \sum_{i=1}^{n} p_i u(x_i), \tag{2.16}$$

where $u(x_i)$ is the utility that a decision maker experiences from receiving an outcome x_i. This expectation principle entails an axiom known as the substitution axiom which states that; if a gamble g_1 is preferred to a gamble g_2, then weighing all the outcomes of each gamble with the same probability does not change this order of preference. In other words, let $\succ$ denote a preference relation where $g_1 \succ g_2$ implies that g_1 is preferred to g_2, the substitution axiom is stated as follows:

$$g_1 \succ g_2 \Rightarrow (g_1, p) \succ (g_2, p). \tag{2.17}$$

- *Asset integration:* The second principle of EUT states that a decision maker values a prospect as acceptable if the expected utility resulting from this prospect exceeds the original value of the decision maker's assets w, i.e. original state of wealth. This condition is mathematically expressed as follows:

$$U(w + x_1, p_1; ...; w + x_n, p_n) > U(w). \tag{2.18}$$

- *Risk aversion:* The third principle of EUT states that a decision maker has a diminishing marginal utility which translates into risk aversion since the value of an additional unit of gain decreases with an increase in wealth. This is mathematically modeled using a concave function of wealth, $u(.)$, i.e.:

$$u''(w) < 0, \tag{2.19}$$

  where $u''(.)$ denotes the second derivative of $u(.)$ with respect to the wealth level w.

However, various experiments and empirical observations, as described in [148, 149], have shown that decision making under uncertainty does not typically abide by the tenets of EUT. To this end, to more accurately capture decision making under risk, prospect theory was proposed in [148] as an alternative theory of choice which describes and predicts the way humans make decisions under uncertainty.

Prospect theory models and predicts more closely the way humans subjectively value outcomes and the probability of their occurrence. In this regard, PT experiments have shown that humans typically value outcomes subjectively as gains and losses with respect to a certain subjective reference point rather than as an absolute quantity. This effect is known as the *framing effect*. In addition, PT has observed that humans do not typically perceive probabilities objectively but weight the probability of occurrence of outcomes subjectively. This effect is known as the *weighting effect*. Here, the word "typically" is used to reflect that, statistically, the vast majority of humans follows these decision making traits.

In this regard, the observations leading to the framing effect are summarized next.

- *Outcomes as gains and losses:* PT has shown that humans do not perceive outcomes as absolute quantities. In fact, they typically perceive outcomes as gains and losses with respect to a certain reference point which, for example, can represent their original state of wealth.

- *Risk aversion in gains – risk seeking in losses:* Based on such observation of outcomes as gains and losses, PT experiments have shown that humans are risk averse when it comes to gains and risk seeking when it comes to losses. In other words, experiments have shown that humans would typically prefer a sure gain over a larger probable one (up to a certain extent) even if the expected value of the probable gain exceeds that of the sure gain. On the other hand, experiments have shown that when it comes to losses, humans typically prefer probable outcomes over sure ones (up to a certain extent) even if the expected value of the sure loss exceeds that of the probable one.

- *Losses loom larger than gains:* PT experiments have shown that humans typically exaggerate losses. Losses are typically perceived to be much larger then they really are. In other words, one can think about the following experiment: if one is presented with a game in which a coin is tossed and the participant would loose $\$1$ if "heads" is the outcome of the toss and wins $\$x$ if the outcome of the toss is "tails". How large should x be for such a game to be attractive to a player. PT experiments have actually shown that for this game to be attractive x falls in the range of $\$2 - \$3$.

As such, to model this valuation of outcomes, a value function, $v(.)$, must replace the wealth function $u(.)$ in (2.16). This value function has been derived to capture the various empirical observations and is defined as follows:

$$v(X) = \begin{cases} X^{\beta^+}, & x \geq R \\ -\lambda(-X)^{\beta^-}, & x < R \end{cases} \quad \text{for } \beta^+, \beta^- \in (0,1) \text{ and } \lambda > 1, \tag{2.20}$$

where X is defined with respect to a reference point R. In other words, if x is an outcome of a prospect, then $X = x - R$.

This value function is plotted in Fig. 2.2. It is concave in gains and convex in losses to reflect risk aversion in gains and risk seeking in losses. The parameters β^+ and β^- shape the concavity/convexity of this function. The value of these parameters are typically derived based on the application. Moreover, the value function in (2.20) incorporates the loss factor λ which represents the exaggeration of losses with respect to gains.

The weighting effect, on the other hand, models the way humans typically perceive the probability of occurrence of events subjectively. In this respect, PT experiments have shown that humans typically overweight low probabilities and underweight high probabilities. At its extreme (i.e. when the perception of probabilities is most distorted) this probability weighting would have the following effect. Rather than observing a continuum of probabilities, humans tend to perceive three states of likelihood: 1) outcomes that would never occur (probability of occurrence is 0), 2) outcomes that will certainly occur (probability of occurrence is 1), and 3) all other outcomes are almost equally likely to occur. This weighting effect is captured by a weighting function, $\omega(.)$, which takes an objective probability as input and returns a subjective decision weight as output. Two weighting functions are most commonly used: 1) the weighting function proposed in [149], the mathematical expression of which is given in (2.21) and associated plot is given in Fig. 2.3, and 2) the weighting function proposed in [162], known as the Prelec function, whose mathematical expression is given in (2.22), and which is plotted in Fig. 2.4.

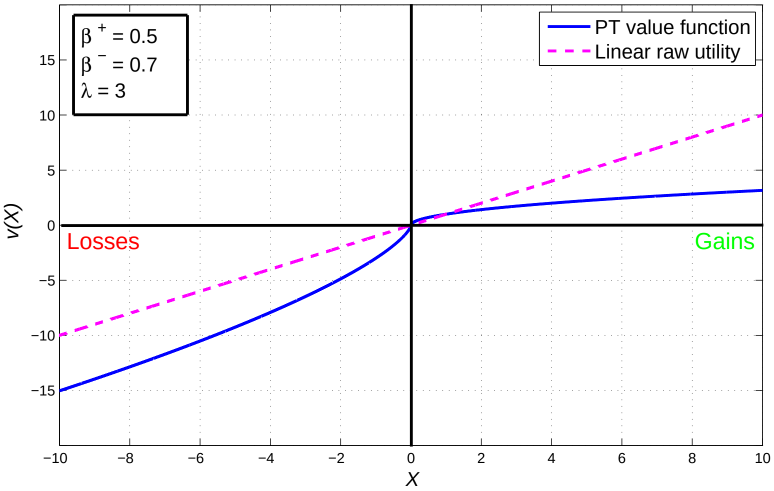

Figure 2.2: Prospect-theoretic value function

$$\omega^+(p_i) = \frac{{p_i}^\gamma}{({p_i}^\gamma + (1-p_i)^\gamma)^{1/\gamma}}. \tag{2.21}$$

$$\omega(p_i) = e^{-(\,-ln(p_i)\,)^\gamma}. \tag{2.22}$$

The rationality parameter, $\gamma \in [0,1]$, in (2.21) and (2.22) reflects the degree of subjectivity of a player. A lower γ implies that a decision maker has a more subjective (distorted) perception of probabilities. In this respect, for $\gamma = 1$, $\omega(p_i)$ reduces to the objective probability, p_i.

Here, we note that a number of alternative weighting functions have also been derived in literature and are discussed thoroughly in [163].

Based on these framing and weighting effects, in contrast to the predictions of EUT in (2.16), a decision maker values a gamble $(x_1, p_1; ...; x_n, p_n)$ based on its personal subjective valuation captured by the following valuation function, $V(.)$:

$$V(x_1, p_1; ...; x_n, p_n) = \sum_{i=1}^{n} \omega(p_i) v(x_i), \tag{2.23}$$

where $v(.)$ follows the value function in (2.20) and $\omega(.)$ follows the weighting function in, for instance, (2.21) or (2.22).

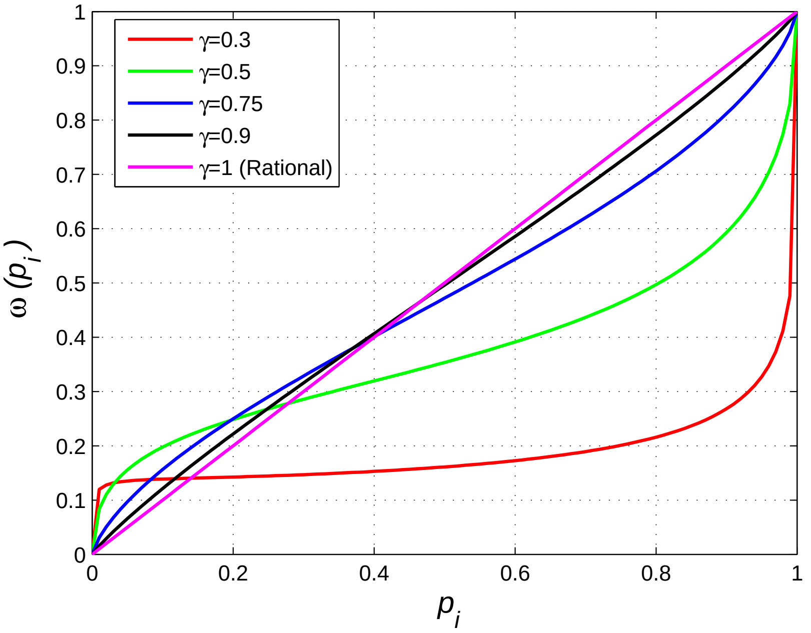

Figure 2.3: Weighting function.

Cumulative Prospect Theory

Cumulative prospect theory (CPT) was introduced in [149] as an extension to the fundamental concepts of prospect theory introduced in [148]. In this regard, CPT can account for prospects that have large number of outputs. CPT admits the same framing effect, captured by the value function shown in (2.20), but admits a different method for probability weighting. In this regard, rather than weighting individual probabilities, CPT weights cumulative probabilities of occurrence of outcomes. The underlying mathematical framework of CPT is presented next.

Considering prospect $g(x_i, p_i)$, which lists every possible outcome x_i and its associated probability of occurrence p_i. In cumulative prospect theory, the value of every outcome x_i, denoted by $v(x_i)$, is defined with respect to a reference point R, as shown in (2.20). As such, based on the signs of each $v(x_i)$, prospect g can be split into two prospects: a negative prospect, g^-, and a positive prospect, g^+. In this respect, g^- contains the outcomes valued as losses, and g^+ contains the outcomes valued as gains. In addition, let each of the two prospects be ranked in ascending order based on the values, $v(x_i)$. As such, consider that g^- is composed of m terms, which we index from $-m$ to -1, and g^+ is composed of n terms, which we index from 1 to n. Under cumulative prospect theory – different to the valuation under classical prospect theory in (2.23) – the valuations $V(g^+)$ and $V(g^-)$ of the positive and negative prospects are given by:

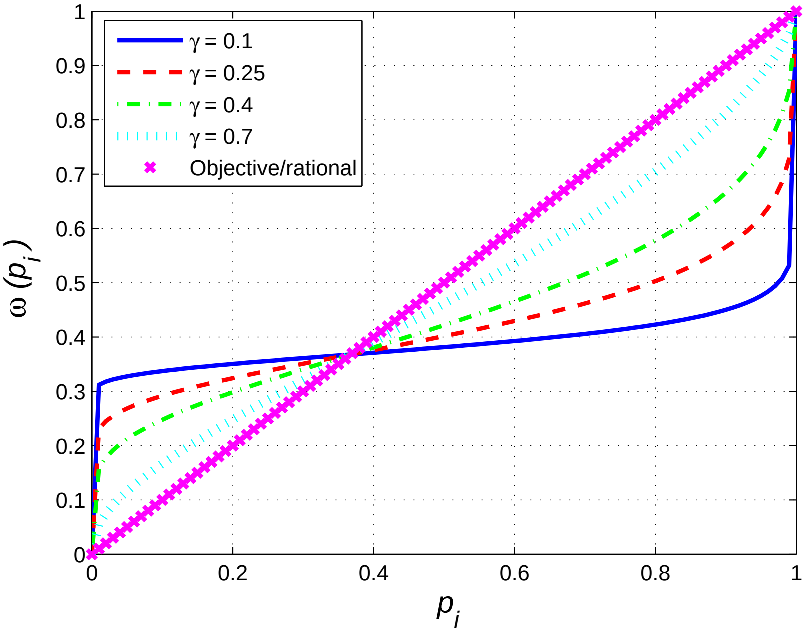

Figure 2.4: Prelec weighting function.

$$V(g^+) = \sum_{i=1}^{n} \pi_i^+ v(x_i), \tag{2.24}$$

$$V(g^-) = \sum_{i=-m}^{-1} \pi_i^- v(x_i). \tag{2.25}$$

As such, the valuation, $V(g)$, of prospect g is given by:

$$V(g) = V(g^+) + V(g^-). \tag{2.26}$$

Here, π_i^+ and π_i^- capture the decision weights. However, in CPT, these weights are defined based on the cumulative probability of occurrence of their corresponding outcomes, x_i. In this regard, π_i^+ and π_i^- are defined as follows:

$$\pi_i^+ = \omega^+(\sum_{j=i}^{n} p_i) - \omega^+(\sum_{j=i+1}^{n} p_i), \tag{2.27}$$

$$\pi_i^- = \omega^-(\sum_{j=-m}^{i} p_i) - \omega^-(\sum_{j=-m}^{i-1} p_i). \tag{2.28}$$

Here, $\omega^+(.)$ and $\omega^-(.)$ are the weighting functions, each of which follows the weighting function expression in (2.21), but may contain different parameter values for the positive and negative prospects. In this regard, $\omega^+(.)$ and $\omega^-(.)$ are defined as follows:

$$\omega^+(p) = \frac{p^{\gamma^+}}{(p^{\gamma^+} + (1-p)^{\gamma^+})^{1/\gamma^+}}, \tag{2.29}$$

$$\omega^-(p) = \frac{p^{\gamma^-}}{(p^{\gamma^-} + (1-p)^{\gamma^-})^{1/\gamma^-}}. \tag{2.30}$$

As shown in (2.27) and (2.28) the decision weights under CPT are defined based on cumulative rather than individual probabilities. Indeed, in the positive prospect, $\sum_{j=i}^{n} p_i$ is the probability that a certain outcome is at least as good as the obtained outcome, x_i; while $\sum_{j=i+1}^{n} p_i$ is the probability that an outcome is strictly better than x_i. Moreover, in the negative prospect, $\sum_{j=-m}^{i} p_i$ is the probability that an outcome is at least as bad as the obtained outcome, x_i; while $\sum_{j=-m}^{i-1} p_i$ is the probability that the outcome is strictly worse than x_i.

Prospect Theory for CPS Security Games

In CPS security games, the preferences and behavior of the players must be accurately modeled and incorporated in the game formulation. In fact, CPS security settings incorporate various uncertainties such as: i) uncertainty about the system due to its complexity, ii) uncertainty about the opponent types and possible strategies, and iii) uncertainty pertaining to the probability of occurrence of natural events, natural failures, or likelihood of attacks, among others. As such, attackers and defenders make strategic decisions under uncertainty and high risk which can lead to their deviation from the fully rational behavior. To this end, prospect theory provides established quantitative tools to model such subjective behavior. As such, we propose the incorporation of the principles of prospect theory in our formulated CPS security games to account for the way in which human agents in CPS security settings make decisions under risk.

In fact, due to the uncertainty that the attackers and defenders face while interacting in a CPS security setting, each of them will have its own perception of what the other can do. Indeed, as shown in [153] through working with pen testers, adversaries carefully study their target and anticipate defensive actions that could be taken. The weighting framework of prospect theory can, hence, include this subjective perception of the players in a game-theoretic model for CPS security. Framing, on the other hand, reflects a subjective perception of an attacker's or defender's own utility. In fact, different attackers can have different reference points to assess the damage that they can cause to the system. For example, an individual attacker manipulating some meter readings in its own basement has a different reference point than a state coordinated attack on a national power grid. The same logic also applies for defenders. This framing process can also capture whether an attacker or defender is risk seeking or risk averse and incorporates their attitudes towards taking risks in the security analyses.

In this respect, prospect theory provides the necessary mathematical tools to model a wider variety of strategic behaviors that the players involved in CPSs security settings may admit. In fact, the incorporation of prospect theory in games provides a more general analysis as compared to restricting the players, as is the case in classical game theory, to the fully rational behavior (or equivalently to follow the tenets of expected utility theory). Mathematically, the subjective nonlinear valuation and weighting, proposed by PT, significantly influences the equilibria of the associated games and can affect their existence, properties, and efficiency which entails various technical challenges in terms of the derivation and analysis of these equilibria.

A number of recent research works have used classical prospect-theoretic tools for applications in smart grids [164, 165], wireless communication [166, 167], and security [168–170]. For instance, the work in [168] and [169] proposed a prospect-theoretic model for the analysis of advanced persistent threats targeting could storage systems. Prospect theory was used to model the subjective perception that the attacker and defender have on one another. The work in [170] proposes a prospect-theoretic model to study jamming in cognitive radio networks. Hence, even though prospect theory has been applied in few instances for cyber security analyses, the use of this theory, and specially cumulative prospect theory, as a fundamental and holistic tool for CPS security analyses is still largely unexplored.

Prospect theory, hence, enables the modeling and prediction of decision makers' subjective perception of outcomes and of their likelihood. However, PT does not capture the disparate cognitive and computational skills that each player, attacker or defender, might have and the players' subjective beliefs about their skills as compared to their opponents. This cognitive hierarchy and subjective perception of skills is captured using cognitive hierarchy theory which is introduced and detailed next.

2.5.2 Cognitive Hierarchy Theory

In conflicting and competitive situations, an entity incorporates predictions of what competitors would do, how would they think and act, in their decision making frameworks. This same decision process also applies in CPS security situations in which defenders and attackers aim at investigating the nature, behavior, and skills of their opponents before implementing their attack or defense strategies. In fact, as stated in [153], adversaries carry out a reconnaissance phase in which they deeply learn about the system they are targeting, including its operator, before launching their attack. Moreover, in CPS security applications, attackers and defenders might have different skill levels. These skills can reflect actual technical attack/defense skills or they can reflect a level of knowledge of the system being attacked. In fact, many recent reports claim that worms can infiltrate in systems to learn about that system in preparation to issue future attacks [33, 47]. As such, understanding, capturing, and modeling such skills levels in CPS security analyses generates fundamental insights towards understanding attackers' behavior which enables deriving accurate and efficient defense strategies.

To this end, *cognitive hierarchy theory* (CHT) [150] is a behavioral game-theoretic framework, which enables differentiating players based on their skill levels and reasoning abilities. In this framework, each player considers its own strategy to be the most sophisticated and presumes a ranking of the sophistication level of other players' strategies [150]. In fact, under cognitive hierarchy theory, a player assumes k potential levels of thinking (i.e. levels of sophistication) and regards herself to be at the highest step, i.e. step k. Then, this player anticipates the fraction of players corresponding to each of the lower steps. Hence, each player assumes having the most sophisticated strategy (level k) and presumes a probability distribution over the skill levels of its opponents; these skill levels range from 0 to $k-1$. This player will then play a best response strategy against the set of opponents based on the associated perceived skills levels. In this regard, each player chooses its action based on its belief about the skill levels of its opponents. However, such beliefs can be distorted which can be due, for example, to overconfidence based on which an attacker (defender) assumes that its attack (defense) strategy is the most sophisticated strategy and considers that the opponent can never guess this strategy and can never properly respond to it.

Cognitive hierarchy can be highly beneficial in modeling the security interaction between attackers and defenders, in CPS security applications. In fact, in certain security scenarios, the defender (being a system operator) may have the highest knowledge of the system and can rank possible attackers based on their possible level of knowledge about the system and its security. Hence, the defender can design its security strategy based on its perception of the fraction of attackers at each level of knowledge. In addition, an attacker can anticipate – based on a performed reconnaissance phase – the way in which the defender would design its defense strategy, based on which a more sophisticated attack strategy could be devised. The use of cognitive hierarchy for the analysis of CPS security situations is still unexplored. As such, our work provides a novel incorporation of such beliefs over skills levels and cognitive skills in security analyses.

Using cognitive hierarchy theory allows, hence, capturing the disparate skill levels that the attacker(s) and defender(s) may possess and their subjective perceptions of such skill levels. Here, PT and CHT both assume that the defender and attacker has a certain knowledge level about the defender (which they subjectively perceive) which they can exploit in the design of their, respective, defense and attack strategies. However, in a number of practical CPS analyses, even such a minimal knowledge might not be available to the attacker or defender due to the confidentiality involved. Hence, next, a mathematical framework modeling human behavior under such scarcity of information is introduced and investigated.

2.5.3 Satisfaction Equilibrium

Due to the high level of confidentiality involved in CPS security settings, an attacker might not be able to acquire the needed information about the system and about the potentially implemented defense policies in order to accordingly choose its optimal attack strategy; the attack strategy which maximizes, for example, the inflicted damage on the system. Similarly, the defender might not have the means to learn about the attackers, their presence, and their potential attack strategies in order to be able to choose the defense strategy which minimizes, for example, the deviations from the standard operating state which can be caused by an attack. Hence, the attacker and defender may not always aim at choosing a best response strategy since the needed knowledge for the derivation of such best response strategy may not be available or even obtainable (for example, an attacker or defender may not have enough knowledge about the strategy spaces of the opponents or even about their existence).

Under such information scarcity, it is reasonable for a defender to aim at meeting a certain performance requirement rather than at maximizing performance or minimizing damage; since such optimal solutions may not be obtainable. As such, in CPS security analyses, if the achieved CPS performance is within the desired range of a certain operation requirement, the defense strategy can be considered to have achieved the defender's goal. Similarly, an attack that causes a certain guaranteed minimum damage to the system, can be considered to meet the attacker's goal. In other words, if an attack strategy induces a level of degradation in system performance which surpasses a certain threshold, such attack strategy can be considered to have met the attacker's goal.

Such targeted goal-oriented security behavior can be captured using the tools of *satisfaction equilibrium* [151, 152]. In the satisfaction equilibrium framework, rather than having an objective function, a player would admit a satisfaction function which indicates if the chosen strategy meets the performance requirement. Hence, in a CPS security setting, the defender's satisfaction function indicates whether the chosen defense strategy guarantees that the deviation from the normal operating state, or potential caused damage to the system, is below a certain required limit. As for the attacker, its satisfaction function would indicate whether an attack strategy guarantees that the inflicted damage to the system is above a certain required threshold. In this respect, assuming that the defender requires the deviation from the nominal operating state, $r^d(.)$, to be below a threshold ζ^d, for an attacker strategy s^a and defender strategy s^d, the satisfaction function $h^d(.)$ would hence take the following form:

$$h^d(s^a, s^d) = \begin{cases} 1, & \text{if } h^d(s^a, s^d) \leq \zeta^d \\ 0, & \text{otherwise.} \end{cases}$$

As such, when a player's – attacker or defender – requirement is met, this player is satisfied and has no incentive to deviate from its chosen strategy. Hence, the game has reached a *satisfaction equilibrium* which is formally defined as follows:

Definition 4. *For an attack strategy $s^a \in \mathcal{S}^A$ and defense strategy $s^d \in \mathcal{S}^D$, and denoting the satisfaction functions of the attacker and defender, respectively, by $h^a(.)$ and $h^d(.)$, these attack* *and defense strategy are at a satisfaction equilibrium if:*

$$h^a(s^a, s^d) = 1 \textit{ and } h^d(s^a, s^d) = 1. \tag{2.31}$$

The concept of satisfaction equilibrium have been implemented in wireless communication [171–173]. For instance, the works in [171] and [172] used a satisfaction equilibrium framework for quality of service provisioning in self-configuring networks in which radio devices aim at meeting a minimum quality of service requirement. In addition, the work in [173] proposed a framework based on satisfaction equilibrium for distributed power allocation while meeting a minimum signal to interference plus noise ratio. However, incorporating the concepts of satisfaction equilibrium in security analyses remains unexplored.

The mathematical concept of satisfaction equilibrium enables the modeling of a unique trait of the bounded rationality of human behavior in security games. Satisfaction equilibrium, in fact, enables capturing and modeling the decision making processes of the attackers and defenders when faced with scarce information about the system or about one another; a condition whose occurrence is highly likely in confidential CPS security situations. Hence, our work presents a novel incorporation of this concept in the analysis of security situations.

Chapter 3

Graph-Theoretic Framework for Unified Analysis of Observability and Data Injection Attacks in the Smart Grid

3.1 Introduction

With the integration of information and communication technologies in power systems, new security concerns have emerged due to the potential exploitation of this cyber layer to infiltrate and compromise the underlying physical system. Indeed, in recent years, various studies have focused on analyzing the security of emerging cyber-physical power systems [39, 74, 75, 91, 120, 174, 175] and the effect of potential cyber attacks on the various operational components of the grid, ranging from power system state estimation [75], to electricity markets [74, 174, 175] and power system dynamics and control [91, 120].

Such attacks can become more pronounced when they target critical power system functions such as state estimation. In this regard, the power system state estimation is an integral smart grid process in which system-wide measurements are collected and processed to estimate the global state of operation of a power system [176]. State estimation is the basis for various grid operational decisions such as congestion management, economic dispatch, contingency analysis, and electricity pricing [122]. As a result, the critical importance of state estimation to the sustainable operation of the grid makes it a primary target of possible cyber-physical attacks [39]. Such attacks may target the availability of the collected measurements as well as their integrity.

In this respect, intercepting a subset of the collected measurement data using availability attacks (such as denial-of-service attacks) can render the power system unobservable (i.e. not fully observable), a state in which the collected measurements do not provide enough independent equations to estimate the states. Such cyber-physical attacks, to which we refer as *observability attacks* hereinafter, will make the operator partially oblivious to the real state of operation of the system, leading to uninformed operational decisions. Beyond observability attacks, *data injection attacks* (DIAs) have emerged as a malicious type of integrity attacks which aim at manipulating the collected state estimation data, leading to inaccurate state estimation outcomes that result in misinformed operational decisions with potentially detrimental consequences [39, 75, 174]. As shown in [75], such DIAs can stealthily target the power system state estimation process – manipulating the collected measurements and altering the state estimation outcome – while being undetectable by the system operator using traditional bad data detection mechanisms. Hence, due to their potential danger to system operation, such stealthy data injection attacks (SDIAs) and observability attacks have been the focus of various recent research efforts [29, 30, 177–181].

3.1.1 Related Works

In this regard, the works in [177] and [178] focused on computing a security set which comprises the minimum set of measurements which must be attacked in addition to a certain specific measurement in order to make the system unobservable. Moreover, the work in [30] focused on computing the cardinality of the smallest set of meters which when attacked render the system unobservable. The authors in [179–181] extended such observability problems to studying SDIAs. In this regard, these works focused on characterizing the sparsest stealthy attack containing a certain specific measurement. In addition, the work in [29] focused on characterizing a set of measurements to defend so that no attack which concurrently manipulates a set of meters whose cardinality is below a certain threshold can be stealthy. Hence, this latter analysis focuses on the defense against resource-limited attackers. As such, these works have focused on formulating and studying mathematical problems whose solutions enable anticipating potential sophisticated attacks – which constitutes a first step towards deriving corresponding defense mechanisms – and designing optimal defense strategies to thwart such attacks and mitigate their potential effect.

The computational complexity of these problems [29, 30, 177–181] has led to limiting the analysis of their solutions to special, often approximated, cases or required the use of heuristics and relaxation techniques which led to suboptimal solutions. For example, for characterizing the sparsest observability attacks containing a specific measurement, the work in [177] focused on the special case of measurement sets of low cardinality while the work in [178] derived an approximate solution that is based on the solution of a min-cut problem. In addition, with regard to the analysis of the sparsest SDIAs containing a certain measurement [179–181], the work in [179] focused on deriving an upper-bound on this stealthy attack set while the work in [180] used min-cut relaxation techniques to approximate the sought solution. Moreover, the work in [181] proposed a heuristic algorithm which can approximate the solution of the studied problem while an exact solution was found for the special case in which power flows over all the transmission lines and power injections into and out of every bus are assumed to be measured. To defend against a resource-limited data injection attacker, the authors in [29] used an l_1 relaxation method for characterizing the set of meters to defend to thwart SDIAs launched by attackers whose attack space is limited by a certain cardinality threshold. Other related security works are also found in [78, 182–186].

Therefore, this rich body of literature [29, 30, 78, 177–186] employs heuristics and approximation techniques to numerically approximate the solutions to these fundamental observability attacks and SDIA problems rather than analytically characterizing their solutions. As such, there is a need for an analytical framework which allows modeling and studying such data availability and integrity attacks and enables an analytical characterization of mathematical solutions to such widely-studied security problems. In addition, the fact that these works [29, 30, 177–181] studied correlated problems but from different perspectives highlights the need for a unified framework using which solutions to such correlated observability attacks and SDIA problems can be studied and derived.

3.1.2 Contributions

The main contribution of this chapter is a novel unified graph-theoretic framework that enables a global detailed modeling and understanding of observability attacks and SDIAs. As a result, this framework provides a unified tool for analyzing various widely-studied observability attacks and SDIA problems such as those studied in [29, 30, 177–181], among others. In addition, the proposed framework enables the characterization of exact analytical solutions to such security problems, instead of relying on numerical approximations or heuristics. This will enable a fundamental analysis and modeling of potential attack strategies and the derivation of defense strategies which can thwart and mitigate the effect of such observability attacks and SDIAs. In this regard, our proposed framework is based on a shift in the modeling of observability attacks and SDIAs from a linear algebra frame of reference to a graph-theoretic perspective. As a result, based on this proposed framework, such attacks can be modeled and analyzed by requiring only power system topological data, namely, the power system 1-line diagram and the location of deployed measurement units without the need for neither line parameters data nor the exact knowledge of power flow levels throughout the system.

To build the proposed framework, we first begin by introducing a graph-theoretic basis of observability attacks and, then, we prove that SDIAs are a special case of such observability attacks. In this respect, we introduce an algorithm providing a step-by-step approach for building *critical sets*, a set of measurements – containing a certain specific measurement – which, when removed, render the system unobservable. We then prove that for a DIA to be stealthy, the attacked measurements should strictly result in leaving critical sets unmatched as part of a maximum matching over an introduced bipartite graph. As such, a graph-theoretic model of SDIAs is then introduced based on which the solutions to various well-studied SDIA problems are analytically characterized. In particular, *we show that our developed framework can be readily applied to characterize analytical solutions to various SDIA problems* such as, but not limited to: 1) Finding the stealthy attack of lowest cardinality, 2) Finding the stealthy attack of lowest cardinality, including a specific measurement, 3) Finding a set of measurements which when defended can thwart all possible stealthy attacks, and 4) Finding a set of measurements to defend against a resource-limited attacker, among others. A case study using the IEEE 14-bus system, with 17 distributed measurement units, is considered throughout the chapter to showcase the developed analytical concepts. In this case study, we characterize the sparsest SDIAs which can successfully target the system and show that the cardinality of such attacks is equal to 2. In addition, the performed case analysis on the IEEE 14-bus system shows that defending a characterized set of 13 (out of 17) measurements is necessary to prevent any successful SDIAs, while defending only 3 measurements is enough to thwart any stealthy attack of cardinality lower than 3. This, hence, enables the defender to build on some acquired knowledge regarding the resources of the adversaries to derive a corresponding defense strategy.

In this respect, the derived analytical results and presented case study showcase the importance of the proposed framework for studying various correlated observability attacks and SDIA problems and pave the way for further analyzing additional emerging problems in that field.

The rest of the chapter is organized as follows. Section 3.2 introduces state estimation and power system observability. Section 3.3 introduces our proposed graph-theoretic foundation of observability attacks and shows its impact on modeling and analyzing such data availability attacks. Section 3.4 introduces the proposed graph-theoretic framework for modeling SDIAs, as well as studies and solves various well-studied SDIA problems. Section 3.5 concludes the chapter and provides an outlook detailing the impact of the proposed framework on studying future observability and data injection attacks.

3.2 State Estimation and Observability

We next provide an overview of state estimation and of the algebraic and topological concepts of observability in power systems. This overview provides background material which is useful for the analysis that follows.

3.2.1 State Estimation Process

Consider a power system state estimation process which uses various measurements collected from across the system to estimate the voltage magnitudes and phase angles at every bus in the system, known as the system states [176]. Let $\boldsymbol{z} \in \mathbb{R}^m$ (m being the number of measurements) be the vector of collected measurements, which includes power flow levels (real and reactive) over transmission lines, power (real and reactive) injected in or withdrawn from certain buses, as well as bus voltage magnitudes. In addition, let $\boldsymbol{x} \in \mathbb{R}^n$ be the vector of system states. The relationship between the measurements and the states directly follows from the linearized power flow equations [176]:

$$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{e}, \tag{3.1}$$

where $\boldsymbol{H} \in \mathbb{R}^{m \times n}$ is the measurement Jacobian matrix and $\boldsymbol{e} \in \mathbb{R}^m$ is the vector of random errors that typically follows a Gaussian distribution, $N(0, \boldsymbol{R})$, where $\boldsymbol{R}$ is positive definite. Here $m \geq n$, that is the dimension of $\boldsymbol{x}$ cannot be larger than the dimension of the measurement vector,

$\boldsymbol{z}$. Further, we assume that $\boldsymbol{H}$ is a full-rank matrix. Using a maximum-likelihood estimator – a weighted least squares estimator (WLS) for a Gaussian error vector $\boldsymbol{e}$ – an estimate of the states, $\hat{\boldsymbol{x}}$, will be:

$$\hat{\boldsymbol{x}} = (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{z}. \tag{3.2}$$

This estimate of all the states provides visibility of the steady-state operating conditions of the system, based on which various operational decisions are performed [176].

3.2.2 Power System Observability

The observability of the power system consists of the ability to uniquely determine its states based on the collected set of measurements [176]. Observability, hence, requires the collected measurements to provide enough independent equations to allow the estimation of the state vector, $\boldsymbol{x}$. In this respect, the power system is *observable*[1] if and only if the measurement matrix $\boldsymbol{H}$ is of full column rank [176], which was our initial assumption. This is known as *algebraic observability*. Due to the $P-\theta$, $Q-V$ decoupling[2] in power systems [122], the observability analysis can be decoupled by separately studying the observability of voltage phase angles, using real power measurements, and the observability of voltage magnitudes, based on reactive power measurements. Since the two analyses are identical, we focus here on phase angle observability. To this end, we consider $\boldsymbol{z} \in \mathbb{R}^m$ to be a vector of real power measurements (bus injections and line flows), and the state vector $\boldsymbol{x} \in [-\pi, \pi]^n$ to be the vector of voltage phase angles (in radians). Here, $n = N-1$ for a power system with N buses given that the phase angle of the reference bus is fixed and is taken to be the reference with respect to which all other phase angles are calculated [176].

An alternative measure of observability, which is equivalent to algebraic observability, is proposed in [187] and uses graph-theoretic techniques to introduce the concept of *topological observability*. In this regard, let the power system 1-line diagram be represented as a graph $\mathcal{G}(\mathcal{N}, \mathcal{L})$ in which the set of vertices $\mathcal{N}$, $|\mathcal{N}| = N$, represents the set of buses of the power system while the set of branches $\mathcal{L}$, $|\mathcal{L}| = L$, represents the set of lines. One key result that was shown in [187] and that will be of relevance to our work is the following:

Remark 1. *A power system is* observable *if and only if the set of measurements can be assigned to the edges of the power system graph, following a set of assignment rules, in a way to form a* spanning tree *over this graph.*

In this respect, let $\mathcal{M}$ be the set of measurements and let $f(.)$: $\mathcal{M} \to \mathcal{L}$ be an assignment function defined as follows.

[1] Otherwise, when this observability condition is not met, the power system is dubbed *unobservable*.

[2] P denotes real power, θ denotes voltage phase angles, Q denotes reactive power, and V denotes voltage magnitudes.

Definition 5. *$f(.)$: $\mathcal{M} \rightarrow \mathcal{L}$ is a* measurement assignment function *which assigns measurements in $\mathcal{M}$ to lines in $\mathcal{L}$ following a set of assignment rules defined as [187]:*

1. *If $l_1, l_2 \in \mathcal{L}$ and $l_1 \neq l_2$, then $f^{-1}(l_1) \neq f^{-1}(l_2)$. In other words, a measurement cannot be simultaneously assigned to two different lines.*

2. *If m is a measurement over a transmission line l, then m can only be assigned to l.*

3. *If m is an injection measurement over bus $\eta \in \mathcal{N}$, then m can only be assigned to an unmeasured line l that is incident to η.*

If such a measurement assignment that yields a spanning tree over the power network $\mathcal{G}$ can be found, the power system will be observable (and vice versa). Fig. 3.1 shows an example of measurement assignments over the IEEE 14-bus system. This figure shows the tree branches (marked in solid red lines) to which measurement where assigned as part of the measurement assignment function. The measurements that were assigned to each one of these branches are identified using dashed arrow lines originating from the assigned measurement and pointing to the line to which this measurement is assigned. This tree is formed of branches $\{1, 2, 4, 6, 8, 9, 10, 12, 13, 15, 16, 17, 19\}$ and spans the whole vertex set $\mathcal{N}$ of the power system graph $\mathcal{G}$, and hence, is a spanning tree. As a result, since this measurement assignment yields a spanning tree, then the available set of measurements renders the system observable.

Various algorithms of low complexity have been proposed to find and build such a spanning tree [187–189]. In this regard, the work in [187] proposes an algorithm to find a spanning tree over $\mathcal{G}$, which will be used in some of the derivations in the following sections. This algorithm starts by processing flow measurements by assigning each flow measurement to its corresponding branch to form disjoint tree components. Then, injection measurements are assigned to lines in a way to connect these tree components to form one spanning tree. Here, we highlight one type of injection measurements, namely, *boundary injections*, which will play a crucial role in our derivations.

Definition 6. *A boundary injection is an injection measurement over a bus incident to lines whose flow is measured and lines whose flow is not measured [187].*

Boundary injections play a major role in connecting these tree components. Indeed, for a bus which is not incident to a measured line to be connected to the spanning tree, it has to be reachable from a boundary injection through a series of measurement assignments [187]. As such, boundary injections are considered to be sources and unmeasured buses are considered to be sinks which must be connected to these sources following the set of measurement assignment rules.

We next build on the foundation of topological observability to present a graph-theoretic framework for modeling and studying the security of the smart grid facing observability attacks and SDIAs. This framework is based on our proposed concepts of critical sets and observability sets, which we define and derive in the next section.

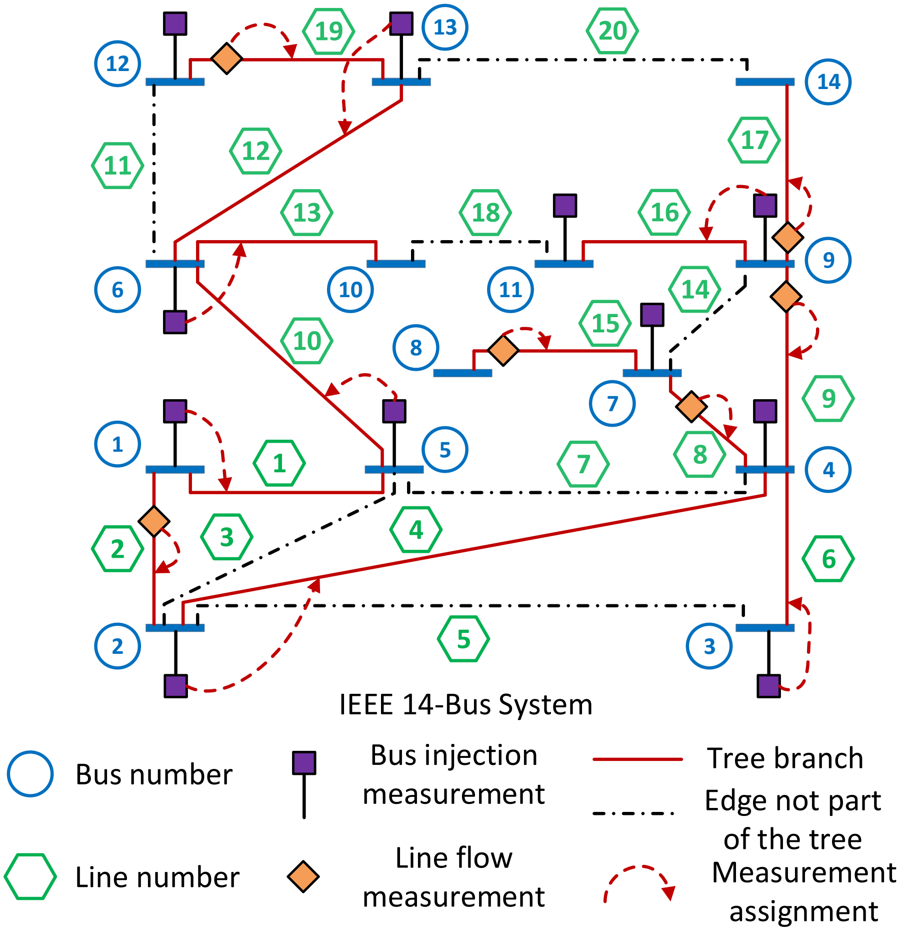

Figure 3.1: IEEE 14-bus system with measurement assignment.

3.3 Observability Attacks

The sustainable and efficient operation of the power system requires an accurate observability of all its states [176]. Security attacks that target this observability can cause a limited (or partial) monitoring ability for the operator over the power system which can lead to incorrect operational decisions. Hence, studying and modeling attacks which can target the full observability of the system is indispensable for the sustainable operation of the grid. In this respect, we define a cyber-physical attack, dubbed *observability attack*, that consists of launching availability attacks against a set of measurements to make the system unobservable. We next study this type of attacks by introducing and characterizing what we define as critical sets and observability sets and prove that the well-studied stealthy data injection attack is a subset of our defined observability attacks. This latter finding will provide us with a unified set of tools to solve various widely-studied SDIA problems.

3.3.1 Critical Sets

Understanding and modeling observability attacks requires an in-depth understanding of the effect of the loss of any bundle of measurements on the observability of the system. In this regard, we next introduce a structured method for identifying, for each measurement m, the set of additional measurements including m (denoted as the critical set of m), which when removed renders the system unobservable. To this end, we first characterize the set of potential measurements to be investigated, for each measurement m, and then provide the necessary discussion and introduce the underlying method for characterizing the critical set of m. In this process, we show that characterizing such a critical set requires solving a maximum matching problem over a developed bipartite graph. Then, a detailed algorithm is introduced to provide a step-by-step method for characterizing such critical sets.

Let $\mathcal{M}^C \subseteq \mathcal{M}$ be the set of measurements which are part of the assignment function, i.e., the measurements assigned to form a spanning tree over the power network. We refer to measurements not part of $\mathcal{M}^C$ as *unassigned measurements*. Such unassigned measurements are, hence, by definition redundant measurements. We consider that the system is originally observable. Hence, such a spanning tree and its corresponding set of assigned measurements exist. We also let $\mathcal{T}(\mathcal{N}, \mathcal{B})$ be the spanning tree whose set of branches are captured by the set $\mathcal{B} \subseteq \mathcal{L}$. $\mathcal{B}$, in essence, represents the set of lines to which measurements were assigned as part of the assignment function $f(.)$. For example, as previously mentioned, in Fig. 3.1, the branches of the spanning tree are represented in solid red lines.

Consider an assigned measurement $m \in \mathcal{M}^C$. Since m is assigned, its removal will split the tree $\mathcal{T}$ into two spanning trees $\mathcal{T}_1^m(\mathcal{N}_1^m, \mathcal{B}_1^m)$ and $\mathcal{T}_2^m(\mathcal{N}_2^m, \mathcal{B}_2^m)$ spanning subgraphs $\mathcal{G}_1^m$ and $\mathcal{G}_2^m$, respectively, such that $\mathcal{N} = \mathcal{N}_1^m \cup \mathcal{N}_2^m$ and $\mathcal{B} = \mathcal{B}_1^m \cup \mathcal{B}_2^m \cup \{f(m)\}$. Fig. 3.2 provides an illustrative example of the two spanning trees created by the deletion of the flow measurement over line 2 (we denote this flow measurement by F_2). Fig. 3.2 represents the same system shown in Fig. 3.1 and will be used throughout this work to provide a practical example of the defined concepts and analytical derivations.

To investigate observability, we define a set of measurements for each measurement $m \in \mathcal{M}^C$, which we refer as the *critical set* of m and we denote by $\mathcal{C}^m$, as follows:

Definition 7. *For a measurement $m \in \mathcal{M}^C$, the* critical set *of m, denoted as $\mathcal{C}^m \subseteq \mathcal{M}$, is a set of measurements which can be used to reconnect $\mathcal{T}_1^m$ and $\mathcal{T}_2^m$ when m is deleted.*

Consequently, when m is removed, any $m' \in \mathcal{C}^m$ can be used to reconnect $\mathcal{T}_1^m$ and $\mathcal{T}_2^m$. For convenience, we consider m to be part of its own critical set $\mathcal{C}^m$. Let $\mathcal{L}^m$ be the set of lines connecting a bus in $\mathcal{T}_1^m$ to a bus in $\mathcal{T}_2^m$. In addition, let $\mathcal{N}_{1,2}^m \subseteq \mathcal{N}_1^m$ and $\mathcal{N}_{2,1}^m \subseteq \mathcal{N}_2^m$ be the set of nodes in, respectively, $\mathcal{N}_1^m$ and $\mathcal{N}_2^m$ which are connected to a node in, respectively, $\mathcal{N}_2^m$ and $\mathcal{N}_1^m$. An example of these notations is provided in Fig. 3.2. $\mathcal{L}^m$ is, hence, formally defined as:

$$\mathcal{L}^m = \{l \in \mathcal{L} \,|\, l = (\eta_1, \eta_2), \eta_1 \in \mathcal{N}_{1,2}^m, \eta_2 \in \mathcal{N}_{2,1}^m\}. \tag{3.3}$$

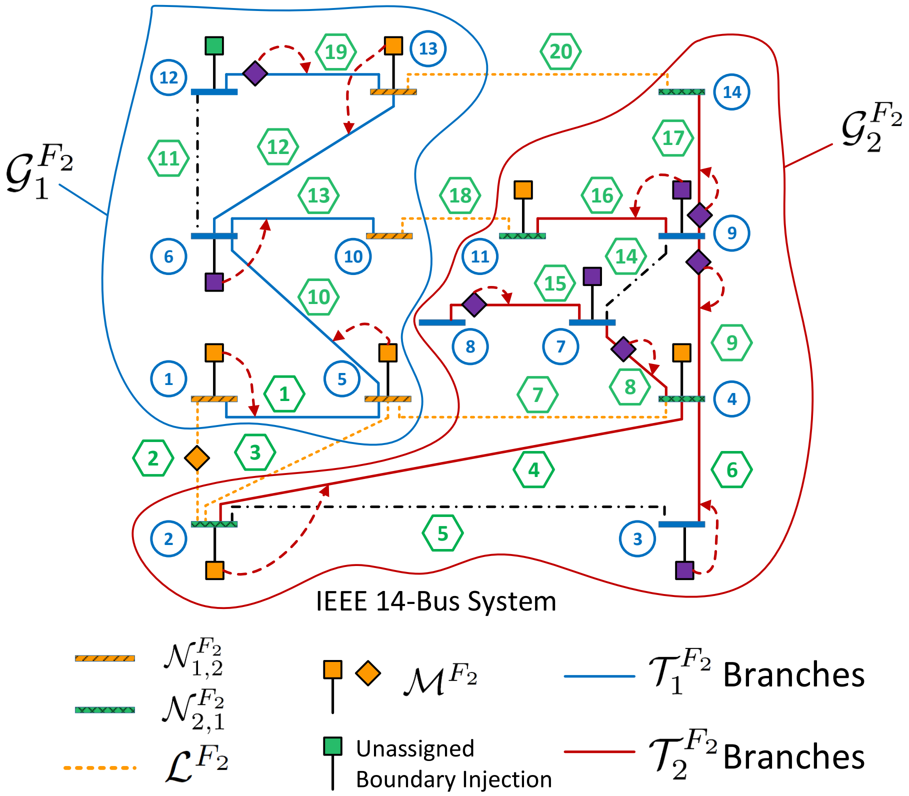

Figure 3.2: Critical set of the flow measurement over line 2, F_2, of the IEEE 14-bus system.

We next introduce the set of rules that should be followed to build the critical set of a certain measurement, following which, we provide a structured algorithm for building such critical sets.

Based on the measurement assignment rules described in Section 3.2.2, a necessary condition for a measurement m' to be in $\mathcal{C}^m$ is for it to be either a line flow measurement over a line $l \in \mathcal{L}^m$ or an injection measurement over a bus $\eta \in \{\mathcal{N}_{1,2}^m \cup \mathcal{N}_{2,1}^m\}$. We denote this set of measurements, for a measurement m, by $\mathcal{M}^m$. Here, for convenience[3], we consider $\mathcal{M}^m$ not to include measurement m. The measurements in $\mathcal{M}^m$ are the only measurements which can be assigned to a line in $\mathcal{L}^m$, and hence, are the only measurements with the potential of reconnecting $\mathcal{T}_1^m$ and $\mathcal{T}_2^m$. An example of the set $\mathcal{M}^m$ for $m := F_2$ is shown in Fig. 3.2.

The measurements in $\mathcal{M}^m$ can be split into three different categories: 1) flow measurements over lines in $\mathcal{L}^m$, which we denote as $\mathcal{M}_F^m$,[4] 2) unassigned injection measurements over buses in $\mathcal{N}_{1,2}^m \cup$

[3] Given that m is always considered to be part of its critical set $\mathcal{C}^m$, m is always added to $\mathcal{C}^m$ after investigating the measurements in $\mathcal{M}^m$.

[4] Such measurements are unassigned measurements. In fact, if m is a line measurement, lines in $\mathcal{L}^m$ would form a loop with $f(m)$ and hence cannot be part of the original spanning tree. Moreover, if m is an injection measurement, $\mathcal{M}_F^m$ would be an empty set since, otherwise, based on the spanning tree building method described in Section 3.2.2 and originally presented in [187], one of the measurements in $\mathcal{M}_F^m$ would have been assigned to a line in $\mathcal{L}^m$, and m would not have been part of $\mathcal{M}^C$. As a result, measurements in $\mathcal{M}_F^m$ are redundant.

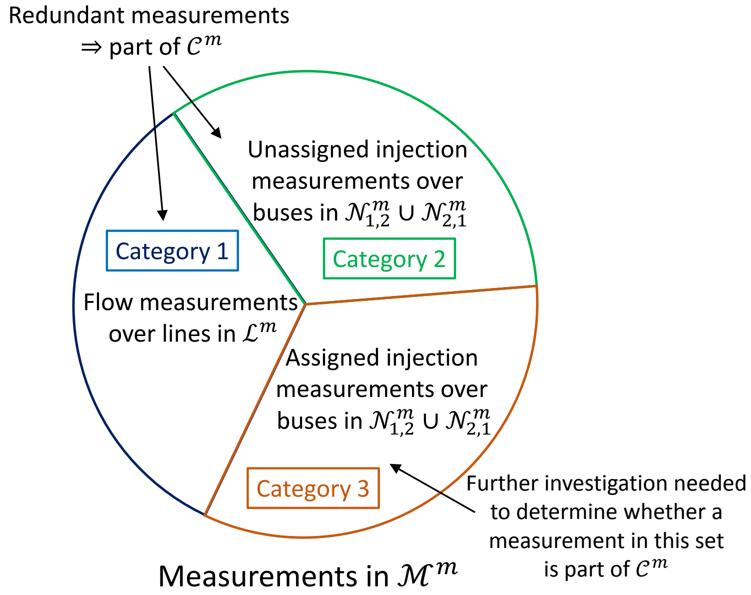
Redundant measurements
⇒ part of $\mathcal{C}^m$
Unassigned injection measurements over buses in $\mathcal{N}_{1,2}^m \cup \mathcal{N}_{2,1}^m$
Category 1
Category 2
Flow measurements over lines in $\mathcal{L}^m$
Assigned injection measurements over buses in $\mathcal{N}_{1,2}^m \cup \mathcal{N}_{2,1}^m$
Category 3
Further investigation needed to determine whether a measurement in this set is part of $\mathcal{C}^m$
Measurements in $\mathcal{M}^m$

Figure 3.3: The three categories of measurements in $\mathcal{M}^m$.

$\mathcal{N}_{2,1}^m$, and 3) assigned injection measurements over buses in $\mathcal{N}_{1,2}^m \cup \mathcal{N}_{2,1}^m$, i.e., measurements in $\mathcal{M}^m \cap \mathcal{M}^C$. A representation of this partition is shown in Fig. 3.3

In this regard, not all measurements in $\mathcal{M}^m$ are necessarily in $\mathcal{C}^m$. In fact, for $m' \in \mathcal{M}^m$ to be in $\mathcal{C}^m$, it must be redundant. Namely, m' must be assignable to a line in $\mathcal{L}^m$ to reconnect $\mathcal{T}_1^m$ and $\mathcal{T}_2^m$, without causing any disconnections within either $\mathcal{T}_1^m$ or $\mathcal{T}_2^m$. In this respect, if $m' \in \mathcal{M}^m$ is unassigned, i.e $m' \notin \mathcal{M}^C$, m' would be part of $\mathcal{C}^m$. For example, consider the injection measurement over bus 4 in Fig. 3.2, which we denote by I_4. Measurement I_4 is in $\mathcal{M}^{F_2}$ and is a redundant measurement since it was not assigned to any line as part of the original tree $\mathcal{T}$. Hence, when F_2 is removed, I_4 can be assigned to line 7 to reconnect $\mathcal{T}_1^{F_2}$ and $\mathcal{T}_2^{F_2}$ without causing any disconnection in $\mathcal{T}_2^{F_2}$, in which it is located. Hence, $I_4 \in \mathcal{C}^{F_2}$.

As a result, since the measurements in $\mathcal{M}_F^m$ and the unassigned injection measurements over buses in $\mathcal{N}_{1,2}^m \cup \mathcal{N}_{2,1}^m$ (which are the first two categories of measurements in $\mathcal{M}^m$, as shown in Fig. 3.3) are redundant, they are part of $\mathcal{C}^m$. Now, when $m' \in \mathcal{M}^m$ is assigned as part of the original assignment function, i.e., $m' \in \mathcal{M}^m \cap \mathcal{M}^C$ (which corresponds to the third category of measurements in $\mathcal{M}^m$, indicated in Fig. 3.3), then additional investigation is needed to determine whether m' is redundant, and hence, whether it can be considered in $\mathcal{C}^m$.

In this regard, consider that $m' \in \mathcal{M}^m$ is assigned to a line l', that is $f(m') = l' \in \mathcal{B}$. If m' is to be reassigned to a line $l \in \mathcal{L}^m$, $\mathcal{T}_1^m$ and $\mathcal{T}_2^m$ will be reconnected, but since m' was originally assigned as part of the original tree, another portion of the tree gets disconnected by this reassignment of m' to l instead of l'. Hence, m' can be part of $\mathcal{C}^m$ if another measurement can be used to reconnect the subgraph which was disconnected by the reassignment of m' from l' to l. For example, consider the injection measurement over bus 13 in Fig. 3.2, which we denote by I_{13}. I_{13} has been assigned to line 12 as part of the original spanning tree. Hence, if I_{13} is assigned to line 20 to reconnect $\mathcal{T}_1^{F_2}$ and $\mathcal{T}_2^{F_2}$ after measurement F_2 is removed, it cannot be assigned to line 12 anymore which will split $\mathcal{T}_1^{F_2}$ into two subtrees, one formed by buses $\{12,\ 13\}$ and line 19 and the other subtree composed of buses $\{6,\ 10,\ 1,\ 5\}$ and lines $\{13,\ 10,\ 1\}$. We denote these two subtrees as $\mathcal{T}_{1,1}^{F_2}$ and $\mathcal{T}_{1,2}^{F_2}$, respectively. In this respect, if another measurement can replace I_{13} in reconnecting $\mathcal{T}_{1,1}^{F_2}$ and $\mathcal{T}_{1,2}^{F_2}$, then I_{13} can be assigned to line 20 and, hence, should be part of $\mathcal{C}^{F_2}$. To this end, consider the injection measurement over bus 12, denoted by I_{12}, which was not part of the original spanning tree assignment. I_{12} can be assigned to line 11 to reconnect $\mathcal{T}_{1,1}^{F_2}$ and $\mathcal{T}_{1,2}^{F_2}$ in case I_{13} is reassigned to line 20 instead of line 12. Hence, I_{13} is indeed redundant, resulting in $I_{13} \in \mathcal{C}^{F_2}$. To generalize the analysis in this example, we next provide a general discussion of measurements in $\mathcal{M}^m \cap \mathcal{M}^C$ (i.e., the third category of measurements in $\mathcal{M}^m$, shown in Fig. 3.3) which allows determining whether a measurement in this set is part of $\mathcal{C}^m$.

More generally, consider $m' \in \mathcal{M}^m \cap \mathcal{M}^C$ to be a measurement assigned to a branch $l' = f(m')$ in $\mathcal{T}_1^m$, and let $\mathcal{M}_1^m$ be the set of measurements in $\mathcal{G}_1^m$. Reassigning m' to $l \in \mathcal{L}^m$ instead of l', to reconnect $\mathcal{T}_1^m$ and $\mathcal{T}_2^m$, will split $\mathcal{T}_1^m$ into two subtrees $\mathcal{T}_{1,1}^m$ and $\mathcal{T}_{1,2}^m$. These trees, respectively, span subgraphs $\mathcal{G}_{1,1}^m$ and $\mathcal{G}_{1,2}^m$. Let $\mathcal{M}_{1,1}^m$ and $\mathcal{M}_{1,2}^m$ be the sets of measurements in $\mathcal{G}_{1,1}^m$ and $\mathcal{G}_{1,2}^m$. m' can be reassigned to l only if some measurement in $\mathcal{M}_1^m$ can reconnect $\mathcal{T}_{1,1}^m$ and $\mathcal{T}_{1,2}^m$. Hence, this corresponds to finding a measurement assignment that connects the two subtrees $\mathcal{T}_{1,1}^m$ and $\mathcal{T}_{1,2}^m$. As discussed in Section 3.2.2, two subtrees can be interconnected by using a measurement assignment if the processing of an unassigned boundary injection in one of them reaches a node in the other. We denote such unassigned boundary injections as *backup boundary injections*, which we formally define as follows:

Definition 8. *A measurement $m'' \in \mathcal{M}_1^m \setminus \{\mathcal{M}_1^m \cap \mathcal{M}^m\}$ is a* backup boundary injection *for a measurement m', if m'' can be used to reconnect $\mathcal{T}_{1,1}^m$ and $\mathcal{T}_{1,2}^m$ generated by the reassignment of $m' \in \mathcal{M}^m \cap \mathcal{M}^C$ to a line $l \in \mathcal{L}^m$ instead of its original line assignment $f(m') = l'$. The set of all such backup boundary injections for this measurement $m' \in \mathcal{M}^m \cap \mathcal{M}^C$ is referred to as the* backup boundary injection set *of m' and is denoted by $\mathcal{I}_{b-m'}^m$.*

Since the algorithm in [187] is based on connecting subtrees – to build a full spanning tree – by starting from an unassigned boundary injection in a certain subtree (as a source) to reach a node in another subtree (as a sink), this algorithm can be employed to locate a backup boundary injection for a measurement $m' \in \mathcal{M}^m \cap \mathcal{M}^C$. To this end, to find a backup boundary injection of m', we run the algorithm in [187] by starting from an unassigned boundary injection in either $\mathcal{T}_{1,1}^m$ or $\mathcal{T}_{1,2}^m$ and checking whether the algorithm reaches a bus in $\mathcal{T}_{1,2}^m$ or $\mathcal{T}_{1,1}^m$, respectively. As such, using the spanning tree building algorithm provided in [187, Fig. 1], one can identify the backup boundary injections for each injection measurement in $m' \in \mathcal{M}^m \cap \mathcal{M}^C$. Here, we note that a backup boundary injection cannot be an injection measurement in $\mathcal{M}^m$, since if $m'' \in \mathcal{M}^m$ and m'' is unassigned, m'' will itself be part of $\mathcal{C}^m$, as previously discussed. For example, consider the injection measurements on buses 2 and 4 of Fig. 3.2, denoted by I_2 and I_4, respectively. I_2 is an assigned injection measurement in $\mathcal{M}^{F_2}$. I_2 can be assigned to line 3 instead of line 4 to reconnect $\mathcal{T}_1^{F_2}$ and $\mathcal{T}_2^{F_2}$. However, this will split bus 2 from the rest of $\mathcal{T}_2^{F_2}$. I_4 is an unassigned boundary

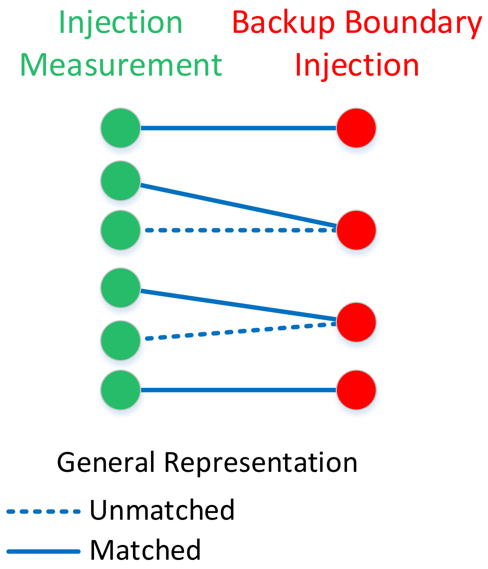

Figure 3.4: Illustration of a maximum matching over the injection measurements - backup boundary injections bipartite graph.

injection in $\mathcal{G}_2^{F_2}$ and can reconnect bus 2 to $\mathcal{T}_2^{F_2}$ by assigning I_4 to line 4. However, I_4 is itself an injection at a bus in $\mathcal{N}_{2,1}^{F_2}$. Hence, I_4 is an unassigned injection in $\mathcal{M}^{F_2}$, and is as a result part of $\mathcal{C}^{F_2}$. Thus, it cannot be considered a backup boundary injection for I_2.

Therefore, an assigned injection measurement $m' \in \mathcal{M}^m \cap \mathcal{M}^C$ is a redundant measurement and is, as a result, part of $\mathcal{C}^m$ if it has a nonempty boundary injection set $\mathcal{I}_{b-m'}^m$. However, a boundary injection may be part of multiple backup boundary injection sets. In this regard, based on the measurement assignment rules, an injection measurement can be assigned to only one line at a time. In relation to backup boundary injections, an unassigned boundary injection can act as a backup boundary injection for *only one* measurement in $\mathcal{M}^m \cap \mathcal{M}^C$, at a time. Hence, if two measurements m_1 and m_2 in $\mathcal{M}^m \cap \mathcal{M}^C$ have only one and the same backup boundary injection, only one of them can be in $\mathcal{C}^m$, concurrently. As a result, due to this one-to-one assignment requirement between backup boundary injections and injection measurements in $\mathcal{M}^m \cap \mathcal{M}^C$, finding this assignment can be performed by solving a *maximum matching problem over a bipartite graph*[5], as the one shown in Fig. 3.4. We refer to this graph as the *injection measurements - backup boundary injections bipartite graph*.

In this bipartite graph, the left-side nodes denote the injection measurements in $\mathcal{M}^m \cap \mathcal{M}^C$ and right-side nodes denote the union of their backup boundary injections, $\bigcup\limits_{m' \in \mathcal{M}^m \cap \mathcal{M}^C} \mathcal{I}_{b-m'}^m$, in which each node represents one backup boundary injection. In this bipartite graph, an edge exists between a node $m' \in \mathcal{M}^m \cap \mathcal{M}^C$, on the left-side of the graph, and a boundary injection m'', on the right-side of the graph, if $m'' \in \mathcal{I}_{b-m'}^m$. Here, we note that a boundary injection can be simultane-

[5] A matching over a graph is a subset of edges sharing no vertices. A maximum matching is a matching having the maximum possible number of edges [145].

ously part of different backup boundary injection sets. Hence, finding the injection measurements in $\mathcal{M}^m \cap \mathcal{M}^C$ which are part of the critical set of m, $\mathcal{C}^m$, requires solving a maximum matching problem over this bipartite graph, which is a problem whose exact solution can be obtained efficiently[6]. As a result, the matched left-side nodes in this maximum matching over the injection measurements - backup boundary injections bipartite graph are the injection measurements in $\mathcal{M}^m \cap \mathcal{M}^C$ which will be part of the critical set of m, $\mathcal{C}^m$.

Based on these introduced rules for building critical sets, Algorithm 1 provides a structured step-by-step method for building the critical set, $\mathcal{C}^m$, for each measurement $m \in \mathcal{M}^C$.

3.3.2 Example and Case Analysis

As an example of characterizing the critical sets of the various measurements in a power system, we consider the IEEE 14-bus system in Fig. 3.1. In this example, we refer to an injection measurement over bus k as I_k and a flow measurement over line k as F_k. We first consider the measurement over line 2, F_2, for which we find the critical set $\mathcal{C}^{F_2}$ using Algorithm 1.

From Fig. 3.2, we can see that removing F_2 will result in splitting the original spanning tree into two trees, $\mathcal{T}_1^{F_2}(\mathcal{N}_1^{F_2}, \mathcal{B}_1^{F_2})$ and $\mathcal{T}_2^{F_2}(\mathcal{N}_2^{F_2}, \mathcal{B}_2^{F_2})$, such that $\mathcal{N}_1^{F_2} = \{1, 5, 6, 10, 12, 13\}$ and $\mathcal{N}_2^{F_2} = \{2, 3, 4, 7, 8, 9, 11, 14\}$ are the sets of nodes of the two trees and $\mathcal{B}_1^{F_2} = \{1, 10, 13, 12, 19\}$ and $\mathcal{B}_2^{F_2} = \{4, 6, 8, 15, 9, 16, 17\}$ are their sets of branches. In addition, $\mathcal{N}_{1,2}^{F_2} = \{1, 5, 10, 13\}$, $\mathcal{N}_{2,1}^{F_2} = \{2, 4, 11, 14\}$, $\mathcal{L}^{F_2} = \{2, 3, 7, 18, 20\}$, and $\mathcal{M}^{F_2} = \{F_2,\ I_4,\ I_{11},\ I_2, I_1,\ I_5,\ I_{13}\}$. Now, for characterizing the critical set of F_2, we explore the set $\mathcal{M}^{F_2}$.

The first measurement in $\mathcal{M}^{F_2}$ is F_2. F_2 is a flow measurement[7]. Hence, $F_2 \in \mathcal{C}^{F_2}$.

The second and third measurements in $\mathcal{M}^{F_2}$ are I_4 and I_{11}. I_4 and I_{11} are unassigned injection measurements, i.e. $I_4 \notin \mathcal{M}^C$ and $I_{11} \notin \mathcal{M}^C$. Hence, $\{I_4, I_{11}\} \subseteq \mathcal{C}^{F_2}$. Indeed, I_4 can be assigned to line 7 to reconnect $\mathcal{T}_1^{F_2}$ and $\mathcal{T}_2^{F_2}$, while I_{11} can be assigned to line 18 for that purpose.

I_2 is the fourth measurement in $\mathcal{M}^{F_2}$ and the last remaining injection measurement on $\mathcal{N}_{2,1}^{m}$ to be explored. I_2 is an assigned measurement, originally assigned to line 4 as part of the spanning tree $\mathcal{T}$. Since $I_2 \in \mathcal{M}^C$, assigning I_2 to lines 2 or 3 to reconnect $\mathcal{T}_1^{F_2}$ and $\mathcal{T}_2^{F_2}$ will disconnect bus 2 from the rest of $\mathcal{T}_2^{F_2}$. Hence, we next characterize the backup boundary injection set of I_2, i.e. $\mathcal{I}_{b-I_2}^{F_2}$. The only unassigned boundary injection in $\mathcal{G}_2^{F_2}$ that is not part of $\mathcal{M}^{F_2}$ is I_7. However, using the algorithm in [187, Fig. 1], we can observe that starting from I_7, the algorithm does not reach bus 2. Hence, bus 2 cannot be reconnected to the rest of $\mathcal{T}_2^{F_2}$ using any unassigned boundary injections over buses in $\mathcal{G}_2^{F_2}$. Hence, $\mathcal{I}_{b-I_2}^{F_2} = \emptyset$, and as a result $F_2 \notin \mathcal{C}^{F_2}$.

Similarly, exploring I_1 and I_5 – the fifth and sixth measurements in $\mathcal{M}^{F_2}$ – which are both assigned

[6] The solution of a maximum matching problem over a bipartite graph can be efficiently obtained in polynomial time by transforming the matching problem into a max-flow problem, which can be solved in polynomial time using various known algorithms such as *Ford-Fulkerson* [145].

[7] F_2 is the only flow measurement in $\mathcal{M}^{F_2}$.

Algorithm 1 Critical sets step-by-step procedure

```
Input: Power system 1-line diagram $\mathcal{G}(\mathcal{N}, \mathcal{L})$, measurement set $\mathcal{M}$, spanning tree $\mathcal{T}(\mathcal{N}, \mathcal{B})$, set
    of assigned measurements $\mathcal{M}^C$, assignment function $f(.)$: $\mathcal{M} \rightarrow \mathcal{L}$
Output: Critical set $\mathcal{C}^m$ for all measurements $m \in \mathcal{M}^C$
for $m \in \mathcal{M}^C$ do
    Characterize $\mathcal{T}_1^m$, $\mathcal{T}_2^m$, $\mathcal{N}_{1,2}^m$, $\mathcal{N}_{2,1}^m$, $\mathcal{L}^m$, $\mathcal{M}^m$
    Initialize $\mathcal{C}^m$
    Initialize $\mathcal{M}_{\text{test}}^m$
    Add $m$ to $\mathcal{C}^m$
    for $m' \in \mathcal{M}^m$ do
        if $m'$ is a flow measurement then
            Add $m'$ to $\mathcal{C}^m$
        end if
        if $m'$ is an injection measurement then
            if $m' \notin \mathcal{M}^C$ then
                Add $m'$ to $\mathcal{C}^m$
            end if
            if $m' \in \mathcal{M}^C$ then
                Characterize its backup boundary injection set $\mathcal{I}_{b-m'}^m$
                Add $m'$ to $\mathcal{M}_{\text{test}}^m$
            end if
        end if
    end for
    Solve maximum matching over the injection measurements - backup boundary injections
        bipartite graph
    for $m' \in \mathcal{M}_{\text{test}}^m$ do
        if $m'$ is a matched node as part of the maximum matching then
            Add $m'$ to $\mathcal{C}^m$
        end if
    end for
end for
return Critical set $\mathcal{C}^m$ for all measurements $m \in \mathcal{M}^C$
```

measurements, i.e. $\{I_1, I_5\} \subseteq \mathcal{M}^C$, shows that they both have empty backup boundary injection sets[8], i.e. $\mathcal{I}_{b-I_1}^{F_2} = \emptyset$ and $\mathcal{I}_{b-I_5}^{F_2} = \emptyset$. Hence, neither I_1 nor I_5 are part of $\mathcal{C}^{F_2}$.

The only remaining measurement in $\mathcal{M}^{F_2}$ is I_{13}. I_{13} is an assigned measurement, $I_{13} \in \mathcal{M}^C$. As previously discussed in Section 3.3.1, when I_{13} is reassigned to line 20 to reconnect $\mathcal{T}_1^{F_2}$ and $\mathcal{T}_2^{F_2}$,

[8] If I_1 or I_5 are to be reassigned to lines 2 or 3, respectively, to reconnect $\mathcal{T}_1^{F_2}$ and $\mathcal{T}_2^{F_2}$, each of these reassignments will split $\mathcal{T}_1^{F_2}$ into two subtrees which cannot be reconnected using the unassigned boundary injection I_{12}, as can be shown by a run of the algorithm in [187, Fig. 1]. Here, we note that I_{12} is the only unassigned boundary injection in $\mathcal{G}_1^{F_2}$.

Table 3.1: Critical sets of the measurements in $\mathcal{M}^C$.

Measurement $(m \in \mathcal{M}^C)$	**Critical Set** $(\mathcal{C}^m)$
F_2	$\{F_2, I_4, I_{11}, I_{13}\}$
F_8	$\{F_8, I_4, I_7, I_9\}$
F_9	$\{F_9, I_4, I_7, I_{11}, I_{13}\}$
F_{15}	$\{F_{15}, I_7\}$
I_1	$\{I_1, I_4, I_{11}, I_{13}\}$
I_2	$\{I_2, I_4, I_{11}, I_{13}\}$
I_3	$\{I_3, I_2, I_4\}$
I_5	$\{I_5, I_{11}, I_{13}\}$
I_6	$\{I_6, I_{11}\}$
I_9	$\{I_9, I_{11}\}$
I_{13}	$\{I_6, I_{12}, I_{13}\}$
F_{17}	$\{F_{17}, I_9, I_{13}\}$
F_{19}	$\{F_{19}, I_6, I_{12}\}$

the subtree containing buses 12 and 13 and line 19 gets disconnected from the rest of $\mathcal{T}_1^{F_2}$. Hence, we next characterize the backup boundary injection set of I_{13}, i.e. $\mathcal{I}^{F_2}_{b-I_{13}}$. To this end, I_{12}, the only unassigned boundary injection measurement in $\mathcal{G}_1^{F_2}$, can be assigned to line 11 to reconnect the two subtrees, and is the only boundary injection which can do so. Hence, $\mathcal{I}^{F_2}_{b-I_{13}} = \{I_{12}\}$.

As a result, the injection measurements - backup boundary injections bipartite graph is composed of only I_{13} on the left-side connected to $\mathcal{I}^{F_2}_{b-I_{13}} = \{I_{12}\}$ on the right-side. Hence, I_{13} is matched to the backup boundary injection I_{12}. As a result, $I_{13} \in \mathcal{C}^{F_2}$.

The processing of $\mathcal{M}^{F_2}$ is thus complete, resulting in $\mathcal{C}^{F_2} = \{F_2, I_4, I_{11}, I_{13}\}$.

Similarly, Algorithm 1 can be carried out to characterize the critical sets of all of the measurements in $\mathcal{M}^C$ in the IEEE 14-bus system in Fig.3.1. The results are listed in Table 3.1.

We next discuss the value of critical sets with regard to understanding and analyzing observability attacks. We also introduce the concept of observability sets, a generalization of critical sets, which provides a holistic modeling of observability attacks.

Notation: We use the following notation in the derivations that ensue. For the Jacobian matrix $\boldsymbol{H}$, we let $\boldsymbol{H}^{(-\mathcal{K})+(\mathcal{K}')}$ correspond to $\boldsymbol{H}$ but with the removal of the rows corresponding to measurements in $\mathcal{K}$ and the addition of rows corresponding to measurements in $\mathcal{K}'$.

3.3.3 Observability Sets

Next, in Theorem 1, we show that the derived critical sets are indispensable for modeling observability attacks.

Theorem 1. *For $m \in \mathcal{M}^C$, removing its critical set, $\mathcal{C}^m$, renders the system unobservable.*

Proof. By topological observability, we know that a system is observable if and only if a spanning tree could be formed using an assignment function. When m is removed, the original spanning tree $\mathcal{T}$ is split into two disjoint trees $\mathcal{T}_1^m$ and $\mathcal{T}_2^m$, spanning subgraphs $\mathcal{G}_1^m$ and $\mathcal{G}_2^m$, respectively. By definition of $\mathcal{C}^m$, the only way to reconnect $\mathcal{T}_1^m$ and $\mathcal{T}_2^m$ is to use measurements in $\mathcal{C}^m$. Hence, if all measurements in $\mathcal{C}^m$ are removed, then $\mathcal{T}_1^m$ and $\mathcal{T}_2^m$ cannot be connected using an assignment function, which implies that a spanning tree cannot be formed, implying that the system is not observable. As such, removing a critical set renders the power system unobservable. □

Based on Theorem 1, the critical measurements[9] of a power system can be characterized using critical measurement sets, as shown in the following corollary.

Corollary 1. *m is a critical measurement if and only if its critical set is $\mathcal{C}^m = \{m\}$.*

Proof. By definition, if m is a critical measurement, removing it will render the system unobservable. Hence, if the critical set of m is such that $\mathcal{C}^m \supset m$, then removing m would not affect the observabilty of the system since any other measurement $m' \in \mathcal{C}^m \setminus \{m\}$ can be used to replace m and reconnect the tree. As such, $\mathcal{C}^m \supset \{m\} \Rightarrow m$ is not a critical measurement, which proves the contrapositive: m is critical $\Rightarrow m$ is the only element in its critical set, i.e. $\{m\} = \mathcal{C}^m$. Conversely, if m is the only element in its critical set, its removal constitutes removing a complete critical set, which by Theorem 1 renders the system unobservable. As a result, $\mathcal{C}^m = \{m\} \Rightarrow m$ is a critical measurement. Thus, m is critical if and only if $\mathcal{C}^m = \{m\}$. □

In addition, removing a full critical set decreases the rank of the Jacobian matrix by 1. This is shown in Theorem 2, which will be proven next. However, we first present the following preliminary lemma, which is essential for the proof of Theorem 2.

Lemma 1. *Let $m \in \mathcal{M}$ be an injection measurement over a bus η that is assigned to a line l, $f(m) = l$. Then, replacing m by a hypothetical line flow measurement m' over line l will not affect the rank of matrix $\boldsymbol{H}$. In other words, let $\boldsymbol{H}^{(-m)+(m')}$ be the the Jacobian matrix with the removal of the row corresponding to measurement m and the addition of the row corresponding to the hypothetical measurement m', then rank($\boldsymbol{H}$) = rank($\boldsymbol{H}^{(-m)+(m')}$).*

Proof. Since m is assigned, i.e. is part of the original spanning tree measurement assignment, removing it will split the original spanning tree into two subtrees $\mathcal{T}_1^m$ and $\mathcal{T}_2^m$. By the definition of the critical set $\mathcal{C}^m$, any measurement in $\mathcal{C}^m$ could replace m to reconnect $\mathcal{T}_1^m$ and $\mathcal{T}_2^m$. If m' existed, it would have been part of $\mathcal{C}^m$ because m' can reconnect $\mathcal{T}_1^m$ and $\mathcal{T}_2^m$. Hence, replacing m by m' will not affect the connectivity of the spanning tree and, hence, rank$(\boldsymbol{H})$ = rank$(\boldsymbol{H}^{(-m)+(m')})$. □

Theorem 2. *For $m \in \mathcal{M}^C$, removing its critical set, $\mathcal{C}^m$, results in rank($\boldsymbol{H}^{(-\mathcal{C}^m)}$) = rank($\boldsymbol{H}$) $- 1$.*

[9] In power systems, a critical measurement is a single measurement which when removed renders the system unobservable [176].

Proof. Since the system is originally fully observable, rank($\boldsymbol{H}$) $= N-1$. Now, let $\mathcal{M}_1^m$ and $\mathcal{M}_2^m$ be the measurement sets in subgraphs $\mathcal{G}_1^m$ and $\mathcal{G}_2^m$, respectively, and let $\boldsymbol{H}_1^{(-\mathcal{C}^m)}$ and $\boldsymbol{H}_2^{(-\mathcal{C}^m)}$ be the Jacobian matrices of $\mathcal{G}_1^m$ and $\mathcal{G}_2^m$, respectively, composed of measurements in $\mathcal{M}_1^m \setminus \{\mathcal{M}_1^m \cap \mathcal{C}^m\}$ and $\mathcal{M}_2^m \setminus \{\mathcal{M}_2^m \cap \mathcal{C}^m\}$. Since $\mathcal{T}_1^m$ and $\mathcal{T}_2^m$ respectively span $\mathcal{G}_1^m$ and $\mathcal{G}_2^m$, this implies that rank($\boldsymbol{H}_1^{(-\mathcal{C}^m)}$) $= N_1 - 1$ and rank($\boldsymbol{H}_2^{(-\mathcal{C}^m)}$) $= N_2 - 1$. In addition, let $m' \in \mathcal{M}_1^m \setminus \{\mathcal{M}_1^m \cap \mathcal{C}^m\}$ be an injection measurement over a bus in $\mathcal{N}_{1,2}^m$. Since $m' \in \mathcal{M}_1^m \setminus \{\mathcal{M}_1^m \cap \mathcal{C}^m\}$, then m' is assigned to a certain branch $b' = f(m') \in \mathcal{T}_1^m$; otherwise, m' would have also been in $\mathcal{C}^m$. By Lemma 1, m' can be replaced by a hypothetical line flow measurement over b' without affecting the rank of $\boldsymbol{H}_1^{(-\mathcal{C}^m)}$. As such, let $\boldsymbol{H}_1^{(-\mathcal{C}^m)'}$ be the same as $\boldsymbol{H}_1^{(-\mathcal{C}^m)}$ but replacing any row corresponding to an injection measurement in $\mathcal{N}_{1,2}^m$ by its corresponding hypothetical line flow measurement. The same can be done to form Jacobian matrix $\boldsymbol{H}_2^{(-\mathcal{C}^m)'}$ from $\boldsymbol{H}_2^{(-\mathcal{C}^m)}$. By Lemma 1, rank($\boldsymbol{H}_1^{(-\mathcal{C}^m)'}$)=rank($\boldsymbol{H}_1^{(-\mathcal{C}^m)}$) $= N_1 - 1$ and rank($\boldsymbol{H}_2^{(-\mathcal{C}^m)'}$)=rank($\boldsymbol{H}_2^{(-\mathcal{C}^m)}$) $= N_2 - 1$.

Now, let us return to $\boldsymbol{H}^{(-\mathcal{C}^m)}$. By rearranging its elements to include first the measurements in $\mathcal{M}_1^m \setminus \{\mathcal{M}_1^m \cap \mathcal{C}^m\}$ then the elements of $\mathcal{M}_2^m \setminus \{\mathcal{M}_2^m \cap \mathcal{C}^m\}$, $\boldsymbol{H}^{(-\mathcal{C}^m)}$ can be written as $\boldsymbol{H}^{(-\mathcal{C}^m)} = \begin{bmatrix} \boldsymbol{H}_1^{(-\mathcal{C}^m)} \\ \boldsymbol{H}_2^{(-\mathcal{C}^m)} \end{bmatrix}$. In this respect,

$$\begin{aligned}
\text{rank}(\boldsymbol{H}^{(-\mathcal{C}^m)}) &= \text{rank}\Big(\begin{bmatrix} \boldsymbol{H}_1^{(-\mathcal{C}^m)} \\ \boldsymbol{H}_2^{(-\mathcal{C}^m)} \end{bmatrix} \Big) \\
&= \text{rank}\Big(\begin{bmatrix} \boldsymbol{H}_1^{(-\mathcal{C}^m)'} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{H}_2^{(-\mathcal{C}^m)'} \end{bmatrix} \Big) \\
&= (N_1 - 1) + (N_2 - 1) \\
&= N - 2 = \text{rank}(\boldsymbol{H}) - 1.
\end{aligned}$$

□

Therefore, Theorem 2 shows the effect of the removal of a single critical set on the rank of the Jacobian matrix. Theorem 1 and Theorem 2 provide a necessary condition for observability of the power system under observability attacks. In fact, the contrapositive of Theorem 1 states that if a power system is fully observable, then the investigated observability attack (i.e. the removal of measurements) did not result in removing a full critical set. Next, we extend this concept to account for the interconnection between multiple critical sets.

In fact, for a measurement m' to be in the critical set of a measurement m, i.e. $m' \in \mathcal{C}^m$, the critical set of m', $\mathcal{C}^{m'}$, must contain measurements other than m', i.e. $\mathcal{C}^{m'} \supset \{m'\}$. Otherwise, m' would not be redundant. For example, consider injection measurements I_6 and I_9. Removing I_6 and I_9 will render the system unobservable – even though I_6 and I_9 do not form a critical set – since $\mathcal{C}^{I_6} = \{I_6, I_{11}\}$ and $\mathcal{C}^{I_9} = \{I_9, I_{11}\}$. As such, if I_6 is removed, I_{11} can be used to replace I_6 since $I_{11} \in \mathcal{C}^{I_6}$. However, if I_9 is also removed, even though $I_{11} \in \mathcal{C}^{I_9}$, I_{11} cannot be used to replace I_9 since I_{11} has already been used as a replacement to I_6. Therefore, removing I_9 and I_6 does render the system unobservable. Indeed, $\text{rank}(\boldsymbol{H}^{-(I_6)-(I_9)}) = 12 < N - 1 = 13$.

This concept can be extended to the interconnection between multiple critical sets. For example, consider F_2, I_1, I_2, and I_5 and their critical sets shown in Table 3.1. We can see that F_2, I_1, and I_2 have critical sets sharing measurements I_4, I_{11}, and I_{13}. Hence, if F_2, I_1, and I_2 are removed, I_4, I_{11}, and I_{13} are assigned, one to each of these measurements, to preserve system observability and, hence, cannot be used as part of further critical sets in case further measurements are removed. Hence, since $\mathcal{C}^{I_5} = \{I_5, I_{11}, I_{13}\}$, removing F_2, I_1, I_2 and I_5 will render the system unobservable, even though $\{F_2,\ I_1,\ I_2,\ I_5\}$ is not a critical set.

In this respect, the concept of critical sets must be further developed to yield a general graph-theoretic concept of observability attacks. This development is provided as follows. We build a bipartite graph in which each left-side node represents one of the critical sets of the power system, and each right-side node represents one measurement of the system. An example of this bipartite graph is shown in Fig. 3.5. In this respect, an edge is drawn between a critical set $\mathcal{C}^i$ and a measurement j if $j \in \mathcal{C}^i$. We refer to this bipartite graph as the *critical sets - system measurements bipartite graph*. Based on this formulation, a general concept of observability is established in Theorem 3.

Theorem 3. *If the system is observable, then a maximum matching over the critical sets - system measurements bipartite graph includes all critical sets.*

Proof. We prove this theorem by proving its contrapositive which is the following: if a maximum matching does not include all critical sets, then the system is not observable.

The contrapositive can be proven as follows. If one critical set is not matched to any measurements, then this critical set cannot be used to connect two subgraphs of the system. Since these two subgraphs can only be connected by this critical set, then there is no measurement assignment which will connect these two subgraphs. As a result, a spanning tree cannot be formed, implying that the system is not observable.

This proves the contrapositive of this theorem and, hence, proves the theorem. □

Theorem 3 can be used to fully characterize observability attacks as follows. An observability attack is one in which measurements are removed (i.e. nodes from the right-side of the critical sets - system measurements bipartite graph) such that a maximum matching over the bipartite graph does not include all critical sets (i.e. nodes on the left-side of the critical sets - system measurements bipartite graph), which renders the system unobservable. This, as a result, provides a general analytical characterization of observability attacks and enables an analytical prediction of the effect of the removal of a subset of measurements on the observability of the system. For example, such characterization allows analytical derivation of various security indices related to observability attacks such as finding the observability attack of lowest cardinality, or finding the minimal set of measurements to remove in addition to a certain measurement to make the system unobservable. This, as a result, provides analytical tools which are necessary to further assess the vulnerability of a system against observability attacks as well as derive defense strategies to thwart such attacks. Indeed, in what follows, we focus on stealthy data injection attacks – proving that they are a subset of observability attacks – and show how our provided analytical characterization of observability attacks enables solutions of various widely-studied stealthy data injection attack problems. To this end, we introduce sets of measurements, dubbed *observability sets*, as follows, which are valuable for the analysis of data injection attacks which ensues.

Definition 9. *An* observability set $\mathcal{S} \in \mathcal{M}$*, is a set of measurements such that strictly removing* $\mathcal{S}$ *leads a maximum matching over the critical sets - system measurements bipartite graph not to include a certain critical set.*

The term "strictly" in this definition reflects that adding any measurement $s \in \mathcal{S}$, which was removed, back to the right-side of the bipartite graph will result in reincluding the previously unmatched critical set in the maximum matching. A *union of observability sets* is, then, defined to be a set of measurements composed of a number of observability sets such that, when each of these sets is successively removed, each such removal leads to excluding one additional critical set from being part of a maximum matching over the critical sets - system measurements bipartite graph. Adding back any of the removed measurements to the right-side of the bipartite graph will result in reincluding one of the unmatched critical sets in the maximum matching. These observability sets play a crucial role in characterizing stealthy data injection attacks, as will be shown next.

We next introduce stealthy data injection attacks and prove that they are a variant of our introduced observability attacks. This enables further studying and solving various problems related to SDIAs using our developed analytical tools.

3.4 Stealthy Data Injection Attacks

3.4.1 Stealthy Data Injection Attacks

Recalling the measurement-state equation in (3.1), data injection attacks aim at replacing the measurement vector, $\boldsymbol{z}$ by a manipulated measurement vector $\boldsymbol{z}^a = \boldsymbol{z} + \boldsymbol{a}$, where $\boldsymbol{a} \in \mathbb{R}^m$ is the *attack vector*, resulting in a new state estimate $\hat{\boldsymbol{x}}^a$. However, typically, the state estimation process is run in conjunction with what is known as a bad data detector and identifier (BDD). The BDD aims at detecting and identifying the presence of outliers in the collected data set, so that such outliers can be removed preventing them from affecting the estimation outcome. Such BDDs rely on the statistical analysis of what is known as measurement residuals, $\boldsymbol{r}$, defined as [176]:

$$\hat{\boldsymbol{z}} = \boldsymbol{H}\hat{\boldsymbol{x}} = \boldsymbol{S}\boldsymbol{z}, \ \boldsymbol{r} = \boldsymbol{z} - \hat{\boldsymbol{z}} = (\boldsymbol{I}_n - \boldsymbol{S})\boldsymbol{z} = \boldsymbol{W}\boldsymbol{z}, \tag{3.4}$$

where $\boldsymbol{S} = \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}$ and $\boldsymbol{W} = \boldsymbol{I}_n - \boldsymbol{S}$.

A statistical analysis on the residuals enables analysis of the magnitudes of the errors associated with each measurement, and hence, allows the identification of outliers [176]. Regarding data injection attacks, when data is added to certain measurements, the adversary aims at keeping the residuals unchanged, so that the attack cannot be detected by the BDD. Indeed, as shown in [76], an attack vector that falls in the column-space of the Jacobian matrix $\boldsymbol{H}$, i.e. $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$, cannot be detected by residual statistical analysis. Indeed, for $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$,

$$\begin{aligned}\boldsymbol{r}^a &= \boldsymbol{W}(\boldsymbol{z} + \boldsymbol{a}) = \boldsymbol{r} + \boldsymbol{W}\boldsymbol{a} \\ &= \boldsymbol{r} + [\boldsymbol{I}_n - \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}]\boldsymbol{H}\boldsymbol{c} \\ &= \boldsymbol{r} + \boldsymbol{H}\boldsymbol{c} - \boldsymbol{H}\boldsymbol{c} = \boldsymbol{r}. \end{aligned} \tag{3.5}$$

As such, given the weighted least squares state estimation equation in (3.2), the attack vector $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$ generates an arbitrary new state estimate $\hat{\boldsymbol{x}}^a = \hat{\boldsymbol{x}} + \boldsymbol{c}$ by choosing the constant vector $\boldsymbol{c}$ without inducing any changes to the residual vector, as shown in (3.5). Such DIAs are, hence, stealthy and are referred to as stealthy DIAs. The ability of SDIAs to stealthily manipulate the state estimates poses various challenges to the operation of the grid. Hence, understanding and modeling such attacks is indispensable to the secure and sustainable operation of power systems.

To this end, we next introduce a holistic graph-theoretic modeling of SDIAs that is based on the graph-theoretic modeling of observability attacks introduced in Section 3.3.

3.4.2 Graph-Theoretic Modeling of SDIAs

The observability attacks and observability sets introduced in Section 3.3 provide the basis for a graph-theoretic interpretation of SDIAs as will be shown in Theorem 4. However, before introducing and proving Theorem 4, we introduce a preliminary lemma which will be used in the proof of Theorem 4.

Lemma 2. *If a DIA is stealthy (i.e. $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$), then removing the attacked measurements renders the system unobservable.*

Proof. Since the attack vector $\boldsymbol{a}$ is stealthy, then $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$. Since $\boldsymbol{H}$ is of full rank, then the only solution to $\boldsymbol{H}\boldsymbol{c} = 0$ is $\boldsymbol{c} = \boldsymbol{0}$. Hence, $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$ has zero and nonzero elements for $\boldsymbol{c} \neq \boldsymbol{0}$. Now, if all of the rows of $\boldsymbol{H}$ corresponding to nonzero elements of $\boldsymbol{a}$ are removed to form matrix $\boldsymbol{H}_{\text{new}}$, then, this results in $\boldsymbol{a}_{\text{new}} = \boldsymbol{H}_{\text{new}}\boldsymbol{c} = \boldsymbol{0}$ for $\boldsymbol{c} \neq \boldsymbol{0}$. Hence, $\boldsymbol{H}_{\text{new}}$ is not of full rank and the power system whose Jacobian matrix is given by $\boldsymbol{H}_{\text{new}}$ is unobservable. Therefore, when the attack is stealthy, removing the attacked measurements renders the system unobservable. □

Here we note, that the result of Lemma 2, provides a one directional relation stating that if $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$, i.e. the attack is stealthy, then the removal of the nonzero elements of $\boldsymbol{a}$, i.e. the attacked measurements, causes the system to be unobservable. However, the reverse direction does not always hold true. Indeed, the reverse statement of Lemma 2 states that, if removing a set of measurements renders the system unobservable, then this guarantees that a stealthy DIA can be constructed which targets all of these measurements, and only these measurements. We next provide a counter example which proves that this reverse statement does not hold true. In this regard, we consider the Jacobian matrix $\boldsymbol{H}$ to be represented as follows: $\boldsymbol{H} = \begin{bmatrix} \boldsymbol{H}_0 \\ \boldsymbol{H}_1 \end{bmatrix}$. We let $\mathcal{M}_0$ and $\mathcal{M}_1$ represent the subset of measurements corresponding to the rows of $\boldsymbol{H}_0$ and $\boldsymbol{H}_1$, respectively. Consider $\mathcal{M}_0$ to contain one critical measurement, i.e., one row of $\boldsymbol{H}_0$ is independent of all of the other rows of $\boldsymbol{H}$. As such, removing the subset of measurements $\mathcal{M}_0$ renders the system unobservable. In addition, consider two measurements $m_0 \in \mathcal{M}_0$ and $m_1 \in \mathcal{M}_1$ such as m_0 measures the power flow from bus i to bus j and m_1 measures the power flow from bus j to bus i (i.e., m_0 and m_1 are installed on the same transmission line but measure the flow in two opposite directions). In this regard, let $\boldsymbol{h}_0$ and $\boldsymbol{h}_1$ correspond to the rows of m_0 and m_1 in, respectively, $\boldsymbol{H}_0$ and $\boldsymbol{H}_1$. Then, we have[10] $\boldsymbol{h}_0 = -\boldsymbol{h}_1$. As a result, one cannot find a stealthy attack vector $\boldsymbol{a} = \begin{bmatrix} \boldsymbol{a}_0 \\ \boldsymbol{a}_1 \end{bmatrix} = \begin{bmatrix} \boldsymbol{H}_0 \\ \boldsymbol{H}_1 \end{bmatrix} \boldsymbol{c}$, in which all the elements of $\boldsymbol{a}_0$ are nonzero and all the elements of $\boldsymbol{a}_1$ are zero, since if $\boldsymbol{h}_0\boldsymbol{c} \neq 0$, then $\boldsymbol{h}_1\boldsymbol{c} \neq 0$, due to the fact that $\boldsymbol{h}_0 = -\boldsymbol{h}_1$. This implies that for the attack to target all the measurements in $\mathcal{M}_0$ and be stealthy, this attack must also target measurements in $\mathcal{M}_1$. Otherwise, this attack must be limited to a strict subset of $\mathcal{M}_0$ and may not target all the measurements in $\mathcal{M}_0$. As a result, even though removing the measurements in $\mathcal{M}_0$ renders the system unobservable, one cannot necessarily construct a stealthy attack vector that only targets all the measurements in $\mathcal{M}_0$. Hence, this provides a counter example of the reverse statement of Lemma 2 proving that this reverse statement does not always hold true.

Theorem 4. *A DIA is stealthy if and only if the attacked measurements constitute a union of observability sets.*

Proof. We begin by proving that when the attacked measurements (i.e. nonzero elements of the attack vector $\boldsymbol{a}$) constitute a union of observability sets, then $\boldsymbol{a}$ is stealthy (i.e. $\boldsymbol{a}$ can be represented as $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$). As shown in Theorem 3, when an observability set (equivalently, a union of observability sets) is removed, the system is unobservable. Hence, consider an observability set $\mathcal{S}$ which has been removed. Let $\boldsymbol{H}^{(-\mathcal{S})}$ be the system's Jacobian matrix without the measurements in $\mathcal{S}$ and let $\mathcal{C}$ be the critical set which cannot be part of a maximum matching over the critical sets - system measurements bipartite graph when $\mathcal{S}$ is removed. Since the system is unobservable when removing $\mathcal{S}$, $\boldsymbol{H}^{(-\mathcal{S})}\boldsymbol{y} = 0$ for a $\boldsymbol{y} \neq \boldsymbol{0}$. However, the addition of any measurement $s \in \mathcal{S}$ will reinclude $\mathcal{C}$ in the maximum matching over the critical sets - system measurements bipartite graph, and hence, reconnect the tree. As such, let $\boldsymbol{H}^{(-\mathcal{S})+(k)}$ correspond to $\boldsymbol{H}^{(-\mathcal{S})}$ with the addition of a row corresponding to a measurement $k \in \mathcal{S}$. In this regard, since the system is rendered observable, $\boldsymbol{H}^{(-\mathcal{S})+(k)}$ is of full rank and $\boldsymbol{H}^{(-\mathcal{S})+(k)}\boldsymbol{y}$ will have one nonzero element corresponding to the row of $\boldsymbol{H}^{(-\mathcal{S})+(k)}$ pertaining to the added measurement k. This procedure can be repeated for

[10] Since $P_{ij} = -P_{ji}$, where P_{ij} and P_{ji} are the real power flow from bus i to bus j and from bus j to bus i, respectively, over the same transmission line.

all $k \in \mathcal{S}$. As such, adding the rows corresponding to $\mathcal{S}$ back to the Jacobian matrix results in $\boldsymbol{b} = \boldsymbol{H}\boldsymbol{y}$ in which only the elements of $\boldsymbol{b}$ corresponding to measurements in $\mathcal{S}$ are nonzero. As a result, $\boldsymbol{a} = \boldsymbol{b}$ is an attack vector in which only the observability set $\mathcal{S}$ is attacked and is proven to be stealthy.

Now, we prove that, when an attack is stealthy, i.e. $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$, then the nonzero elements of $\boldsymbol{a}$ correspond to a union of observability sets. In this regard, from Lemma 2, we know that removing the nonzero elements of $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$ will render the system unobservable, which implies that the nonzero elements of $\boldsymbol{a}$ contain at least one observability set. Let $\mathcal{S}$ denote this observability set, and let $\boldsymbol{H}^{(-\mathcal{S})}$ be the system's Jacobian matrix without the measurements in $\mathcal{S}$. Removing $\mathcal{S}$ will lead to two subsystems each of which is fully observable (i.e. it will split the spanning tree, $\mathcal{T}$, into two subtrees each of which spans its own subgraph). Let $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$ be the Jacobian matrices of each of these two subsystems (we denote these subsystems as subsystem 1 and subsystem 2) and let $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$ correspond to the portions of $\boldsymbol{a}$ (excluding the measurements of the previously removed observability set) corresponding to the measurements in $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$, respectively. In addition, let $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ correspond to the portions of $\boldsymbol{c}$ pertaining to nodes in subsystem 1 and subsystem 2, respectively. Now, if $\boldsymbol{a}_i$ for $i \in \{1, 2\}$ has nonzero elements, this implies that removing these elements will make subsystem i unobservable, which implies that the nonzero elements of $\boldsymbol{a}_i$ contain an observability set. Following this same logic, removing this observability set will subsequently split subsystem i into two subsystems, each of which is observable. This process can be continued recursively until no measurement m corresponding to a nonzero element of $\boldsymbol{a}$ remains. Hence, this shows that when $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$, then the nonzero elements of $\boldsymbol{a}$ correspond to a union of observability sets.

This proves both directions of the theorem, and hence, concludes the proof. □

Theorem 4 provides an analytical graph-theoretic modeling of SDIAs using the fundamentals of observability attacks introduced in Section 3.3. This enables a fundamental understanding of SDIAs since it allows the characterization of the subset of measurements which would be compromised as part of an SDIA and hence enables defense against such attacks. In addition, this analytical characterization of SDIAs enables a more in-depth analysis of such integrity attacks and allows a unified derivation of analytical solutions to a wide-range of well-studied problems in this field, as will be explored in Section 3.4.3.

Example 1. *As an illustrative example of the result*[11] *in Theorem* 4*, we consider the IEEE 14-bus system, shown in Fig.* 3.1*, whose line transmission data can be found in [190]. We consider the stealthy attack* $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$ *with* $\boldsymbol{c} = [1, 0, ..., 0]^T$*, which corresponds to having the attack vector equal to the first column of the Jacobian matrix* $\boldsymbol{H}$ *given by* $\boldsymbol{H}(:, 1) = [\ -16.9,\ 0,\ 0,\ 0,\ -16.9,\ 33.37,\ -5.05,\ -5.67,\ -5.75,\ \textit{zeros}(1, 8)\ ]^T$*. This attack consists of attacking measurement indices* $\{\ 1,\ 5,\ 6,\ 7,\ 8,\ 9\}$ *which correspond to* $\{F_2, I_1, I_2, I_3, I_4, I_5\}$*. In this respect, we next verify whether this attack is stealthy, following Theorem* 4*. To this end, Fig.* 3.5 *shows a portion of the critical sets*

[11] In this example, we index the measurements in Fig. 3.1 from 1 to 17 in an incremental manner based on the following order (F_2, F_8, F_9, F_{15}, I_1, I_2, I_3, I_4, I_5, I_6, I_7, I_9, I_{11}, I_{12}, I_{13}, F_{17}, F_{19}).

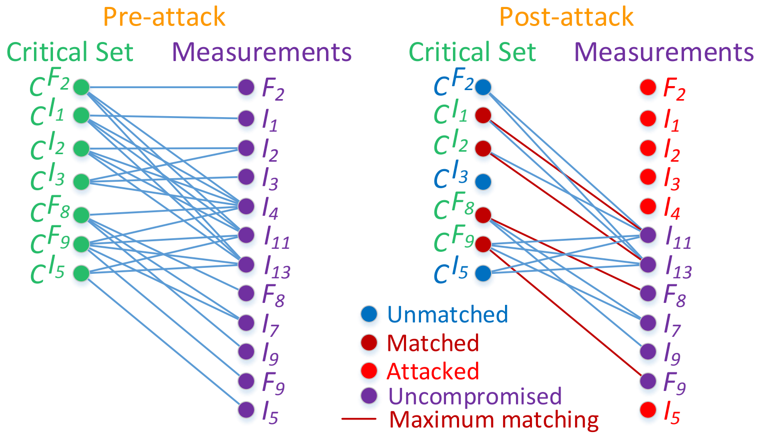

Figure 3.5: Critical sets – system measurements maximum matching and SDIAs.

- system measurements bipartite graph that is relevant to the attacked measurements. The post-attack portion of Fig. 3.5 *marks the nodes corresponding to measurements* $\{F_2,I_1,I_2,I_3,I_4,I_5\}$*, on the right-side of the bipartite graph, as attacked (following the attack vector* $\boldsymbol{a}$*). As a result, all the edges connecting these nodes to the critical sets on the left-side of the bipartite graph are removed. Then, building a maximum matching over the post-attack bipartite graph shows that, indeed, not all the critical sets are matched. Hence, the removed measurements lead to a maximum matching that does not include all critical sets. Furthermore, the addition of a node corresponding to any of the attacked measurements, i.e.* $\{F_2,I_1,I_2,I_3,I_4,I_5\}$*, would lead to reincluding one of the unmatched critical sets* $\{\mathcal{C}^{F_2},\mathcal{C}^{I_3},\mathcal{C}^{I_5}\}$ *in the maximum matching. This implies that the attack consists of a union of observability sets which implies that the attack is, indeed, stealthy.*

3.4.3 Unified Solution to Diverse SDIA Problems

Theorem 4 provides a basis for studying various SDIA problems from a graph-theoretic perspective. Indeed, this representation provides a unified approach for characterizing analytical solutions to various widely-studied SDIA problems. In this regard, we next present a set of such SDIA problems and show that the derivations leading to Theorem 4 enable the understanding and characterization of analytical solutions to these problems.

SDIA analyses can be categorized based on whether the focus is on modeling the attack or the defense strategies. As such, we first present two problems focusing on *modeling attack strategies* followed by two problems focusing on the derivation of *defense strategies* to thwart SDIAs.

Modeling SDIA Attack Strategies

Modeling SDIA attack strategies enables a vulnerability assessment of the system and allows anticipating sophisticated attack strategies which can target the system. This, in turn, allows the derivation of adequate defense strategies to thwart such attacks. As such, solving SDIA problems focusing on modeling the attack strategies is indispensable to understanding such attacks and, as a result, defending the system against them. We next focus on two problems which aim at modeling potential attack strategies.

Problem 1: If measurement $k \in \mathcal{M}$ is attacked, what is the minimal set of measurements which must be attacked along with k for the attack to be stealthy? In other words, *Problem 1* seeks the solution to the following optimization problem:

$$\min_{\boldsymbol{c}} ||\boldsymbol{H}\boldsymbol{c}||_0,$$
$$\text{subject to: } \boldsymbol{H}(k,:)\boldsymbol{c} = 1. \tag{3.6}$$

Problem 1 has been proposed in [179] and studied in [180] and [181]. However, the derived solution in [180] is based on an approximate relaxation method while the solution in [181] focuses on the special case assuming that the measurement set consists of all injection measurements at all buses and all line flow measurements at all transmission lines, which limits its generality. Instead, here, we provide a general analytical characterization of the solution to this problem using our developped graph-theoretic framework.

The solution to this problem enables a vulnerability assessment of each measurement against SDIAs since it shows, for each measurement, what is the minimum number of measurements which must be additionally compromised to potentially launch an SDIA against the system. This can represent a security index of that measurement following which, a measurement with a lower (higher) security index is more (less) vulnerable to SDIAs. In other words, a measurement which has a low security index is more easily targeted by SDIAs since the adversary would not need to comprise a large number of additional measurements to lunch the stealthy attack. Such knowledge can be used to improve the security of the system, by adding redundancy or incorporating security defense mechanisms at the meters which are deemed the most vulnerable to SDIAs.

The analytical graph-theoretic solution to *Problem 1* is characterized in Theorem 5.

Theorem 5. *The stealthy attack of smallest cardinality containing measurement k corresponds to attacking the measurements of the critical set of lowest cardinality which contains k.*

Proof. First, we show that the attack containing the critical set of lowest cardinality containing k is, indeed, stealthy. Then, we prove that this attack corresponds to the stealthy attack containing k that has a minimum cardinality.

By Theorem 4, for the attack to be stealthy, the removal of the attacked measurements must lead a maximum matching over the critical sets - system measurements bipartite graph not to include all the critical sets (i.e. all the left-side nodes of the bipartite graph). In other words, the attack must be composed of a union of obseravbility sets. In this respect, removing the critical set containing k that is of smallest cardinality is, indeed, stealthy since removing a whole critical set will disconnect the node corresponding to this critical set (on the left-hand side of the critical sets - system measurements bipartite graph) from the right-side of the bipartite graph which prevents this critical measurement from being part of a maximum matching.

Next, we prove that there are no stealthy attacks containing k that have a smaller cardinality. In this regard, for an attack containing k to be stealthy, it must prevent a critical set, in which k exists, from being part of a maximum matching over the critical sets - system measurements bipartite graph. To this end, a critical set would be excluded from a maximum matching in two cases: 1) if all the measurements corresponding to this critical set are attacked, or 2) if all the measurements corresponding to this critical set are part of a different matching, which assigns these measurements to other critical sets.

In the first case, considering attacking all the measurements in a critical set, then attacking the critical set that has the fewest number of measurements – as stated in this theorem – corresponds to the minimum cardinality attack.

As for the second case, if a measurement k' in a critical set containing k is matched – as part of a maximum matching – to another critical set (we denote this set by $\mathcal{C}^p$), then measurement p must be attacked since, otherwise, $\mathcal{C}^p$ would have been matched to p sparing k to be matched to another critical set to maximize the cardinality of the matching. In other words, matching a critical set $\mathcal{C}^p$ with a measurement $k' \neq p$ while p is not attacked is contradictory to the assumption that this matching is maximum. As a result, for a critical set $\mathcal{C}$, such that $k \in \mathcal{C}$, to be discarded from the maximum matching, every measurement in $\mathcal{C}$ must be matched to another critical set. This implies that at least one measurement of each of these critical sets is attacked. Thus, the number of attacked measurements will be at least equal to the number of measurements within $\mathcal{C}$ for the attack to be stealthy. Consequently, the stealthy attack containing k that has the lowest cardinality corresponds to attacking only the measurements within the critical set containing k that has the lowest cardinality. □

Solving *Problem 1* will also facilitate solving another key SDIA problem, referred to as *Problem 2*, and stated as follows.

Problem 2: What is the SDIA with the lowest cardinality? In other words, which SDIA is a solution to:

$$\begin{aligned} &\min_{\boldsymbol{a}} ||\boldsymbol{a}||_0, \\ &\text{subject to: } \boldsymbol{a} = \boldsymbol{Hc}. \end{aligned} \tag{3.7}$$

Similarly to *Problem 1*, the solution to *Problem 2* also provides a vulnerability assessment of the system against SDIAs. In fact, *Problem 1* focuses on finding the security index associated with each measurement. On the other hand, *Problem 2* focuses on the system as a whole by focusing on finding, in general, the sparsest data injection attack which can target the system and be stealthy. This corresponds to a security index for the whole system. Indeed, this security index reflects the amount of effort that an attacker must put to potentially launch an SDIAs against the system. A low security index shows that, even when manipulating a small set of measurements, the attack can be stealthy. In contrast, a high security index reflects the robustness of the system against SDIAs since the attacker would need to concurrently manipulate a large number of measurements to potentially launch a successful SDIA.

The solution to *Problem 2* is provided in Proposition 1.

Proposition 1. *The stealthy attack with the lowest cardinality corresponds to attacking the smallest critical set.*

Proof. This proof follows directly from the proof of Theorem 5. Indeed, since the stealthy attack containing measurement k that is of smallest cardinality corresponds to the critical set of lowest cardinality containing k, then searching for the global stealthy attack of lowest cardinality can be limited to only critical sets. Based on this fact, the stealthy attack of lowest cardinality is the one in which the measurements in the critical set of lowest cardinality are the only measurements that are attacked (the only measurements having nonzero corresponding elements in the attack vector $\boldsymbol{a}$). □

Here, we note that the solutions to *Problem 1* and *Problem 2* may not be unique.

Example 2. *For example, by inspecting the critical sets in Table* 3.1*, we can solve* Problem 1 *and* Problem 2 *for the IEEE 14-bus system shown in Fig.* 3.1*. With regard to* Problem 1*, the results of Theorem* 5 *can be readily applied to find the minimum stealthy attack containing a certain measurement k. For example, the minimum stealthy attack containing measurement I_4 corresponds to attacking $\mathcal{C}^{I_3} = \{I_3, I_2, I_4\}$, since that is the critical set of smallest cardinality containing I_4. As for* Problem 2*, the stealthy attack of lowest cardinality is one in which either $\mathcal{C}^{F_{15}} = \{F_{15}, I_7\}$, $\mathcal{C}^{I_6} = \{I_6, I_{11}\}$, or $\mathcal{C}^{I_9} = \{I_9, I_{11}\}$ are attacked. As such, the minimum possible cardinality of a stealthy attack for this IEEE 14-bus system is* 2*. To find such a stealthy attack, the basis of the null space can be found for matrices $\boldsymbol{H}^{-(\mathcal{C}^{F_{15}})}$, $\boldsymbol{H}^{-(\mathcal{C}^{I_6})}$, or $\boldsymbol{H}^{-(\mathcal{C}^{I_9})}$. We refer to these vectors as $\boldsymbol{n}^{F_{15}}$, $\boldsymbol{n}^{I_6}$, and $\boldsymbol{n}^{I_9}$, respectively. As a result, these stealthy attack vectors of minimum cardinality can be obtained as $\alpha\boldsymbol{H}\boldsymbol{n}^{F_{15}}$, $\alpha\boldsymbol{H}\boldsymbol{n}^{I_6}$, or $\alpha\boldsymbol{H}\boldsymbol{n}^{I_9}$, where α is a scalar multiplier.*

Modeling SDIA Defense Strategies

The knowledge acquired from our introduced graph-theoretic framework enables the derivation of adequate defense policies which can thwart potential SDIAs. In this regard, next, two fundamental widely-studied problems for defending the system against SDIAs are presented and investigated in *Problem 3* and *Problem 4*.

Problem 3: What is the minimum set of measurements that need to be protected (i.e. made immune to SDIAs) to guarantee no SDIAs can be successful?

The solution to this problem enables finding a minimum-cost defense strategy to thwart all potential SDIAs. Hence, this makes the system robust against all possible SDIAs. However, even though the solution to this problem provides the minimum-cost defense strategy (assuming that protecting each measurement is equally costly), for a practically large power system with several thousand buses, such a defense strategy is likely to exceed any practical security budget.

The solution to *Problem 3* is presented in Theorem 6.

Theorem 6. *The minimum set of measurements that must be protected to guarantee that no SDIAs can be successful corresponds to protecting all measurements in $\mathcal{M}^C$, i.e. all measurements that are part of the original assignment function forming the spanning tree over the power system.*

Proof. By Theorem 4, for an attack to be stealthy, it must lead to a critical set not to be matched as part of a maximum matching over the critical sets - system measurements bipartite graph. Hence, to guarantee that no attack can be stealthy, all critical sets must be guaranteed to be matched. Thus, the minimum number of measurements to be protected must be at least equal to the number of critical sets, which is equal to the number of measurements in $\mathcal{M}^C$. In this regard, protecting every measurement $m \in \mathcal{M}^C$ results in protecting the minimum possible number of measurements which guarantees that $\mathcal{C}^m$ can be matched to m for all $m \in \mathcal{M}^C$, hence, guaranteeing that no stealthy attack can be successfully carried out.

This proof can also be carried out equivalently using the techniques of linear algebra. Indeed, protecting all the measurements in $\mathcal{M}^C$ will guarantee that these measurements will be part of the Jacobian matrix $\boldsymbol{H}$. Since these measurements form a spanning tree over the power system, their rows in $\boldsymbol{H}$ are linearly independent. As such, let $\boldsymbol{H}^C$ be the Jacobian matrix corresponding only to measurements in $\mathcal{M}^C$, then $\boldsymbol{H}^C\boldsymbol{c} = \boldsymbol{0}$ has no solution other than $\boldsymbol{c} = \boldsymbol{0}$. The rows of $\boldsymbol{H}^C$ are a subset of the rows of $\boldsymbol{H}$. As such, one cannot find an attack vector $\boldsymbol{a} = \boldsymbol{Hc}$ such that all the elements of $\boldsymbol{a}$ corresponding to the rows of $\boldsymbol{H}^C$ are zero. Hence, one cannot find a stealthy attack $\boldsymbol{a} = \boldsymbol{Hc}$ which does not attack the measurements in $\mathcal{M}^C$. As a result, protecting these measurements will guarantee that no stealthy attack can be carried out. □

Here, the minimum defense set, solution to *Problem 3*, might not be unique. In other words, the set $\mathcal{M}^C$ might not be the only minimum set of measurements which, when defended, makes the system immune to SDIAs. However, characterizing a solution to this problem provides important information regarding the size of investments needed to make a power system immune to SDIAs. In this regard, regardless of how high the number of measurements in an N-bus system is, the number of measurements that must be protected to render the system immune to SDIAs is always equal to $N - 1$. As such, by assessing the costs of reinforcing the security of each measurement unit, the solution to *Problem 3* enables the calculation of the cost needed to make the system robust against SDIAs. However, as the solution implies, for practical power systems, securing this number of measurements might exceed practical budget constraints.

Example 3. *Applying the results in Theorem* 6 *to our treated IEEE 14-bus system case analysis, protecting the measurements in the first column of Table* 3.1 *is the set of measurements of minimal cardinality which when protected renders the IEEE 14-bus system in Fig.* 3.1 *immune to SDIAs.*

Theorem 4 and the solutions to *Problem 1*, *Problem 2*, and *Problem 3* can be used to solve *Problem 4* which was proposed in [29] and which is presented next. The solution to *Problem 4* in [29] was derived based on an l_1 relaxation of the corresponding optimization problem which leads to approximate, rather than generally accurate solutions.

Problem 4: What is the minimum set of measurements to protect as to force the attacker to manipulate at least τ_a measurements to stay stealthy?

As discussed in *Problem 3*, making the system completely robust against SDIAs may be very costly and exceed any practical budgetary constraints. As a result, rather than considering all theoretically possible SDIAs, the solution to *Problem 4* focuses on defending the system against a large subset of practical SDIAs in which the attacker's limited resources prevents its attack vector's cardinality from exceeding τ_a. In other words, an attacker might not be able to concurrently comprise more than τ_a measurement units. This, hence, enables defending the system against a practically large subset of potential SDIAs. In addition, the solution to this problem allows using the knowledge about the resources of potential attackers – which can be potentially acquired from historical data – to compute adequate defense policies against such attacks.

The solution to *Problem 4* is presented in Proposition 2.

Proposition 2. *A minimum set of measurements to protect so that no attack with cardinality* $||\boldsymbol{a}||_0 < \tau_a$ *can be stealthy, corresponds to protecting one distinct measurement from each critical set whose cardinality is less than* τ_a.

Proof. Solving *Problem 4* entails ensuring that all critical sets of cardinality smaller than τ_a are part of the maximum matching. Hence, when one distinct measurement in each of these sets is secured, it is ensured that these critical sets will be part of a maximum matching over the critical sets - system measurements bipartite graph. As a result, additional measurements would need to be attacked to target critical sets of higher cardinality, if a stealthy attack were to be found, which would require the attacker to manipulate more than τ_a measurements. Hence, the solution to *Problem 4* is a direct result of Theorem 6 but by considering critical sets that have cardinality smaller than τ_a rather than all critical sets, as is the case in Theorem 6. As such, the rest of the proof of Proposition 2 follows directly from the proof of Theorem 6. □

This result is very important since it allows the defender to build on some knowledge that it has about the capacity and resources of the attacker, to build a corresponding defense policy. In other words, knowing that the attacker does not have the capacity to concurrently manipulate more than τ_a measurements enables the defender to focus on defending a smaller set of measurements rather than aiming to thwart any theoretically possible SDIA. This can lead to a significant reduction in the needed resources for such a defense since, as shown in the solution of *Problem 3*, the latter defense policy requires committing a large volume of resources which can exceed practical constraints.

Example 4. *For our studied IEEE 14-bus system, consider that* $\tau_a = 3$. *This indicates that a set of measurements to protect must be found to ensure that no attacker can have a successful stealthy* *attack by attacking less than 3 measurements. The critical sets that have cardinality lower than 3 are $\mathcal{C}^{F_{15}}$, $\mathcal{C}^{I_6}$, and $\mathcal{C}^{I_9}$ which all have a cardinality of* 2. *Now, we consider a distinct measurement in each of these three sets, such that I_7, I_6, and I_9. As a result, $\{I_7, I_6, I_9\}$ is a minimum set of measurements which, when defended, no stealthy attack vector of cardinality less than $\tau_a = 3$ can be successfully launched.*

As such, showing that SDIAs are a subset of our introduced observability attacks, enables using our proposed graph-theoretic framework to model, understand, and thwart such types of cyber-physical attacks. Indeed, the four problems that we have discussed show the way in which our developed framework enables analytical characterization of the solutions to these various well-studied SIDA problems. Such analytical characterization allows assessing the vulnerability of the system against SDIAs as well as deriving adequate defense strategies.

3.5 Summary and Future Outlook

In this chapter, we have introduced a novel graph-theoretic framework which enables a fundamental modeling of observability attacks targeting power systems and have proven that the widely-studied stealthy data injection attacks are a special case of such observability attacks. Based on this proposed framework, we have characterized the analytical solutions to various central observability and data injection attack problems. These solutions aim at capturing potential attack strategies as well as suggesting defense policies to thwart such attacks. In this respect, we have shown that our derived framework enables characterization of the sparsest stealthy attack as well as the sparsest stealthy attack including a certain measurement. With respect to defense policies, we have shown that our graph-theoretic framework enables the analytical characterization of the minimum measurement set which when defended guarantees thwarting any potential stealthy attack as well as the minimum set of measurements whose defense guarantees that no attack below a certain cardinality can be stealthy.

The proposed graph-theoretic framework provides a general analytical tool using which a wide set of key observability attacks and data injection attacks problems can be modeled and analyzed, and is not limited to the set of problem examples which are studied in this chapter. For example, the problem of characterizing the sparsest stealthy attack containing a certain measurement can be extended to studying the sparsest stealthy attack containing a certain set of measurements. Using our proposed framework, a solution approach can be investigated to potentially derive analytical solutions to this critical problem. The solution of this problem enables a risk assessment of the power system by quantifying the risk of having a vulnerable set of measurements and the way that such a vulnerability can be leveraged by an intelligent malicious attacker. Along the same lines, for security assessment, a central problem is quantifying the sparsest stealthy attack possible when a certain set of measurements is defended. The solution to this problem enables assessment of the effectiveness and impact of an implemented defense strategy. This problem has been formalized in [29]. However, the proposed solution approach in [29] relied on an l_1 relaxation of the original optimization problem formulation which leads to approximate numerical solutions. However, our introduced graph-theoretic framework can be used to attempt the characterization of analytical solutions to this problem.

Beyond these one-sided attack and defense problems, the ability to analytically characterize attack and defense policies using the proposed framework allows studying problems that involve interactions between attackers and defenders from a game-theoretic perspective. Such analyses can account for the opponent's potential attack or defense strategies when designing, respectively, defense policies or attack vectors. As a result, such analyses allow the modeling and investigation of practical competitive attack vs. defense settings. This enables studying the effects of sophisticated observability attacks and data injection attacks on the system as well as the impact of proposed defense strategies within various application domains such as electricity markets, congestion management, and contingency analysis, among others, while also taking the application of our framework beyond the domain of power systems which motivated this study.

Chapter 4

Data Injection Attacks on Smart Grids with Multiple Adversaries

4.1 Introduction

With the evolution of the traditional power system to a more interactive CPS, *data injection attacks* have recently emerged as an exceedingly malicious type of cyber-attacks which can target the grid. Using data injection, malicious adversaries can target the state estimator of a power system, by targeting a number of measurement units, in order to alter the estimate of the real-time system state [29, 76].

Data injection can significantly impact the overall well-being of the power system by targeting the state estimator, an integral component of the grid which is used by the system operator to monitor, protect, control, and economically operate the system [29, 76]. Using data injection attacks, malicious adversaries can achieve a variety of goals that range from compromising the security of the grid to impeding the real-time operation of the system or making financial profit through energy prices manipulation. Data injection attacks are inherently challenging due to their stealthiness which makes the task of detecting them highly challenging [29]. In fact, data injection attacks can modify the estimation process while remaining unnoticed by the operator.

Recently, data injection attacks have attracted significant attention [29, 74, 76, 78, 93]. The work in [76] introduces a data injection scheme that can evade detection when compromising a number of measurements. The authors in [29] propose an optimal data injection scheme and derive an optimized subset of measurements that can be defended to face this attack. The work in [78] targets coordinated attacks and discusses efforts for detecting those attacks. An analysis of the economic effects of data injection on energy markets is discussed in [74]. In [93], a zero-sum game is formulated between an attacker and a defender in which the attacker modifies an estimated line flow to manipulate prices.

While interesting, this existing body of literature [29, 74, 76, 78, 93] has primarily focused on data injection attacks with a single attacker and assume no cost for attacking or defending the system. However, in practice, due to their potential profitability and stealthiness, data injection attacks can occur concurrently from *multiple adversaries* that can target various state estimation sensors. Due to the networked nature of the smart grid, the manipulation of measurements in one part of the system, by an adversary, has an overall effect on the system as a whole. Hence, an attack executed by one attacker does not only impact the grid's performance, but it also affects the benefits of the other attackers. Such an interdependence can be, on the one hand, beneficial to the grid for cases in which the different simultaneous attacks mitigate the severity of one another. On the other hand, multiple attacks can lead to a more severe combined effect on the electric grid thus further impacting its overall performance. Clearly, there is a necessity for a strategic modeling framework to analyze and understand these interdependencies between attackers. Remarkably, to our best knowledge, no work has previously analyzed the case of multiple adversaries.

The main contribution of this chapter is to introduce novel game-theoretic approaches to analyze data injection attacks that involve a defender and *multiple adversaries*. In this regard, two approaches are proposed. In the first approach, we formulate the problem as a Stackelberg game in which the defender (i.e. grid operator) acts as a leader having the ability to anticipate the actions of the adversaries, which act as followers, prior to selecting a subset of measurements to defend. The defender's goal is to reduce the effect of potential attacks on the system while optimizing a utility that captures both the benefits and costs of the chosen defense strategy. In response to the leader's strategy, the attackers play a noncooperative strategic game in which each attacker chooses its optimal attack scheme in order to maximize the tradeoff between the benefits, obtained from prices manipulation, and costs associated with the attack. We prove the existence of a generalized Nash equilibrium for the attacker's game and we study the existence and properties of the overall game's Stackelberg equilibrium. To solve the game, we propose a distributed learning algorithm which we prove to converge to a solution of the game using limited information that can be available to the players. In the second approach, it is assumed that the defender cannot anticipate the actions of the adversary. To this end, we use the framework of satisfaction equilibrium [151] through a proposed hybrid satisfaction equilibrium - Nash equilibrium game model. In this approach, rather than anticipating the attackers' response and playing a strategy that optimizes its objective function, the defender seeks a defense strategy that meets a certain performance constraint. We introduce an equilibrium concept of this game and propose a search algorithm to find this equilibrium.

The performance of the proposed frameworks is assessed via numerical simulations using the IEEE 30-bus test system. Through the numerical analysis, we simulate the strategic interactions between the attackers and defender over the test system. We show that by defending a minimal number of measurements, the grid operator can enforce an equilibrium in which the attackers have no effect on the system. In addition, our results shed the light on the adversarial behavior in between the attackers. The results show that, at equilibrium, the attackers can choose attack strategies that cancel each other out resulting in no effect on the grid. In addition, we analyze the equilibrium of the hybrid game and compare the obtained solution to the Stackelberg one. In this regard, we define a "price of information" index which compares the utility achieved by the defender under the Stackelberg model and the hybrid model. Hence, it reflects the loss that the defender can be subject to due to lack of information about the potential reactions of the attackers to the different defense strategies available to the defender.

The rest of this chapter is organized as follows. Section 4.2 presents the system model and problem formulation. Section 4.3 introduces the formulated Stackelberg game and associated solution. Section 4.4 introduces our proposed hybrid model and its solution concept. Section 4.5 provides numerical results while a summary of the work in this chapter is presented in Section 4.6.

4.2 System Model and Problem Formulation

4.2.1 Energy Markets

Competitive energy markets' architectures are often based on day ahead (DA) and real time (RT) markets [191]. In the DA market, the system operator issues hourly-based locational marginal prices (LMPs), μ^{DA}, for the next operating day based on the DA energy bids submitted by the participants [191]. The market clearing process is performed by the grid operator through the solution of a linearize Optimal Power Flow (DCOPF) which returns the optimal dispatch for each of the generators participating in the market and the DA LMP at each bus. The most commonly used DCOPF formulation is as follows [191]:

$$\min_{\boldsymbol{P}} \sum_{i=1}^{G} C_i(P_i), \tag{4.1}$$

$$\text{s.t.} \sum_{i=1}^{N} (P_i - D_i) = 0, \tag{4.2}$$

$$P_i^{\min} \leqslant P_i \leqslant P_i^{\max}, \forall i \in \{1, \cdots, G\}, \tag{4.3}$$

$$\sum_{i=1}^{N} (P_i - D_i)\chi_{l,i} \leqslant F_l^{\max}, \forall l \in \{1, \cdots, L\}, \tag{4.4}$$

$$-\sum_{i=1}^{N} (P_i - D_i)\chi_{l,i} \leqslant F_l^{\max}, \forall l \in \{1, \cdots, L\}, \tag{4.5}$$

where N, G and L represent, respectively, the number of buses, generators, and transmission lines. C_i corresponds to the offer of generator i while P_i and D_i are, respectively, the power injection and load at a bus i. Thus, $P_i = 0$ ($D_i = 0$) corresponds to the case in which no generator (or load) is connected to bus i. The upper and lower limits on generator i's output are denoted by $P_i^{\min}$ and

$P_i^{\max}$. Constraints (4.4) and (4.5) place a limit, $F_l^{\max}$, on the level of power that can flow over line l. A reference direction is assigned to the power flow over each transmission line. In this regard, a power flow opposing its assigned reference direction is represented by a negative quantity. Hence, constraints (4.4) and (4.5) correspond to the thermal limit of a line in its reference and opposite directions respectively. $\boldsymbol{X}$ is the generation shift factor matrix which defines the sensitivity of the power flow over each line, $\boldsymbol{F}$, to changes in power injection, $\boldsymbol{P}$, at each bus:

$$\boldsymbol{F}_{(L\times 1)} = \boldsymbol{X}_{(L\times G)} \times \boldsymbol{P}_{(G\times 1)}. \tag{4.6}$$

Therefore the sensitivity of the flow over line l to a change in power injection at bus i is denoted by $\chi_{l,i}$.

In the RT market, actual real-time operating conditions estimated using the state estimator, in lieu of the predictions in DA, are used through an ex-post model to compute the RT LMPs, μ^{RT} [191]. An incremental DCOPF is used to compute the RT LMPs and can be formulated as follows [191]:

$$\min_{\boldsymbol{\varDelta P}} \sum_{i=1}^{G} C_i^{RT}(\varDelta P_i), \tag{4.7}$$

$$\text{s.t. } \sum_{i=1}^{N} (\varDelta P_i) = 0, \tag{4.8}$$

$$\varDelta P_i^{\min} \leqslant \varDelta P_i \leqslant \varDelta P_i^{\max}, \forall i \in \{1, \cdots, G\}, \tag{4.9}$$

$$\sum_{i=1}^{N} (\varDelta P_i)\chi_{l,i} \leqslant 0, \forall l \in \mathcal{C}^+, \tag{4.10}$$

$$-\sum_{i=1}^{N} (\varDelta P_i)\chi_{l,i} \leqslant 0, \forall l \in \mathcal{C}^-, \tag{4.11}$$

where C_i^{RT} is the RT offer of generator i which is computed using its RT power output and its associated offer curve [191]. $\mathcal{C}^+$ ($\mathcal{C}^-$) is the set of congested lines which flow is in (opposite to) their reference directions. $\varDelta P_i^{\max}$ and $\varDelta P_i^{\min}$ define a bandwidth which is employed to allow for solution tolerance. In practice, here, we typically [192] set $\varDelta P_i^{\min} = -2$ MW and $\varDelta P_i^{\max} = +0.1$ MW. A proposed alternative to using this feasibility bandwidth is also available in [192].

Thus, the DA and RT LMPs at each bus, i, are computed using the DA and ex-post DCOPFs. The generated LMPs reflect, both, the incremental cost of energy at bus i and the congestion cost associated with the contribution of this bus to the system congestion. A line is said to be congested if the flow of power over it reaches its maximum limit. The DA and RT LMPs at bus i are given by:

$$\mu_i^{DA} = \lambda_0 + \sum_{l=1}^{L} (\lambda_l^{DA,-} - \lambda_l^{DA,+}) \chi_{l,i}, \tag{4.12}$$

$$\mu_i^{RT} = \lambda_0 + \sum_{l \in \mathcal{C}_l} (\lambda_l^{RT,-} - \lambda_l^{RT,+}) \chi_{l,i}. \tag{4.13}$$

$\mathcal{C}_l \triangleq \{\mathcal{C}^+ \cup \mathcal{C}^-\}$ is the set of congested lines, in RT, obtained using the state estimator. $\mathcal{C}_l \subseteq \mathcal{L}$ where $\mathcal{L} = \{1, \cdots, L\}$ is the set of all lines. λ_0 corresponds to the Lagrange multiplier associated with the energy balance constraints (4.2) and (4.8). $\lambda_l^{DA,+}$ and $\lambda_l^{DA,-}$ are the Lagrange multipliers corresponding, respectively, to constraints (4.4) and (4.5) for line $l \in \mathcal{L}$ whereas $\lambda_l^{RT,+}$ and $\lambda_l^{RT,-}$ are the Lagrange multipliers corresponding, respectively, to constraints (4.10) and (4.11) for line $l \in \mathcal{C}_l$. When $l \in \mathcal{L}$ but $l \notin \mathcal{C}_l$, $\lambda_l^{RT,+} = \lambda_l^{RT,-} = 0$. Moreover, when $l \in \mathcal{C}^+$, $\lambda_l^{RT,-} = 0$; while when $l \in \mathcal{C}^-$, $\lambda_l^{RT,+} = 0$.

Computing the RT LMPs relies on the ex-post DCOPF formulation which depends on the output of the state estimator. Hence, data injection attacks targeting the state estimation affects the LMPs in (4.13). Next, we introduce the data attack model.

4.2.2 State Estimation and Data Injection Attacks

A power system state estimator uses multiple power measurements collected throughout the grid to estimate the system states [176]. The relation between the measurement vector, $\boldsymbol{z}$, and the vector of system states, $\boldsymbol{\theta}$, in a linearized state estimation model (DC SE) is expressed as follows:

$$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{\theta} + \boldsymbol{e}, \tag{4.14}$$

where $\boldsymbol{H}$ is the measurement Jacobian matrix and $\boldsymbol{e}$ is the vector of random errors assumed to follow a normal distribution, $N(0, \boldsymbol{R})$. Using a weighted least square (WLS) estimator the estimated system states are given by [176]:

$$\hat{\boldsymbol{\theta}} = (\boldsymbol{H}^T \boldsymbol{R}^{-1} \boldsymbol{H})^{-1} \boldsymbol{H}^T \boldsymbol{R}^{-1} \boldsymbol{z} = \boldsymbol{M}\boldsymbol{z}. \tag{4.15}$$

Using the estimated states, an estimate of the measurement vector, $\hat{\boldsymbol{z}}$, and residuals, $\boldsymbol{r}$, can be calculated as follows [176]:

$$\hat{\boldsymbol{z}} = \boldsymbol{H}\hat{\boldsymbol{\theta}} = \boldsymbol{S}\boldsymbol{z}, \; \boldsymbol{r} = \boldsymbol{z} - \hat{\boldsymbol{z}} = (\boldsymbol{I}_n - \boldsymbol{S})\boldsymbol{z} = \boldsymbol{W}\boldsymbol{z}, \tag{4.16}$$

where I_n is the identity matrix of size $(n \times n)$, and n is the total number of collected measurements.

When data injection attacks *are concurrently carried out by M attackers* in the set $\mathcal{M} = \{1, \dots, M\}$, the collected measurements are modified through the addition of their corresponding attack vectors denoted by $\{\boldsymbol{z}^{(1)}, \boldsymbol{z}^{(2)}, ..., \boldsymbol{z}^{(M)}\}$ resulting in the following altered measurements and residuals:

$$\boldsymbol{z}^{\text{att}} = \boldsymbol{z} + \sum_{i=1}^{M} \boldsymbol{z}^{(i)},\ \boldsymbol{r}^{\text{att}} = \boldsymbol{r} + \boldsymbol{W} \sum_{m=1}^{M} \boldsymbol{z}^{(m)}. \tag{4.17}$$

In the case in which the measurement errors $\boldsymbol{e}$ follow a normal distribution, the WLS estimator is a maximum likelihood estimator of location of the system states [176]. However, the WLS estimator has a zero robustness against outliers. To overcome this drawback, outliers' detection and identification mechanisms are used so that the final state estimate is only based on "good data". The measurement residuals give an indication of the real and unknown measurement errors. By replacing the expression of $\boldsymbol{z}$ from (4.14) in the expression of $\boldsymbol{r}$ in (4.16), the residuals can be expressed in terms of the true errors as follows [176]:

$$\boldsymbol{r} = \boldsymbol{W}\boldsymbol{e} \tag{4.18}$$

Thus, an analysis of the residuals allow for the detection and identification of bad data (outliers). In this respect, *bad data detection* corresponds to determining whether the collected measurement set contains bad data or not. On the other hand, *bad data identification* corresponds to identifying which measurements may contain bad data. One should note here that outliers can stem from data injection as well as other reasons such as meter biases or communication link failures [176].

Bad data detection is typically performed using a test known as the Chi-squares test over the sum of the squares of the residuals [76, 176]. In fact, when the measurement errors vector $\boldsymbol{e}$ is assumed to follow a normal distribution, $||\boldsymbol{r}||_2^2 = \sum_{i=1}^{n} r_i^2$ follows a χ^2 distribution with $n - N_\theta$ degrees of freedom where N_θ is the number of states to be estimated [176]. Hence, for a measurement set to be considered free from bad data, the residuals must satisfy $||\boldsymbol{r}||_2 \leq \tau$ where τ is a detection threshold [76, 176]. In this respect, in the presence of M attackers, and since $||\boldsymbol{r}^{\text{att}}||_2 = ||\boldsymbol{r} + \boldsymbol{W}\sum_{m=1}^{M} \boldsymbol{z}^{(m)}||_2$ as shown in (4.17), each attacker $m \in \mathcal{M}$ should regulate $\boldsymbol{W}\boldsymbol{z}^{(m)}$ to keep the effect of the attacks on the residuals low to minimize the chance of being detected as outliers [76].

In the case where the Chi-squares test indicates the presence of bad data, various bad data identification and elimination tests can be employed such as the largest normalized residual test, or the hypothesis testing identification (HTI), among others, to identify and eliminate the outliers [176].

In our model, each attacker $m \in \mathcal{M}$ aims at manipulating RT LMPs, μ^{RT}, to make financial benefit via virtual bidding. Using virtual bidding, entities that do not own any physical generation nor load can engage in the energy market settlements by submitting so-called virtual supply and demand offers. Since these energy offers are virtual, an entity offering to buy (sell) virtual power at a given bus in DA is required to sell (buy) that same amount of power at the same bus in RT. Using such virtual bids, the grid operator aims at promoting liquidity in the energy market while, on the other hand, virtual bidders aim to reap financial profit from possible mismatch between the DA and RT LMPs [191]. Using a data injection attack, a virtual bidder can, thus, manipulate the RT LMPs to create a lucrative mismatch with respect to their DA counterparts. On the other hand, to achieve pricing integrity, the system operator aims at protecting the system against such attacks. The strategic interactions between the attackers and the defender (i.e. system operator) are modeled and analyzed next.

4.3 Attackers and Defender Strategic Interaction

Data injection attacks involve interactions between M attackers, which are virtual bidders, and one defender consisting of the grid operator. The defender chooses a set of measurements to secure against potential attacks aiming at decreasing the aggregate effect of the multiple attacks on the system. Securing measurements to block data injection attacks is discussed in [29] and the techniques that can be implemented for securing those measurements are referred to in [29, 93], and [193]. In [29] and [193], protection of measurements is performed through encryption of the associated sensors while, in [93], protection of measurements is performed through the implementation of a set of highly secured measurement units which are assumed to provide more robustness against data attacks. In any case, in practice, attackers can have the ability to detect or watch which measurements are secured by the defender. In fact, a placement of new measurement units can be physically noticeable by the attackers while encrypting the measurement sensors' outputs can also be observed by a hacker attempting to read these outputs.

After observing which measurements are secured, each of the M attackers can choose, accordingly, to carry out a data injection attack over a subset of measurements. Given the networked nature of the electric grid, the actions and payoffs of the different attackers are interconnected thus motivating a game-theoretic approach [146].

Hence, given that the defender acts first and the attackers react to the observed defender's action, the interaction between the defender and attackers is hierarchical. Thus, we formulate a single leader, multi-follower *Stackelberg game* [146] between the defender and the M attackers to capture and analyze the strategic interaction between the two. In this game, the defender acts as a leader who selects a set of measurements to defend while the adversaries interact with one another using a followers noncooperative game to identify the optimal attack in response to the strategy of the defender. By observing or predicting the ways in which the attackers react to its defense strategy, the leader chooses its optimal defense action. Next, we first analyze and solve the followers game and then find the Stackelberg solution.

4.3.1 Attackers' Noncooperative Game Formulation

We formulate a strategic noncooperative game to analyze the optimal decision making of the M attackers in response to any arbitrary defender strategy. This game is formulated in its normal form as follows: $\Xi = \langle \mathcal{M}, (\mathcal{Z}^{(i)})_{i\in\mathcal{M}}, (U_i)_{i\in\mathcal{M}} \rangle$, where $\mathcal{M}$ is the set of M attackers, $\mathcal{Z}^{(i)}$ is the set of actions (attack vectors $\boldsymbol{z}^{(i)} \in \mathcal{Z}^{(i)}$) available to attacker $i \in \mathcal{M}$, and U_i is the utility function of attacker i. Thus, each attacker, $m \in \mathcal{M}$, selects an attack vector, $\boldsymbol{z}^{(m)} \in \mathcal{Z}^{(m)}$ that maximizes its utility U_m. Let $\mathcal{K}_m$ denote the subset of measurements that m can attack. Then, $\mathcal{Z}^{(m)}$ can be represented by a column vector with elements equal to 0 except for those in $\mathcal{K}_m$ which can take values within a compact range reflecting the range of magnitude of the attack.

The utility function of each attacker reflects the financial benefit obtained by virtual bidding. Using virtual bidding, each attacker m buys and sells P_m MW at, respectively, buses i_m and j_m in DA while, conversely in RT, attacker m sells and buys P_m MW at, respectively, buses i_m and j_m. Thus, the goal of attacker $m \in \mathcal{M}$ is to optimize the following (Problem 1):

$$\max_{\boldsymbol{z}^{(m)} \in \mathcal{Z}^{(m)}} U_m(\boldsymbol{z}^{(m)}, \boldsymbol{z}^{-(m)}) = \left[(\mu_{i_m}^{RT} - \mu_{i_m}^{DA}) + (\mu_{j_m}^{DA} - \mu_{j_m}^{RT})\right] P_m - c_m(\boldsymbol{z}^{(m)}), \tag{4.19}$$

$$\text{s.t.} \quad \|\boldsymbol{W}\boldsymbol{z}^{(m)}\|_2 + \sum_{l=1, l\neq m}^{M} \|\boldsymbol{W}\boldsymbol{z}^{(l)}\|_2 \leqslant \epsilon_m, \tag{4.20}$$

where $c_m(\boldsymbol{z}^{(m)})$ is the cost of attack, and $\boldsymbol{z}^{-(m)}$ denotes the strategy vector of all players except m. The number of measurements that can be attacked concurrently by m as well as the attack levels (the level of modification of a measurement) are limited by $\mathcal{Z}^{(m)}$. Since $||\boldsymbol{r}^{\text{att}}||_2 = ||\boldsymbol{r} + \boldsymbol{W}\sum_{m=1}^{M} \boldsymbol{z}^{(m)}||_2 \leq ||\boldsymbol{r}||_2 + ||\boldsymbol{W}\boldsymbol{z}^{(m)}||_2 + \sum_{l=1,l\neq m}^{M} ||\boldsymbol{W}\boldsymbol{z}^{(l)}||_2$, $m \in \mathcal{M}$ chooses $\boldsymbol{z}^{(m)}$ as in (4.20), where ϵ_m is a chosen threshold, to minimize the chance of the attack of being detected as outliers.

4.3.2 Attackers' Game Analysis

Due to the networked nature of the electric grid, the m attackers' actions are interdependent. In fact, by altering a set of measurements, an attacker manipulates the whole estimation outcome and, thus, affects the actions as well as the payoffs of the other attackers. In the event of concurrent attacks by M attackers, the resulting estimates, $\hat{\boldsymbol{z}}^{att}$, are computed as follows:

$$\hat{\boldsymbol{z}}^{att} = \hat{\boldsymbol{z}} + \sum_{m=1}^{M} \boldsymbol{S}\boldsymbol{z}^{(m)} \Rightarrow \Delta\hat{\boldsymbol{z}} = \sum_{m=1}^{M} \boldsymbol{S}\boldsymbol{z}^{(m)}, \tag{4.21}$$

where $\Delta\hat{\boldsymbol{z}}$ represents the change in the generated estimates due to the M attacks. Likewise, the overall change in the measurement residuals due to the M attacks can be expressed as follows:

$$\Delta\boldsymbol{r} = \boldsymbol{W}\sum_{m=1}^{M} \boldsymbol{z}^{(m)}. \tag{4.22}$$

Consequently, the various attackers in the system can impair the ability of attacker m to successfully manipulate a targeted measurement z_i as expressed in Remark 2.

Remark 2. *Depending on the targeted measurements, the collective impact of the M attacks can be either constructive for the attackers by helping each one of them to achieve its goal, or destructive, attenuating the global effect of these attacks on the system.*

In fact, considering the case of two attackers in which attacker 1's (attacker 2's) aim is to increase the estimated flow, $\hat{z}_i$ ($\hat{z}_j$), over a line l_i (l_j) in order to create a false congestion. The objective of attacker 1 (attacker 2) is, hence, to achieve $\Delta\hat{z}_i \geqslant F_{l_i}^{\max} - \hat{z}_i$ ($\Delta\hat{z}_j \geqslant F_{l_j}^{\max} - \hat{z}_j$). Following from (4.21), the change introduced to $\hat{z}_i$ and $\hat{z}_j$ by the two attacks is stated as follows:

$$\Delta\hat{z}_i = s_{i,i} z_i^{(1)} + s_{i,j} z_j^{(2)},\ \Delta\hat{z}_j = s_{j,j} z_j^{(2)} + s_{j,i} z_i^{(1)}, \tag{4.23}$$

where $s_{i,j}$ denotes element (i,j) of matrix $\boldsymbol{S}$. When the measurement errors are independent and identically distributed (i.e. $\boldsymbol{R} = \sigma^2 \boldsymbol{I}_n$), $\boldsymbol{S}$ is a symmetric matrix. This property can be proven based on (4.15) and (4.16) through showing that $\boldsymbol{S}^T = \boldsymbol{S}$ when $\boldsymbol{R} = \sigma^2 \boldsymbol{I}_n$. Since $\boldsymbol{S}$ is symmetric, $s_{i,j} = s_{j,i}$. In the event where $s_{i,j} < 0$, both attackers' actions attenuate the effect of one another. In fact, since $s_{i,j} < 0$, $z_j^{(2)}$ ($z_i^{(1)}$) reduces $\Delta\hat{z}_i$ ($\Delta\hat{z}_j$) preventing it from causing any congestion over line l_i (l_j). In the contrary, if $s_{ij} > 0$, each of the attackers' actions would assist the other in achieving its objective. This result can be trivially generalized to the case of M attackers.

Moreover, the payoffs of the different attackers (i.e. virtual bidders) are also significantly interdependent. In fact, as shown next, an attacker can collect financial benefit or endure loses due to the strategies played by other attackers.

Remark 3. *The payoff of each attacker, m, is dependent on the chosen attack strategies of other attackers. Thus, based on its virtual biding nodes, m can achieve a positive or negative payoff depending on attacks carried out by other attackers.*

In this regard, following from (4.19), attacker m's payoff in the presence of M attackers is governed by:

$$\zeta_m = (\mu_{i_m}^{RT} - \mu_{i_m}^{DA}) + (\mu_{j_m}^{DA} - \mu_{j_m}^{RT}). \tag{4.24}$$

Replacing the expressions of the DA and RT LMPs from (4.12) and (4.13) in (4.24) yields:

$$\zeta_m = \sum_{l=1}^{L} [(\chi_{l,j_m} - \chi_{l,i_m}) \times ((\lambda_l^{DA,-} - \lambda_l^{DA,+}) + (\lambda_l^{RT,+} - \lambda_l^{RT,-}))]. \tag{4.25}$$

As a result, following the sign of $(\chi_{l,j_m} - \chi_{l,i_m})$, determined by the choice of virtual bid nodes i_m and j_m, an attack modifying the congestion status of a line l between DA and RT can introduce a positive or negative payoff to attacker m.

4.3.3 Attackers' Game Solution

The attackers' payoff in (4.19) is a function of DA and RT LMPs. These LMPs are indirectly controlled by the attack vector, $\boldsymbol{z}^{(m)}$, which can control the existence of congestion over transmission lines and hence eventually affect the LMPs in (4.12) and (4.13). Thus, (4.19) can be rewritten using (4.12) and (4.13) as:

$$U_m(\boldsymbol{z}^{(m)}, \boldsymbol{z}^{-(m)}) = \zeta_m \, P_m - c_m(\boldsymbol{z}^{(m)}), \tag{4.26}$$

where ζ_m is given by (4.25). By dropping P_m for being a constant, the objective of attacker m is hence to

$$\max_{\boldsymbol{z}^{(m)} \in \mathcal{Z}^{(m)}} \zeta_m - c_m(\boldsymbol{z}^{(m)}). \tag{4.27}$$

We define the two sets of lines $\mathcal{L}_m^+$ and $\mathcal{L}_m^-$ such that $\mathcal{L}_m^+ = \{l \in \mathcal{L} | \chi_{l,j_m} - \chi_{l,i_m} > 0\}$ and $\mathcal{L}_m^- = \{l \in \mathcal{L} | \chi_{l,j_m} - \chi_{l,i_m} < 0\}$. Moreover, let $\mathcal{L}^R$ and $\mathcal{L}^O$, such that $\mathcal{L} = \{\mathcal{L}^R \cup \mathcal{L}^O\}$, be the sets of lines over which the power flows in, respectively, the reference and opposite to reference directions.

Attacker m seeks to congest or decongest lines in a way that maximizes (4.27). In this regard, for a line $l \in \mathcal{L}_m^+$, i.e. $\chi_{l,j_m} - \chi_{l,i_m} > 0$, attacker m profits from creating a congestion over l in the reference direction, causing $\lambda_l^{RT,+}$ to be positive. Thus, m aims at creating a congestion over a line $l \in \{\mathcal{L}_m^+ \cap \mathcal{L}^R\}$. Similarly, for $l \in \mathcal{L}_m^-$, m benefits from causing a congestion over line l in the direction opposite to its reference direction, causing $\lambda_l^{RT,-}$ to be positive. Accordingly, m aims a creating a congestion over a line $l \in \{\mathcal{L}_m^- \cap \mathcal{L}^O\}$. Combining these two observations, attacker m aims at creating congestions over lines $l \in \{(\mathcal{L}_m^+ \cap \mathcal{L}^R) \cup (\mathcal{L}_m^- \cap \mathcal{L}^O)\}$. In a similar manner, an attacker would also seek to remove congestion from a line l in order to set its $\lambda_l^{RT,+}$ or $\lambda_l^{RT,-}$ to zero in a way that maximizes (4.27). To this end, m aims at removing congestions from lines $l \in \{(\mathcal{L}_m^+ \cap \mathcal{L}^O) \cup (\mathcal{L}_m^- \cap \mathcal{L}^R)\}$.

However, due to the presence of measurement errors, an attacker cannot be completely certain that its attack will lead to the creation or removal of congestion over a given line. In fact, given the estimated states in the presence of attack, $\hat{\boldsymbol{\theta}}^{\text{att}}$, the power flow estimates, $\hat{\boldsymbol{F}}^{\text{att}}$, can be obtained using the linear matrix denoted by $\boldsymbol{H}_F$ relating the power flows to the system states: $\hat{\boldsymbol{F}}^{\text{att}} = \boldsymbol{H}_F \hat{\boldsymbol{\theta}}^{\text{att}}$. Using the expressions of $\hat{\boldsymbol{\theta}}$ given by (4.15),

$$\hat{\boldsymbol{F}}^{\text{att}} = \boldsymbol{H}_F \boldsymbol{M}(\boldsymbol{z} + \sum_{i=1}^{M} \boldsymbol{z}^{(i)}) = \hat{\boldsymbol{F}} + \boldsymbol{H}_F \boldsymbol{M} \sum_{i=1}^{M} \boldsymbol{z}^{(i)}. \tag{4.28}$$

Replacing $\boldsymbol{z}$ by its expression given by (4.14) and noting that $\boldsymbol{M}\boldsymbol{H}$ reduces to the identity matrix, $\hat{\boldsymbol{F}}^{\text{att}}$ can be expressed as:

$$\hat{\boldsymbol{F}}^{\text{att}} = \boldsymbol{H}_F \boldsymbol{\theta} + \boldsymbol{H}_F \boldsymbol{M} \boldsymbol{e} + \boldsymbol{H}_F \boldsymbol{M} \sum_{i=1}^{M} \boldsymbol{z}^{(i)}. \tag{4.29}$$

$\boldsymbol{H}_F \boldsymbol{\theta}$ represents the true flow denoted by $\boldsymbol{F}_t$. Given that $\boldsymbol{e} \sim N(\boldsymbol{0}, \boldsymbol{R})$, $\hat{\boldsymbol{F}}^{\text{att}}$ is also a random variable that is also Gaussian distributed with the following expected value and variance:

$$\mathbb{E}[\hat{\boldsymbol{F}}^{\text{att}}] = \boldsymbol{F}_t + \boldsymbol{H}_F \boldsymbol{M} \sum_{i=1}^{M} \boldsymbol{z}^{(i)}, \; V[\hat{\boldsymbol{F}}^{\text{att}}] = \boldsymbol{H}_F \boldsymbol{M} \boldsymbol{R}. \tag{4.30}$$

Given that $\hat{\boldsymbol{F}}^{\text{att}}$ is a vector of random variables, attacker m aims at altering the expected value of $\hat{\boldsymbol{F}}^{\text{att}}$ to achieve, with highest possible probability, the intended congestion creation or removal to maximize (4.26). In other words, to create (or remove) a congestion over a line l, attacker m designs its attack so that $\mathbb{E}[\hat{F}_l^{\text{att}}] \geqslant F_l^{\max} + \delta_m$ (or $\mathbb{E}[\hat{F}_l^{\text{att}}] \leqslant F_l^{\max} - \delta_m$) and aims at maximizing this δ_m to increase its chances for achieving its congestion. Thus, attacker m aims to solve the following optimization problem where $\boldsymbol{S}^F \triangleq \boldsymbol{H}_F \boldsymbol{M}$ (Problem 2):

$$\max_{\boldsymbol{z}^{(m)},\delta_{k_m},\alpha_{k_m}} \sum_{k_m \in \{\mathcal{L}_m^+ \cup \mathcal{L}_m^-\}} (\delta_{k_m} - \gamma \alpha_{k_m}) - c_m(\boldsymbol{z}^{(m)}) \tag{4.31}$$

$$\text{s.t.} \quad \|\boldsymbol{W}\boldsymbol{z}^{(m)}\|_2 + \sum_{l=1, l\neq m}^{M} \|\boldsymbol{W}\boldsymbol{z}^{(l)}\|_2 \leqslant \epsilon_m, \tag{4.32}$$

$$\hat{F}_{k_m} + \boldsymbol{S}_{k_m}^F \boldsymbol{z}^{(m)} + \sum_{p \in \mathcal{M}\setminus\{m\}} \boldsymbol{S}_{k_m}^F \boldsymbol{z}^{(p)} \geqslant F_{k_m}^{\max} + \delta_{k_m} - \alpha_{k_m} \quad \forall k_m \in \{\mathcal{L}_m^+ \cap \mathcal{L}^R\}, \tag{4.33}$$

$$\hat{F}_{k_m} + \boldsymbol{S}_{k_m}^F \boldsymbol{z}^{(m)} + \sum_{p \in \mathcal{M}\setminus\{m\}} \boldsymbol{S}_{k_m}^F \boldsymbol{z}^{(p)} \leqslant -(F_{k_m}^{\max} + \delta_{k_m}) + \alpha_{k_m} \quad \forall k_m \in \{\mathcal{L}_m^- \cap \mathcal{L}^O\}, \tag{4.34}$$

$$\hat{F}_{k_m} + \boldsymbol{S}_{k_m}^F \boldsymbol{z}^{(m)} + \sum_{p \in \mathcal{M}\setminus\{m\}} \boldsymbol{S}_{k_m}^F \boldsymbol{z}^{(p)} \leqslant F_{k_m}^{\max} - \delta_{k_m} + \alpha_{k_m} \quad \forall k_m \in \{\mathcal{L}_m^- \cap \mathcal{L}^R\}, \tag{4.35}$$

$$\hat{F}_{k_m} + \boldsymbol{S}_{k_m}^F \boldsymbol{z}^{(m)} + \sum_{p \in \mathcal{M}\setminus\{m\}} \boldsymbol{S}_{k_m}^F \boldsymbol{z}^{(p)} \geqslant -(F_{k_m}^{\max} - \delta_{k_m}) - \alpha_{k_m} \quad \forall k_m \in \{\mathcal{L}_m^+ \cap \mathcal{L}^O\}, \tag{4.36}$$

$$0 \leq \delta_{k_m} \leqslant \beta F_{k_m}^{\max} \quad \forall \delta_{k_m}, \quad 0 \leq \alpha_{k_m} \leqslant \beta' F_{k_m}^{\max} \quad \forall \alpha_{k_m}, \tag{4.37}$$

where $\boldsymbol{z}^{(m)} \in \mathcal{Z}^{(m)}$. The constraints in (4.37) put some limits on the variables δ_{k_m} and α_{k_m} relative to the corresponding flow limit $F_{k_m}^{\max}$ where β and β' correspond to the fraction of $F_{k_m}^{\max}$ that δ_{k_m} and α_{k_m} can take respectively. Thus, attacker m aims at maximizing δ_{k_m} to increase the chance of creating congestions over lines $k_m \in \{(\mathcal{L}_m^+ \cap \mathcal{L}^R) \cup (\mathcal{L}_m^- \cap \mathcal{L}^O)\}$ and removing congestions from lines $k_m \in \{(\mathcal{L}_m^+ \cap \mathcal{L}^O) \cup (\mathcal{L}_m^- \cap \mathcal{L}^R)\}$.

On the other hand, due to resource limitation, an attacker cannot concurrently achieve all its favorable congestions. Thus, the α_{k_m} variables are relaxation variables to ensure feasibility of the optimization problem. However, this relaxation is accompanied with a penalty factor, γ, present in the objective function which reflects a decrease in the objective function of the attacker for the case in which a beneficial congestion creation or removal is not performed. Hence, when such a congestion manipulation is feasible, this penalty factor ensures that the attacker has a high incentive to perform this congestion manipulation.

Moreover, similarly to (4.19), $c_m(\boldsymbol{z}^{(m)})$ is the cost associated with the attack. This cost function can be represented as a scaled norm of the attack vector, where κ_m is the scaling factor and m_l is the length of vector $\boldsymbol{z}^{(m)}$:

$$c_m(\boldsymbol{z}^{(m)}) = \kappa_m \sum_{i=1}^{m_l} (z_i^{(m)})^2. \tag{4.38}$$

Following this formulation, one can see that the constraints of the optimization problems of each of the attackers are coupled. In other words, the strategy space of each attacker depends on the strategies selected by the other attackers. Games in which the constraints of the different players are coupled are known as *generalized Nash equilibrium problems (GNEP)*. A widely used solution concept of these games is known as the *generalized Nash equilibrium (GNE)* which is defined as follows [194]:

Definition 10. *In a game of N players in which the control variable, i.e. strategy, of each player $i \in \{1, ..., N\}$, is denoted by $\boldsymbol{x}^i \in \mathbb{R}^{n_i}$ and utility function is denoted by $U_i : \mathbb{R}^{n_1+\dots+n_N} \to \mathbb{R}$, a GNE is a state of the game in which each player aims at*

$$\max_{\boldsymbol{x}^i} \quad U_i(\boldsymbol{x}^i, \boldsymbol{x}^{*,-i}) \quad s.t. \quad (\boldsymbol{x}^i, \boldsymbol{x}^{*,-i}) \in \mathcal{X}, \tag{4.39}$$

where $\boldsymbol{x}^{*,-i}$ denotes the optimal strategies of all other players except for player i and $\mathcal{X}$ is the shared strategy space in between the N players. In other words, as a response to optimal chosen actions of other players, a player aims at choosing the strategy, in the restricting subset dictated by the choice of the other players, that maximizes its own utility.

We next prove the existence of a GNE for the attackers' game.

Theorem 7. *The attackers' game has at least one GNE.*

Proof. Since δ_{k_m} and α_{k_m} are linear functions and $-c_m(\boldsymbol{z}^{(m)})$ is a summation of strictly concave functions, as shown in (4.38), each attacker's utility function given in (4.31) is a continuous and strictly concave function over the attackers' strategy profile. Moreover, $\mathcal{Z}_m$ is a convex and compact set, and as shown in (4.37), the sets in which δ_{k_m} and α_{k_m} lie are also compact and convex. Thus, since a GNEP having compact and convex action sets as well as continuous and quasi-concave utility functions has at least one GNE [195] [196, Theorem 4.1], our attackers' game has at least one GNE. □

The solution to GNEP problems can be obtained using a number of widely adopted solution concepts that are available in literature [194, 196, 197] where the applicability of each technique depends on the characteristics of the utility functions and action spaces. Given the strict concavity of the utility function of each attacker's problem and the convexity of the action space, such techniques converge to a GNE for our derived formulation.

4.3.4 Defender's Side Analysis

Under a given equilibrium of the followers, the leader (grid operator) selects a defense vector $\boldsymbol{a}_0$ that determines which measurements are to be made secure and able to block potential attacks. The objective of the defender is to minimize a cost function capturing the variation between the DA and RT LMPs, on all N buses in the system, as follows:

$$\min_{\boldsymbol{a}_0 \in \mathcal{A}_0} U_0(\boldsymbol{a}_0, \boldsymbol{a}_{-0}) {=} P_L \sqrt{\frac{1}{N} \sum_{i=1}^{N} (\mu_i^{RT} {-} \mu_i^{DA})^2} {+} c_0(\boldsymbol{a}_0), \tag{4.40}$$

$$\text{s.t } \|\boldsymbol{a}_0\|_0 \leqslant B_0, \tag{4.41}$$

where $c_0(\boldsymbol{a}_0)$ is the cost of defense, P_L is the total system load and B_0 is the limit on the number of measurements that the operator can defend simultaneously. In (4.40), μ_i^{RT} depends on the strategies taken by the defender, $\boldsymbol{a}_0$, and attackers, $\boldsymbol{a}_{-0} \triangleq \{\boldsymbol{z}^{(1)}, \boldsymbol{z}^{(2)}, ..., \boldsymbol{z}^{(M)}\}$.

The Stackelberg solution concept is adequate for games with hierarchy in which the leader enforces its strategy and the followers respond, rationally (i.e. optimally), to the leader's strategy [146]. We denote the optimal response of the attackers to action $\boldsymbol{a}_0$ played by the defender by $\mathcal{R}^{\text{att}}(\boldsymbol{a}_0) \triangleq \{\boldsymbol{z}^{(1)^*}(\boldsymbol{a}_0), \boldsymbol{z}^{(2)^*}(\boldsymbol{a}_0), \cdots, \boldsymbol{z}^{(M)^*}(\boldsymbol{a}_0)\}$. This optimal strategy denotes the equilibrium strategy profile of the attackers as a response to the defender's strategy. In this regard, $\boldsymbol{a}_0^* \in \mathcal{A}_0$ is a Stackelberg equilibrium if it minimizes the leader's (i.e. defender's) utility function U_0. In other words,

$$U_0(\boldsymbol{a}_0^*, \mathcal{R}^{\text{att}}(\boldsymbol{a}_0^*)) \leqslant U_0(\boldsymbol{a}_0, \mathcal{R}^{\text{att}}(\boldsymbol{a}_0)) \ \forall \boldsymbol{a}_0 \in \mathcal{A}_0. \tag{4.42}$$

A Stackelberg equilibrium is guaranteed to exist and be unique if the optimal response of the followers is unique in response to every action of the leader. However, Theorem 7 proves the existence of at least one GNE for the attackers' game. Hence, the followers can have multiple optimal responses to a leaders strategy. In this case, the leader can rank the GNEs corresponding to each strategy based on their impact on its utility and retain the one that leads to the worst utility (i.e. maximal utility given that the defender is a utility minimzer). The leader then selects the policy that minimizes this maximal utility. This is known as a hierarchical equilibrium (HE) [146]. In other words, $\boldsymbol{a}_0 \in \mathcal{A}_0$ is a hierarchical equilibrium strategy for the defender if:

$$\max_{\boldsymbol{a}_{-0} \in \mathcal{R}^{\text{att}}(\boldsymbol{a}_0^*)} U_0(\boldsymbol{a}_0^*, \boldsymbol{a}_{-0}) = \min_{\boldsymbol{a}_0 \in \mathcal{A}_0} \max_{\boldsymbol{a}_{-0} \in \mathcal{R}^{\text{att}}(\boldsymbol{a}^0)} U_0(\boldsymbol{a}_0, \boldsymbol{a}_{-0}). \tag{4.43}$$

4.3.5 Distributed Learning Algorithm

Here, we provide a methodology for finding a hierarchical equilibrium of the defender-attackers game as defined by (4.43).

We first consider the attackers subgame. To find an equilibrium that can be reached by the attackers, we propose a distributed learning algorithm, based on the framework of learning automata that was first analyzed in [198]. The main drivers behind this algorithm are as follows. First, this algorithm is fully distributed in the sense that each attacker is only required to know its own action space, and not the shared one, and the observation of its own payoff after choosing an action. In this regard, knowledge of the action spaces of other attackers or even their existence is not required. Second, since the attackers' game might admit multiple GNEs, the use of this algorithm, emulating practical smart grids security settings, enables the characterization of the GNE(s) that can be actually reached in practice.

The proposed learning algorithm is shown in Algorithm 2. In this algorithm, each attacker m first initializes a strategy vector $\boldsymbol{q}^{(m)}$ containing a probability distribution over its attack space[1]. For instance, $q^{(m)}_{\boldsymbol{z}^{(m)}}(t)$ corresponds to the probability that attacker m chooses attack $\boldsymbol{z}^{(m)}$ at time instant t. Then, at time instant t, each attacker chooses an attack randomly and independently from its attack space following the probability distribution available through its strategy vector. The collection of the attackers' actions at time instant t results in a payoff for each attacker denoted by $r_m(t)$. $r_m(t)$ is a positive normalized value which corresponds to a mapping from $[U_m^{\min}, U_m^{\max}] \rightarrow [0,1]$ where $U_m^{\min}$ and $U_m^{\max}$ are the minimum and maximum achievable utilities by m. Based on the payoff that it receives at time instant i, each attacker, $m \in \mathcal{M}$, updates its strategy vector as follows:

$$\boldsymbol{q}^{(m)}(t+1) = \boldsymbol{q}^{(m)}(t) + b\, r_m(t)(\boldsymbol{e}^{(m)}(t) - \boldsymbol{q}^{(m)}(t)), \tag{4.44}$$

where b is an arbitrarily small positive constant and $\boldsymbol{e}^{(m)}(t)$ is a column vector of length equal to the size of the action set of attacker m. $\boldsymbol{e}^{(m)}(t)$ is a vector whose elements are equal to 0 except for the element corresponding to the action that was selected at time instant t. The element corresponding to the selected action will have a value of 1. Thus, given that the j^{th} attack was selected by attacker m at time instant t; then, $e_j^{(m)}(t) = 1$ and $e_k^{(m)}(t) = 0$ for $k \neq j$. This updating scheme is known as a *linear reward-inaction (L_{R-I})* scheme [198]. Hence, with every iteration, the strategy vector of each attacker is updated and the algorithm repeats until each of the attackers' strategy vectors has all elements equal to 0 except for one element which is equal to 1. Such a strategy vector shows which of the strategies is to be chosen by each attacker. The collection of these attacks (having a probability of 1 each) corresponds to the game's equilibrium. This algorithm has been discussed in [198, 199] where it has been proven that, for an arbitrarily small b, this algorithm asymptotically converges to a pure strategy Nash equilibrium (PSNE) when the game admits a PSNE.

Definition 11. *Following the notations of Definition* 10 *a PSNE is a state of the game in which each player aims at*

$$\max_{\boldsymbol{x}^i} \quad U_i(\boldsymbol{x}^i, \boldsymbol{x}^{*,-i}) \;\; \textit{s.t.} \;\; \boldsymbol{x}^i \in \mathcal{X}_i, \tag{4.45}$$

where, on the contrary with GNEP, $\mathcal{X}_i$ is player i's own strategy space which is independent of other players.

[1] This algorithm requires decritization of the action space of the attackers; our discretization approach is provided in Section 4.5.

Algorithm 2 Distributed Learning Automata

```
Input: Number of attackers $M$
       Action space of each attacker $\mathcal{Z}^{(m)}$
Output: Strategy vector of each player $\boldsymbol{q}^{(m)}$
Initialize $\boldsymbol{q}^{(m)}(0)$
while Not Converged do
    Randomly select $\boldsymbol{z}^{(m)}(t)$ based on $\boldsymbol{q}^{(m)}(t)$
    Collect payoff $r_m(t)$
    Update strategy vector
    $\boldsymbol{q}^{(m)}(t+1) = \boldsymbol{q}^{(m)}(t) + b\, r_m(t)\left(\boldsymbol{e}^{(m)}(t) - \boldsymbol{q}^{(m)}(t)\right)$
    Check Convergence
    if Converged then
        Break
    end if
end while
return Strategy vector $\boldsymbol{q}^{(m)}$
```

Thus, the main difference between a GNE and a PSNE is that the GNE is an optimal action profile in which each action does not violate coupled constraints with other players. Thus, given that Algorithm 2 is guaranteed to converge to a PSNE, proving that this PSNE will never violate the coupled constraints is enough to prove the convergence to a GNE.

Theorem 8. *When applied to Problem 1, Algorithm* 2 *is guaranteed to asymptotically converge to a GNE when the step size* b *is chosen to be arbitrarily small.*

Proof. For a strategy $\boldsymbol{z}^{(m)^*}$ to be a best response strategy (BR) for attacker m, it needs to satisfy the property $U_m(\boldsymbol{z}^{(m)^*}, \boldsymbol{z}^{-(m)}) \geq U_m(\boldsymbol{z}^{(m)}, \boldsymbol{z}^{-(m)})\, \forall \boldsymbol{z}^{(m)} \in \mathcal{Z}^{(m)}$. A PSNE is hence a state of the game in which all players play BR strategies with respect to one another. Thus, a strategy that is not a BR strategy cannot be a PSNE strategy.

However, a strategy $\boldsymbol{z}^{(m)}$ that violates the residual threshold constraints in (4.20) cannot be a BR strategy. In fact, consider the case in which attacker m attacks only one measurement z_i and its attack is denoted by $z_i^{(m)}$. If this attack violates the residual threshold of z_i, z_i will be identified as outlier and discarded from the measurement set. Thus, from (4.27), this results in

$$\begin{aligned} U_m(z_i^{(m)}, \boldsymbol{z}^{-(m)}) &= \zeta_m P_m - c_m(z^{(m)}) \\ &< \zeta_m P_m = U_m(0, \boldsymbol{z}^{-(m)}). \end{aligned}$$

Thus, $z^{(m)}$ is not a BR since not launching an attack at all returns a higher U_m. Hence, all actions that violate the coupled constraints are dominated by the alternative of not carrying out an attack at all and hence cannot correspond to BR strategies. As a result, a PSNE is guaranteed not to violate the coupled constraints in (4.20) and hence this PSNE is a GNE of the game. Since all PSNEs are GNEs and that algorithm 2 asymptotically converges to a PSNE for a small b it, as a result, converges to a GNE of our game. □

To be able to choose a hierarchical equilibrium strategy, a defender needs to anticipate the worst case GNE of the attacker to each defense strategy. This anticipation can be done through: i) repeating the learning algorithm of the attackers, Algorithm 1, starting from different initial conditions to find all possible GNEs from which worst case GNEs can be extracted, ii) using one of the various algorithms tailored to find solutions of GNE problems [194, 196, 197], iii) analytical derivation based on its full knowledge of the cyber-physical system model, energy market model and available past data.

When being able to anticipate all worst case GNEs of the attackers, the defender chooses the strategy that results in the best worst case GNE. This strategy and its corresponding GNE corresponds to the HE of the game.

4.4 Game Model under Limited Information

Thus far, we assumed that the defender can anticipate all worst case GNEs of the attackers. However, in some instances, the defender does not have enough knowledge to anticipate the reaction of the attackers. Thus, it cannot seek a strategy that minimizes its utility when the reaction of the followers to any of its actions is unknown. As a result, we employ the framework of *satisfaction equilibrium* (SE) [151, 172]. Under the satisfaction framework, rather than minimizing its objective function (4.40), given a number of measurements that can be defended concurrently, b_0, the defender aims at keeping the overall changes in the LMPs at all buses under a desired threshold $\mathit{\Gamma}_0$:

$$r_0(\boldsymbol{a}_0, \boldsymbol{a}_{-0}) = \sum_{i=1}^{N} (\mu_i^{RT} - \mu_i^{DA})^2 \leq \mathit{\Gamma}_0. \tag{4.46}$$

Given our hierarchical model, we present a hybrid SE-Nash model in which the defender aims at choosing an action that satisfies its performance requirement given potential reaction of the attackers while the attackers observe the action of the defender and play a noncooperative game in which each attacker aims at maximizing its utility. Extending the SE logic to the attackers game, an attacker is satisfied by playing one of its BR strategies facing the actions chosen by other attackers and the defender. We denote an equilibrium of this hybrid model as a hybrid hierarchical equilibrium (HHE).

Definition 12. *A strategy profile* $(\boldsymbol{a}_0^*, \boldsymbol{z}^{(1)^*}, ..., \boldsymbol{z}^{(M)^*})$ *is an HHE if* $r_0(\boldsymbol{a}_0^*, \boldsymbol{a}_{-0}^*) \leq \mathit{\Gamma}_0$ *and* $U_m(\boldsymbol{z}^{(m)^*}, \boldsymbol{z}^{-(m)^*}) \geqslant U_m(\boldsymbol{z}^{(m)}, \boldsymbol{z}^{-(m)^*})$ $\forall \boldsymbol{z}^{(m)} \in \mathcal{Z}^{(m)}$ *and* $m \in \{1, ..., M\}$.

With a proper choice of $\mathit{\Gamma}_0$ this game is guaranteed to have at least one HHE. In fact, if none of the actions available to the defender leads to meeting its satisfaction level then either the satisfaction threshold needs to be increased or more resources should be employed so that a larger number of measurements can be concurrently secured. When the leader chooses an action that satisfies (4.46) it has no incentive to deviate from it. The attackers will respond to this strategy by playing a GNE. Hence, the attackers would also have no incentive to deviate from this GNE. As a result, the satisfaction strategy of the defender and its GNE response by the attackers correspond to an HHE of this hybrid game.

Given the lack of knowledge about the adversaries, the defender has to learn the action(s) that insure the satisfaction of its constraint through trial and observation. To this end, to find a strategy that satisfies its performance constraint, the defender can adopt the following search algorithm:

i) For a maximum number of iterations, N_0, the defender starts by choosing an action from its strategy space $\mathcal{A}_0$ following a uniform probability distribution $\boldsymbol{f}_0$ over this action space. The followers observe this action and react by playing a noncooperative game whose GNE is obtainable via Algorithm 1.

ii) The leader observes if the action it had taken led to the satisfaction of its performance constraint. If this is the case, the strategy is hence deemed satisfactory and the leader has no incentive to deviate from it. The followers response to the leader's satisfaction action is a GNE and hence the followers have no incentive to deviate from their response as well. Thus, this results in an equilibrium.

iii) If the action that the defender had chosen did not lead to the satisfaction of its constraint, another action is randomly chosen from its strategy space and the process repeats.

This algorithm will eventually find a HHE since, for a large number of iterations and given that at least one action exists in its action space that satisfies the defender's threshold, this action would eventually be randomly chosen with a probability that is extremely close to 1. Assume the number of vulnerable measurements to be equal to V and that the defender secures $b_0 < V$ measurements concurrently. Its action space has then a cardinality $|\mathcal{A}_0| = V!/(b_0!(V - b_0)!)$. Assume that n_0 of the alternatives achieve $r_0 \leq \mathit{\Gamma}_0$. Choosing uniformly between the alternatives, the probability of choosing an action that satisfies the defender is equal to $p_0 = n_0/|\mathcal{A}_0|$. Thus, the probability of not finding a satisfaction action in N_0 iterations, i.e. trials, is given by $(1 - p_0)^{N_0}$; and hence, the probability of finding a satisfaction action in N_0 iterations is given by $p_0^* = 1 - (1 - p_0)^{N_0}$. Moreover, the expected number of iterations needed to find a satisfaction equilibrium strategy is equal to $\mu_0 = 1/p_0$ while the variance of that number is equal to $v_0 = (1 - p_0)/p_0^2$. Hence, significantly increasing $\mathit{\Gamma}_0$ will typically increase n_0 leading to an increase in p_0 and p_0^* and a decrease in μ_0 and v_0. As a result, one can see the conflicting effect between the quality of the found solution, reflected by how low the satisfaction threshold $\mathit{\Gamma}_0$ is, and the speed of finding a solution. Reducing the required satisfaction quality leads to finding a solution faster while a higher satisfaction quality requirement (lower $\mathit{\Gamma}_0$) leads to a slower identification of a solution.

Table 4.1: Attackers' Virtual Bidding Configuration

Attacker	VB Bus 1	VB Bus2	Target Line
Attacker 1	Bus 3	Bus 4	Line 4
Attacker 2	Bus 4	Bus 12	Line 15
Attacker 3	Bus 6	Bus 7	Line 9

4.5 Numerical Results and Analysis

For performance evaluation, we consider three data injection attackers and one defender interacting over the IEEE 30-bus test system which represents a segment of the American Electric Power System [200, 201].

In our numerical setting, each attacker is assumed to have a subset of measurements comprising three measurements that it can attack. In particular, attacker 1 can attack line flow measurements over lines 3, 4 and 7, attacker 2 can attack line flow measurements over lines 14, 15 and 16, and attacker 3 can attack line flow measurements over lines 5, 9 and 11. The attack level on any of the measurements is assumed to have one of the following power levels (in MW): $\{-3.5, 2, 0, 2, 3.5\}$. The amount of virtual power that each attacker sells or buys is assumed to be equal to 100 MW and its attack cost is as shown in (4.38) where $\kappa_m = 0.25$. The DA and RT virtual bidding (VB) information of the different attackers are shown in Table 4.1. In this table, VB Bus 1 corresponds to the bus at which an attacker sells energy in DA (respectively buys in RT) and VB Bus 2 corresponds to the bus at which this attacker buys energy in DA (respectively sells in RT). The target line column corresponds to the line connecting the two VB buses which the attacker aims to congest. In our simulations, we assume that the system experiences no congestion in DA and that each attacker primarily aims at creating a fake estimated congestion over its target line so as to reap financial benefit[2].

On the other hand, the defender decides on a subset of measurements to secure out of all the measurements in the system. In our simulations, we assume that a measurement device is placed on every bus and every line in the system so that every power injection and every line flow is measured.

In Fig. 4.1 we show the effect of each attacker's optimal attack, when no defense or other attackers are present in the system, on the RT LMPs. As can be seen from Fig. 4.1, assuming that only one attacker attacks at a time, the action of attacker 3 yields the most detrimental effect on the system. This can be also seen from Fig. 4.2 in which the impact of each of the attacks on the system is shown. The global effect of any attack on the system is captured by the defender's utility function given in (4.40). Fig. 4.2 shows indeed that the attack of 3 has the highest global effect on the

[2] Since our main focus is on the attackers' and defender's strategies, it is assumed that all market participants abide by their DA schedules and, except for the attacks and defense, no change in system conditions occurs between DA and RT. Thus, in case of no attacks, the DA and RT LMPs match.

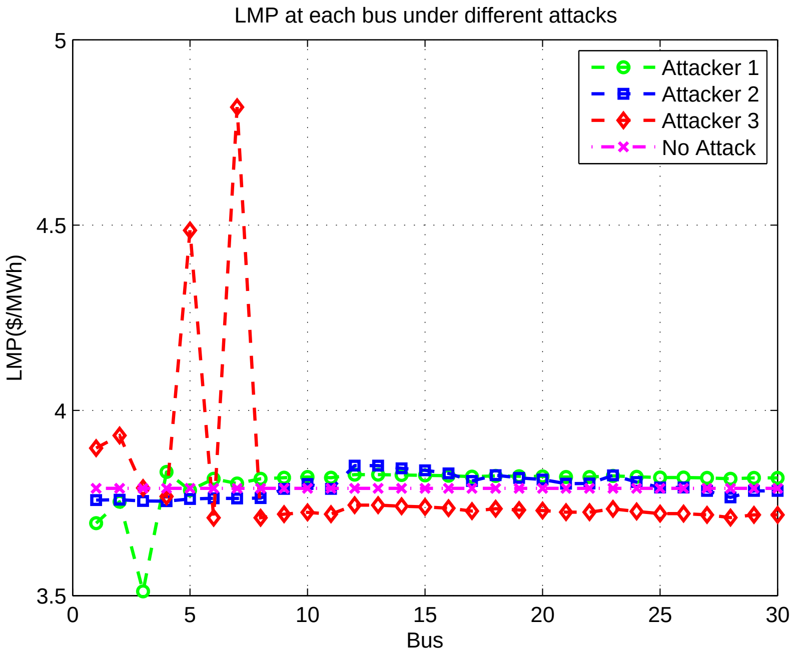

Figure 4.1: System LMPs under a unique adversary's optimal attack with no defense

system followed by that of attacker 1 and of attacker 2 respectively. In fact, the defender's loss under the attack of attacker 3 is equal to $44.69 as compared to $11.61 under that of attacker 1 and $5.74 under that of attacker 2.

Fig. 4.3 shows the effect that a congestion over the target line of attacker j has on the payoff of attacker i denoted as $U_{i,j}$. Accordingly, Fig. 4.3 shows how the attack of an attacker affects the payoffs of the others. To this end, the attackers appear to be in a perfectly conflicting situation since fulfilling the purpose of an attacker i results in a negative payoff to all other attackers.

Next, we consider the strategic interactions between the three attackers and the defender based on our Stackelberg model. In this regard, we find the HE of the game, and the underlying GNE of the attackers, when the defender defends an increasing number of measurements as shown in Table 4.2. We, namely, treat the cases in which the number of measurements that can be defended concurrently, B_0, is 0, 1 and 2. The attackers' optimal strategies are represented in a vector containing their respective optimal attack levels (in MW) such that for attacker 1 the attacked levels correspond to additive power flows over $(\text{line } 3, \text{line } 4, \text{line } 7)$, for attacker 2 to additive power flows over $(\text{line } 14, \text{line } 15, \text{line } 16)$ and for attacker 3 to additive power flows over $(\text{line } 5, \text{line } 9, \text{line } 11)$.

Given that a congestion occurring over line 9 has the largest impact on the system, one can intuitively expect the defender to secure the measurement over that line when only one measurement can be secured (i.e. $B_0 = 1$). Indeed, from Table 4.2, we can see that the HE corresponds to the defender defending line 9 and the attackers carrying out their optimal equilibrium response. For

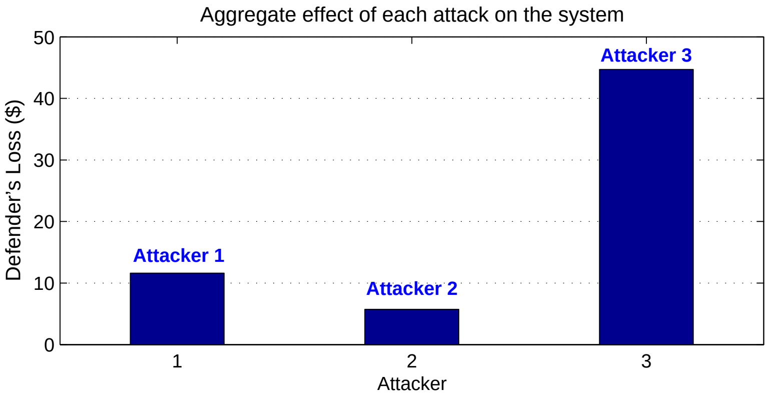

Figure 4.2: Global effect of each attack on the system.

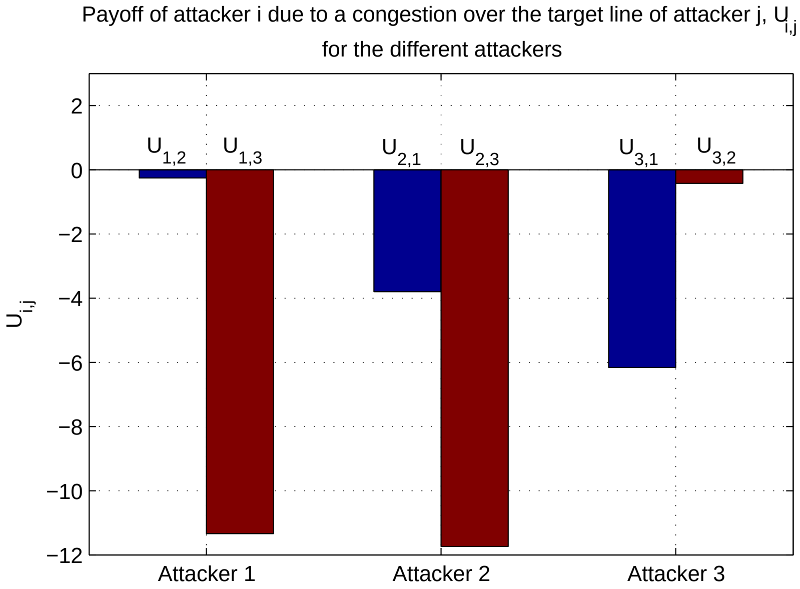

Figure 4.3: Loss to attacker i due to congestion over the target line of attacker j.

the case in which the defender can defend up to two measurements concurrently, i.e. $B_0 = 2$, one expects the defender to secure the measurements of the two lines, lines 4 and 9, which congestion has the largest impact on the system (we refer to this defense, in this context, as the critical defense). However, the HE of the game corresponds to the defender defending lines 4 and 5 instead. In fact, by defending those two lines *the attackers' optimal response yields no effect on the system hence leaving the RT LMPs unaffected.* This is a representation of the analysis provided through Remark 2 in which multiple attackers' attacks can cancel each other out.

Fig. 4.4 provides a comparison between the LMP manipulation outcome under the HE strategy as

Table 4.2: Stackelberg Game Solution for $B_0 = \{0, 1, 2\}$

B_0	Secured Measurements	Attacker 1	Attacker 2	Attacker 3
0	-	(2,3.5,3.5)	(0,0,0)	(3.5,3.5,0)
1	line 9	(0,3.5,2)	(0,0,0)	(0,0,0)
2	lines 4 and 5	(0,0,0)	(0,2,0)	(0,3.5,-3.5)

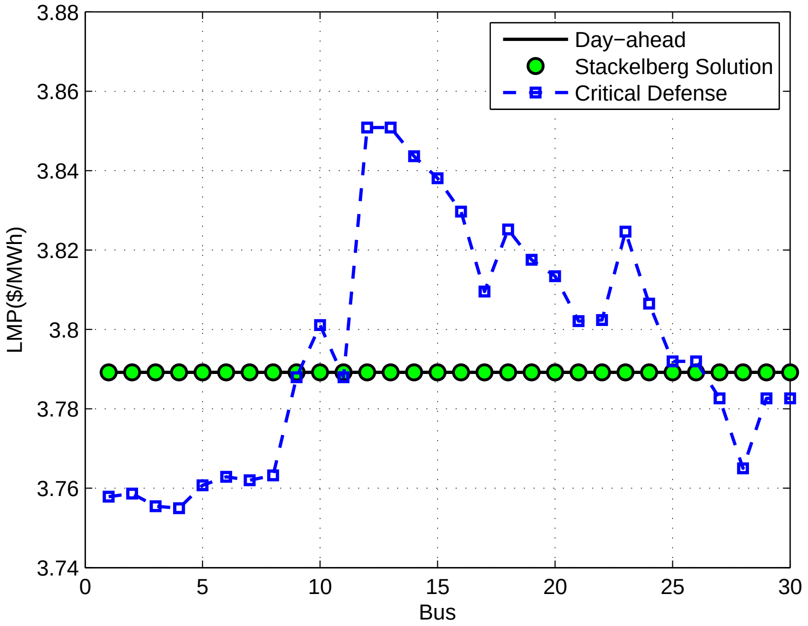

Figure 4.4: Comparison between HE and critical line defense strategies

compared to the critical defense strategy. It can be clearly seen that the HE strategy (i.e. Stackelberg solution) completely prevents the manipulation of the RT LMPs and, hence, is a significantly better strategy than critical defense. In fact, the attackers' optimal response to the critical defense strategy resulted in a successful manipulation of the RT LMPs leading to a 3% root mean square deviation (RMSD) from the DA LMPs where

$$\text{RMSD} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(\mu_i^{RT} - \mu_i^{DA})^2}. \tag{4.47}$$

Fig. 4.5 shows the defender's HE utility for different numbers of concurrently defended measurements. This figure shows that the attackers have a very large impact on the system when no defensive actions are taken. In fact, the aggregate effect of the attacks on the system LMPs, at equilibrium, with no defensive actions is $306. However, when $B_0 = 1$ (defender is able to secure

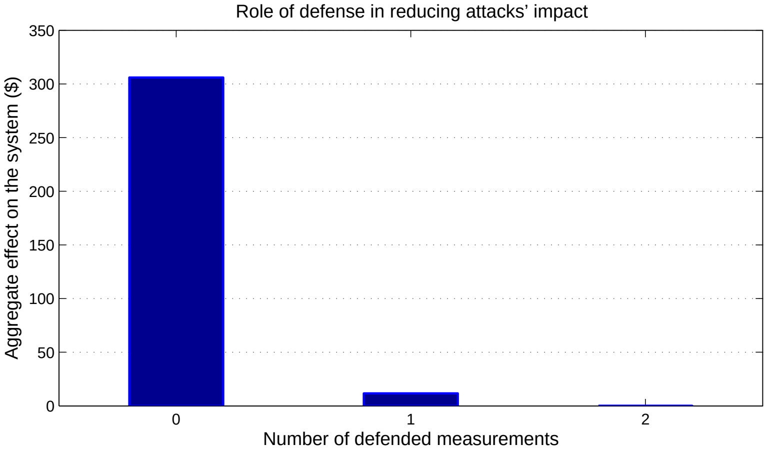

Figure 4.5: Effect of system defense

one measurement), the HE of the game shows that the global effect of the multiple data injections attacks on the system drops significantly to $\$11.6$. Moreover, when $B_0 = 2$ (defender is able to secure two measurements concurrently), the HE of the game shows that the defender's equilibrium strategy completely protects the system against attacks and achieves a zero overall effect of the attacks on the system.

We next consider our proposed SE-Nash framework and we define the *price of information* (PI) to be an index reflecting the loss that the defender endures due to its lack of information about the possible reaction of the attackers to its defense strategies. The PI is defined as follows:

$$\text{PI} = U_0^{\text{HHE}} - U_0^{\text{HE}}. \tag{4.48}$$

The PI hence reflects the difference between the utility achieved under the SE-Nash framework and the one achieved under the Stackleberg model (corresponding to minimum possible utility).

We consider first that the defender can only defend one measurement at a time. Given that there are 9 vulnerable measurement units in the system, the defender has 9 options to choose from. Considering that the defender would be satisfied by having RMSD $\leq 10\%$, we run the search algorithm described in Section 4.4 and the HHE we obtained is similar to the one we obtained using the Stackelberg model for $B_0 = 1$. Thus, in this case, PI $= 0$. Following this HHE, the defender defends the line measurement over line 9 and the attackers' GNE corresponds to that shown in Table 4.2 for $B_0 = 1$. This strategy generates an $RMSD = 6.1\% < 10\%$ hence meeting the performance requirement.

Next, we consider the case in which the defender secures 2 measurements concurrently. Thus, the defender has 36 options to choose from. We consider two different performance requirements. In the first, the defender seeks to have RMSD $\leq 5\%$. Running the search algorithm yields an HHE dictating the defense of lines 4 and 9 which corresponds to the critical defense defined previously.

This HHE results in RMSD $= 3\% < 5\%$ and a PI $= \$5.74$. The second considered performance requirement seeks to have RMSD $\leq 10\%$. In this regard, our search algorithm led to an HHE under which lines 5 and 9 should be defended. This HHE results in RMSD $= 6.1\% < 10\%$ and a PI $= \$11.61$.

4.6 Summary

In this chapter, we have studied the problem of data injection attacks on the smart grid in the presence of multiple adversaries. The strategic interactions between the defender and the attackers have been modeled using a Stackelberg game and a hybrid satisfaction equilibrium - Nash equilibrium game. In these games, the grid operator acts as the leader and the attackers act as followers which play a noncooperative strategic game in response to each defender's strategy. The costs of attack and defense have been integrated in the utility functions of the players. We have proven the existence of a generalized Nash equilibrium of the attackers' game, studied the existence and properties of the equilibria of the Stackelberg and the hybrid games and proposed learning algorithms, and proved their convergence, to compute the games' solutions. Numerical results have shown the critically important role of the defender in protecting the grid and the potential conflicting interaction between the multiple adversaries. Our results also highlight the potential loss that the defender can incur due to a lack of information about the actions of the attackers.

Chapter 5

Time-Critical Network Interdiction Games for Cyber-Physical Security of UAV Systems

5.1 Introduction

Recent developments in unmanned aerial vehicle (UAV) technology have led to its adoption in a variety of commercial, recreational, and military applications such as telecommunications, surveillance, delivery systems, rescue operations, and intelligence missions [12,13,202–208]. Due to their ability to reach relatively inaccessible locations (such as natural disaster sites as well as remote mountains, valleys, and forests) and their capacity to travel without being restricted to predefined pathways, UAVs can effectively carry out *time-critical missions* [12, 209–211].

5.1.1 Prior Art and its limitations

One prominent time-critical UAV application is drone delivery systems [206, 212–217] which can be used to deliver consumer parcels [206, 212–214] (with Amazon Prime Air [212] and Google's Project Wing [206] being key examples) as well as emergency medical products [209–211].

However, the practical deployment of drone delivery systems can be hindered by their vulnerability to a myriad of cyber and physical attacks [83, 85, 133, 218, 219]. On the physical side, to avoid conflict with manned and commercial aviations, the altitude of UAVs is typically limited to around 400 ft [212], putting them in the range of hunting rifles and firearms which can target them (in an similar manner to such attacks which have targeted, for example, power system equipments [44]). Moreover, UAVs are vulnerable to a variety of cyber threats as demonstrated in [83, 85, 133, 218, 219]. For example, the work in [83] provided a general overview of cyber attacks which can target the confidentiality, integrity, and availability of UAV systems. The authors in [218] focused on the security of the communication links between ground control and unmanned aircrafts. Moreover, the work in [85] provided a demonstration in which the authors successfully launched a man-in-the-middle attack against a typical UAV used by law enforcement agencies for critical applications. Meanwhile, the authors in [219, 220] investigated GPS spoofing attacks to manipulate the trajectory of an autonomous UAV while the work in [133] surveyed various detection and localization techniques as well as cyber-physical attacks which can be used against UAVs.

On the other hand, the ability of drones to reach secure or private locations has raised concerns regarding their possible usage for executing malicious missions. In fact, a number of recent research works, such as [133] and [134], studied on the risks of potentially using UAVs to execute nefarious missions such as targeting a public, political, or military figure in a secure perimeter, intruding into a military security perimeter, smuggling illicit products, or gaining unauthorized access to personal property. This has led to the development of what is knows as *anti-drone systems* whose goal is to defend against such intruding drones using developed surveillance technologies and cyber-physical defense mechanisms [133,134]. The interactions between intruding drones and anti-drone systems is clearly a highly time-critical application of UAVs.

Security analyses of these two time-critical UAV applications involve: a) a UAV aiming to achieve a mission (benign or malicious) in the shortest possible time and b) an interdictor (malicious, e.g., in drone delivery systems, or benign, e.g., in anti-drone systems) whose goal is to interdict and delay the UAV and compromise its mission. The highly intertwined decision making processes of these two scenarios motivates the need for a holistic strategic analysis which can capture this underlying interdependent decision making processes and identify optimal interdiction and security strategies. However, prior art [83, 85, 133, 134, 218–220], and references therein, has somewhat remarkably ignored such interactive time-critical situations and, instead, has either provided qualitative analyses or focused on specific and isolated security experiments, rather than on a rigorous study.

5.1.2 Summary of Contributions

The main contribution of this chapter is to develop the first comprehensive framework for the modeling and analysis of the cyber-physical security of time-critical UAV applications. We pose the general problem as a *network interdiction game* between a UAV operator (benign or malicious) and an interdictor (malicious or benign). In this game, the interdictor chooses the optimal attack locations along the area which can be traversed by the UAV to interdict the UAV, via a cyber or physical attack, with the goal of delaying the UAV and compromising its mission. On the other hand, the UAV acts as an evader that chooses the best path selection policy from its origin to its destination, while evading attacks and minimizing its total expected travel time (hereinafter called the *expected delivery time*) needed to complete the mission.

In this regard, we consider both deterministic and probabilistic interdiction strategies. Under deterministic interdiction, we derive and analyze the Stackelberg equilibrium (SE) of the game. We then show that a probabilistic interdiction strategy gives rise to a leader-follower structure in which the UAV's problem corresponds to solving a Markov decision process (MDP) and the interdictor's problem corresponds to setting the parameters of this MDP. In this regard, we characterize the SE of the game under mixed interdiction and propose practical algorithms to solve the underlying UAV operator's and interdictor's problems.

This analysis is carried-out under full rationality of the UAV operator and the interdictor. This is an underlying assumption in classical game theory which implies that all the agents involved assess outcomes and observe probabilities objectively and equally. However, in practice, time-critical UAV applications have two features, a) time criticality, and b) uncertainty, which can lead to a bounded rationality of the involved players. Indeed, a common feature in time-critical UAV applications is the strict goal of accomplishing a mission within a target delivery time. Delays in such applications can have tragic consequences ranging from inability to reach victims on time, in emergency scenarios, to increasing customer dissatisfaction in commercial applications. Equivalently, in anti-drone systems, both the anti-drone and UAV owners wish to complete their mission as quickly as possible, with the slightest delays being the difference between the success or failure of the mission. Given this time criticality, the merit of an achieved delivery time must valued relative to the target delivery time, rather than as an absolute quantity. Moreover, due to the bounded rationality of the agents involved, this valuation can be performed subjectively and differently by the UAV operator and the interdictor. In addition, the choice of interdiction and path selection strategies is influenced by various underlying uncertainties which stem, for example, from the probabilistic risk levels of a certain path and the likelihood with which a carried cyber-physical attack is successful. Hence, due to these uncertainties, the likelihood of achieving a certain delivery time can be assessed differently by the interdictor and UAV operator.

To capture these bounded rationality factors in our game, we use tools from *cumulative prospect theory* (PT) [148, 149]. PT enables modeling the bounded rationality in the decision making processes of the interdictor and UAV operator by capturing a) the subjective perceptions of the risk levels involved (such as the subjective perception of the likelihood with which a certain attack is successful or a certain delivery time is achieved), and b) the subjective assessment of an achieved delivery time relatively to a reference target delivery time. In this respect, we consider both deterministic and probabilistic strategies in the PT game analysis. In this regard, we analytically derive the SE of the deterministic PT game and propose solution algorithms which allow numerically identifying the SE of the PT game under mixed interdiction.

We then complement our theoretical analysis with extensive simulations. Our simulation results provide several key insights pertaining to the effects of the incorporation of PT in our game formulation on the resulting equilibrium strategies and achieved expected delivery times:

- By increasing the target delivery time, the interdictor becomes more prone to choosing risk seeking interdiction strategies while the UAV operator becomes less prone to taking the risky paths.
- At low values of the target delivery time, the PT achieved expected delivery time is lower than that of the conventional game; while for relatively high values of the target delivery

time, the PT achieved expected delivery time exceeds that of the conventional fully rational game.

- A more distorted perception of the probabilities with which a successful attack occurs leads the UAV to choosing risky paths which result in delays in the expected delivery times. Indeed, our results show that a rational path choice by the UAV can lead to achieving a 30% decrease in expected delivery time as compared to the expected delivery time achieved under PT.
- The PT bounded rationality of the player is in general disadvantageous to the UAV operator leading to expected delivery times which exceed the pre-set target delivery times.

The rest of this chapter is organized as follows. Section 5.2 presents the system model and formulates the proposed network interdiction game with fully rational players. Section 5.3 and Section 5.4 study the game under deterministic and probabilistic interdiction strategies, respectively. Section 5.5 introduces the incorporation of cumulative prospect theory in the proposed network interdiction game. Section 5.6 and Section 5.7 formulate and analyze the PT games under deterministic interdiction and probabilistic interdiction strategies, respectively. A number of numerical results are presented in Section 5.8 while Section 5.9 concludes the chapter.

5.2 System Model and Problem Formulation

5.2.1 System Model

Consider a drone system in which a UAV, controlled by an operator, executes a critical mission requiring it to travel from a source location O to a destination location D with minimum time, referred to as the *delivery time*. Meanwhile, an interdictor seeks to interdict the UAV's flight by choosing a certain area or location, among a number of "danger points" (such as i and j in Fig. 5.1), along its path from O to D to launch a cyber-physical attack. The interdictor's attacks [83, 85, 133, 218, 219] include physical attacks against the UAV (such as being targeted by a rifle or a military defense system) as well as cyber attacks (such as de-authentication or GPS spoofing attacks) which cause the UAV operator to lose control of the drone leading to its capture or destruction.

This model readily captures the two use cases of Section 5.1: a) The case in which the UAV is a benign player and the interdictor is malicious, as is the case in a drone delivery system and b) The case in which the interdictor is an anti-drone system seeking to stop a rogue (or malicious) drone from reaching its destination.

A danger point represents a location along the possibles paths between O and D, from which the UAV is exposed to possible cyber-physical attacks. Such points can represent points of high altitude, which allow line-of-sight and spatial proximity (e.g., high hills, high-rise buildings, etc.) between a potential attacker and the UAV. As a result, the set of danger points between O and D

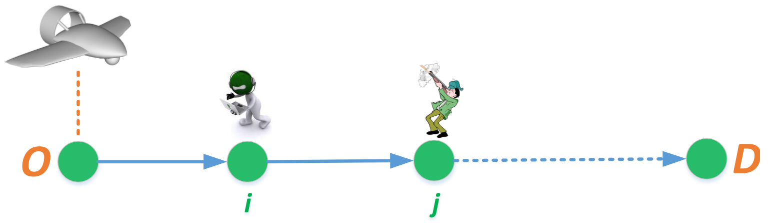

Figure 5.1: Danger points along a certain path from source (O) to destination (D).

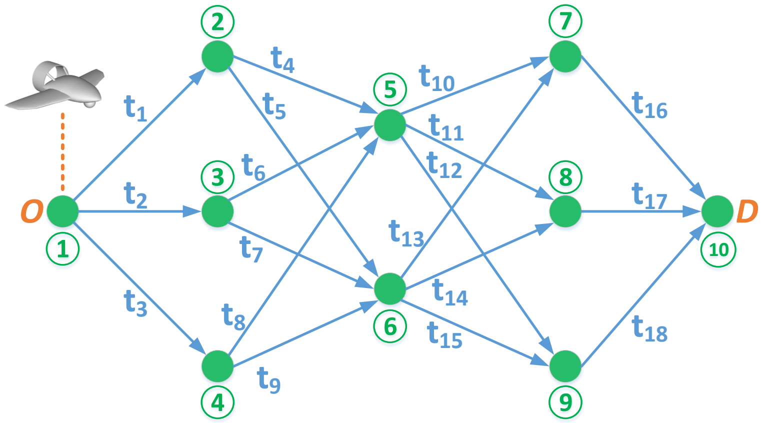

Figure 5.2: Origin to destination security graph.

correspond to inevitable locations along the drone's flight path that are susceptible to attacks by a malicious interdictor or an anti-drone system.

The set of danger points between O and D define a security network represented by a graph $\mathcal{G}(\mathcal{N},\mathcal{E})$, as shown in Fig. 5.2, in which the set of vertices, $\mathcal{N}$, is the set of N danger points between O and D, and the set of edges, $\mathcal{E}$, such that $|\mathcal{E}| = E$, being the set of connections between these danger points. Given that, in practice, the UAV's travel from origin to destination may not be restricted to predefined airways[1], there can be an infinite number of paths which connect O to D. However, each one of these paths will go through a number of danger points that may be shared among different paths. This infinite set of possible O to D paths can, from a security viewpoint, be represented by the set of danger points that each path traverses. Given the time-critical nature of the considered UAV applications, the defined set of edges $\mathcal{E}$ in the security graph $\mathcal{G}$ will comprise the shortest paths between each two danger points.

For two neighboring points i and j connected by edge $e_k \in \mathcal{E}$, we let $t(i,j)$ be the time that the UAV needs to travel from i to j over e_k. Hence, $t(.) : \mathcal{N} \times \mathcal{N} \rightarrow \mathbb{R}$ is a function which returns the travel time needed by the UAV to travel between two connected nodes. We let p_n be the probability with which an attack launched from point $n \in \mathcal{N}$ is successful given that, in practice, an attack

[1] Here, our model can also accommodate future scenarios in which the UAV's flight may be regulated and, as a result, restricted to a defined set of paths.

carried out at $n \in \mathcal{N}$ might not always be successful. Without loss of generality, we consider that for any $n \in \mathcal{N} \setminus \{O, D\}$, $p_n \neq 0$; and for $n' \in \{O, D\}$, $p_{n'} = 0$.

We define $\mathcal{H}$ as the set of H simple paths (containing no repeated vertices[2]) from the origin, O, to destination, D over the security graph $\mathcal{G}$. For each path[3] $h \in \mathcal{H}$, we define a distance function $f^h(.) : h \rightarrow \mathbb{R}$, which takes an input node $n \in h$ and returns the time needed by the UAV to reach $n \in h$ from O following path $h \in \mathcal{H}$. For example, in Fig. 5.2, $f^{h'}(5) = t_2 + t_6$ where $h' \triangleq (1, 3, 5, 8, 10)$.

On this security graph $\mathcal{G}$, the UAV acts as an *evader* who aims at finding the best travel policy, and as a result a path selection strategy, to reach D from O at a minimum delivery time, while the *interdictor* aims at finding the best interdiction strategy (a choice of danger points from which to launch an attack) to intercept/delay the travel of the UAV.

5.2.2 Game-Theoretic Problem Formulation

In this network interdiction game, the UAV, denoted as player U, must find the best possible path to take over $\mathcal{G}$ to reach D from O with minimum time while accounting for the presence of the interdictor (player I). In case the UAV is successfully compromised by the interdictor from a node $n \in \mathcal{N}$, the UAV operator must resend a new UAV with the same mission from node O, which leads to both financial losses and delayed delivery time. Hence, a successful attack by the interdictor at node n can be mathematically modeled as if the UAV had returned to the point of origin from which it needs to travel again to its destination. Hence, with the goal of minimizing delivery time, the UAV operator may not always choose the shortest O-to-D path if this path is suspected to be risky. As such, the path selection strategy must account for possible interdiction strategies so as to successfully accomplish the O-to-D mission in a minimum delivery time. Similarly, the interdiction strategy must anticipate the possible paths that may be taken by the UAV to maximize this delivery time. To model and analyze the intertwined decision making processes of the interdictor and UAV operator, we next introduce a novel *time-critical network interdiction game*.

The proposed time-critical network interdiction game architecture over graph $\mathcal{G}$ is formally defined as follows. The set of players is $\mathcal{P} \triangleq \{U, I\}$. The interdictor moves first and chooses an interdiction strategy $\boldsymbol{x} \in \mathcal{X}$ which is a probability distribution over the set of danger points, $\mathcal{N}$, where x_n (i.e. element n of vector $\boldsymbol{x}$) specifies the probability with which to launch an attack from node $n \in \mathcal{N}$ while satisfying $\sum_{n \in \mathcal{N}} x_n = 1$. We refer to this probabilistic choice of $\boldsymbol{x}$ as a *mixed interdiction strategy*. A special case for the choice of $\boldsymbol{x}$ consists of restricting $\boldsymbol{x}$ to the case in which $x_n = 1$ for an $n \in \mathcal{N}$ and $x_n = 0$ for $n \in \mathcal{N} \setminus n$. This, hence, corresponds to choosing

[2] Loops are naturally dismissed by a UAV operator aiming at minimizing delivery time.

[3] A path is a sequence of nodes and edges which connect O to D. Here, we represent a certain path $h \in \mathcal{H}$ by the set of its constituents nodes. For example, $h \triangleq \{1, 4, 6, 9, 10\}$ constitutes a path from O to D in Fig. 5.2 in which O and D are numbered as nodes 1 and 10 respectively. Thus, we mathematically consider h to be a subset of nodes, i.e. $h \subseteq \mathcal{N}$. In this respect, the notation $n \in h$ represents a node n that is in subset h, i.e., a node n that is traversed by path h.

a deterministic interdiction strategy to which we refer as a *pure interdiction strategy*. Based on the interdiction strategy $\boldsymbol{x}$, U chooses a travel policy (i.e. a path selection strategy). This requires U to choose the next node to go to from each possible node at which it can be situated. In other words, if the UAV is at node n, denoting the set of neighboring node of n over graph $\mathcal{G}$ by $\mathcal{N}_g(n)$, the UAV's travel policy must specify which node $n' \in \mathcal{N}_g(n)$ to go to from each possible node $n \in \mathcal{N}$. Such a policy will result in a certain O-to-D path. Hence, the goal of U is to choose the best possible path $h \in \mathcal{H}$ to minimize the expected delivery time while that of the attacker is to maximize this expected delivery time.

For analyzing the resulting time-critical network interdiction game, we next separately study the games under pure interdiction and mixed interdiction strategies.

5.3 Game Analysis under Pure Interdiction Strategies

5.3.1 Game Formulation under Pure Strategies

Under pure strategies, the interdictor chooses to be located at node n (the strategy space of I is, hence, $\mathcal{N}$) while the UAV seeks to choose an O-to-D path $h \in \mathcal{H}$. If $h \in \mathcal{H}$ contains node n, when traveling from O-to-D along path h, it will traverse all danger points $n' \in h$, $n' \neq n$ without any risk of being attacked. However, when the UAV reaches n, it may continue its path with probability $1 - p_n$, i.e., the probability with which the attack launched from n is not successful, or it may be sent back to O with probability p_n, i.e., the probability with which the attack launched from n is successful.

Let t_a be the re-handling time, which is the time needed by the operator to send a new UAV, if the original one was compromised. Then, the possible delivery times which can occur when $n \in h$ and their probability of occurrence will be:

$$T_k = f^h(D) + k[f^h(n) + t_a], \tag{5.1}$$

$$\tau_k = (1 - q_n)^k q_n = p_n^k q_n, \tag{5.2}$$

$$\text{for } k \in \mathbb{N}_0,$$

where $q_n = 1 - p_n$, T_k is the k^{th} possible delivery time, and τ_k is the probability of occurrence of T_k. Hence, based on the possible delivery times and their likelihood, defined respectively in (5.1) and (5.2), the expected delivery time, denoted[4] by $E_d(h \supset n)$, when the interdictor is located at n and the UAV takes path h containing n is presented in Proposition 3.

[4] The expected delivery time for a node n chosen by I and a path h chosen by U will be denoted by $E_d(n, h)$. Additionally, with a slight abuse of notation, we occasionally denote $E_d(n, h)$ by $E_d(h \supset n)$ or $E_d(n \in h)$ to highlight that node n is part of the chosen path h, or that h contains n, and $E_d(n \notin h)$ to highlight that n is not part of path h.

Proposition 3. *The expected delivery time for each pair of interdiction and path selection strategies* (n, h)*, which consists of interdictor choosing node* n *and the UAV taking path* h*, is given by:*

$$E_d(n,h) = \begin{cases} f^h(D), \textit{ if } n \notin h, & (5.3)\\ \dfrac{p_n}{1-p_n}(f^h(n)+t_a) + f^h(D), \textit{ if } n \in h. & (5.4) \end{cases}$$

Proof. First, we consider the case in which n is not part of h. If the UAV chooses a path h which does not contain the node n at which the interdictor is located, then the UAV cannot be successfully attacked and, hence, the expected delivery time, $E_d(n \notin h)$, will be simply given by

$$E_d(n \notin h) = f^h(D). \tag{5.5}$$

Second, we consider the case in which h contains node n, i.e. $h \supset n$. By inspection of (5.1), one can see that $f^h(D)$ appears in every possible delivery time outcome, while $(f^h(n) + t_a)$ is multiplied by the number of times the UAV had been successfully attacked at n before it was successfully able to traverse n. This latter component of (5.1) corresponds to the number of failures that the UAV experiences before the first success in traversing n. Consider being successfully attacked at n to be a failure of the UAV in traversing n, which can occur with probability p_n, and consider traversing n to be a success for the UAV, which can occur with probability $q_n = 1 - p_n$, then the expected delivery time will be:

$$E_d(h \supset n) = (\text{expected \# failures before } 1^{\text{st}} \text{ success})(f^h(n)+t_a) + f^h(D). \tag{5.6}$$

The number of failures before the first success follows a geometric distribution whose mean is given by:

$$\mu = \frac{1-q_n}{q_n} = \frac{p_n}{1-p_n}. \tag{5.7}$$

As a result,

$$\begin{aligned} E_d(h \supset n) &= (\text{expected \# failures before 1st success})(f^h(n)+t_a)+f^h(D)\\ &= \frac{p_n}{1-p_n}(f^h(n)+t_a) + f^h(D). \end{aligned} \tag{5.8}$$

Detailed and formal derivations leading to (5.8) are given next.

Given the possible outcomes in (5.1) and their probability of occurrence in (5.2), the expected delivery time is given by:

$$E_d(h \supset n) = \sum_{k=0}^{\infty}[f^h(D) + k(f^h(n)+t_a)](1-q_n)^k q_n. \tag{5.9}$$

In this regard, let $A = \sum_{k=0}^{\infty} f^h(D)(1-q_n)^k q_n$ and $B = \sum_{k=0}^{\infty} k(f^h(n)+t_a)(1-q_n)^k q_n$, which results in $E_d(h \subset n) = A + B$. We next compute A and B.

$$\begin{aligned} A &= \sum_{k=0}^{\infty} f^h(D)(1-q_n)^k q_n \\ &= f^h(D) q_n \sum_{k=0}^{\infty} (1-q_n)^k. \end{aligned} \tag{5.10}$$

Now, $\sum_{k=0}^{\infty}(1-q_n)^k$ is a geometric series of the form $\sum_{k=0}^{\infty} ar^k$ with $a=1$ and $r = 1-q_n < 1$. Hence,

$$A = f^h(D) q_n (\frac{1}{1-(1-q_n)}) = f^h(D).$$

$$\begin{aligned} B &= \sum_{k=0}^{\infty} k(f^h(n)+t_a)(1-q_n)^k q_n \\ &= (f^h(n)+t_a) q_n \sum_{k=0}^{\infty} k(1-q_n)^k \\ &= (f^h(n)+t_a) q_n (1-q_n) \sum_{k=0}^{\infty} k(1-q_n)^{k-1} \\ &= (f^h(n)+t_a) q_n (1-q_n) \frac{d}{dq_n}(-\sum_{k=0}^{\infty}(1-q_n)^k), \end{aligned} \tag{5.11}$$

where the interchange between the summation and differentiation in the last step can be performed due to the uniform convergence of the geometric series represented by the summation term. Now, $\sum_{k=0}^{\infty}(1-q_n)^k = \frac{1}{1-(1-q_n)} = \frac{1}{q_n}$ as has been shown in the computation of A. Hence,

$$\begin{aligned} B &= (f^h(n)+t_a) q_n (1-q_n) \frac{d}{dq_n}(-\sum_{k=0}^{\infty}(1-q_n)^k) \\ &= (f^h(n)+t_a) q_n (1-q_n) \frac{d}{dq_n}(-\frac{1}{q_n}) \\ &= (f^h(n)+t_a) q_n (1-q_n) (\frac{1}{q_n^2}) \\ &= (f^h(n)+t_a) \frac{1-q_n}{q_n} = (f^h(n)+t_a) \frac{p_n}{1-p_n}. \end{aligned} \tag{5.12}$$

Hence,

$$E_d(h \subset n) = A + B = f^h(D) + \frac{p_n}{1-p_n}(f^h(n)+t_a). \tag{5.13}$$

□

Hence, the $\frac{p_n}{1-p_n}(f^h(n)+t_a)$ term in (5.4) can be viewed as a delay penalty, which the UAV would endure for taking the risk of traversing a risky danger point at which the interdictor is located.

In this regard, the goal of the interdictor is to choose an interdiction strategy (which consists of choosing a node from which to launch an attack) to maximize this expected delivery time while the goal of the UAV operator is to choose the best O-to-D path to minimize the expected delivery time. Hence, we have a zero-sum network interdiction game.

5.3.2 Equilibrium in Pure Strategies

In our network interdiction game, the interdictor moves first, choosing a certain node from which to attack the UAV, and then the UAV operator responds by choosing the path it wishes to take. As such, for each choice $n \in \mathcal{N}$ by the interdictor, U can identify the best reaction strategy $h = \rho(n)$ specifying the best path to take when I chooses n. Hence, this gives rise to a *hierarchical game structure* whose equilibrium concept, known as the Stackelberg equilibrium [146], is defined as follows:

Definition 13. *A strategy pair (n^*, h^*) constitutes a* Stackelberg equilibrium *of the network interdiciton game if*

$$E_d(n^*, h^* = \rho(n^*)) \geq E_d(n, \rho(n)) \textit{ for all } n \in \mathcal{N}, \tag{5.14}$$

and

$$\rho(n) = \operatorname*{argmin}_{h \in \mathcal{H}} E_d(n, h), \tag{5.15}$$

where $E_d(n, h)$ is as given in (5.3) and (5.4).

Under this hierarchical structure, the interdictor's problem reduces to the following problem:

$$n^* = \operatorname*{argmax}_{n \in \mathcal{N}} E_d(n, \rho(n)). \tag{5.16}$$

In this regard, denoting a shortest O-to-D path by h_s, the SE of our network interdiction game can be analytically characterized as shown in Theorem 9.

Theorem 9. *The interdictor's SE strategy, n^*, is given by:*

$$n^* = \operatorname*{argmax}_{n \in \{n_1, n_2\}} \Big(E_d\big(n_1, \rho(n_1)\big), E_d\big(n_2, \rho(n_2)\big)\Big), \tag{5.17}$$

where

$$n_1 = \operatorname*{argmax}_{n \in \mathcal{N}_{h_s}} \frac{p_n}{1-p_n}(f^{h_s}(n) + t_a) + f^{h_s}(D), \tag{5.18}$$

$$\mathcal{N}_{h_s} = \{n \in h_s | \frac{p_n}{1-p_n}(f^{h_s}(n) + t_a) + f^{h_s}(D) \leq f^{h_n}(D)\}, \tag{5.19}$$

with h_n being a shortest O-to-D path not containing node n, and

$$n_2 = \underset{n \in h_s \setminus \mathcal{N}_{h_s}}{\operatorname{argmax}} f^{h_n}(D). \tag{5.20}$$

The UAV operator's SE strategy is given by

$$h^* {=} \rho(n^*) {=} \begin{cases} h_s, \ \textit{if}\, n^* = n_1; & (5.21) \\ h_{n_2}, \ \textit{if}\, n^* = n_2. & (5.22) \end{cases}$$

In addition, the resulting SE expected delivery time is

$$E_d(n^*, h^*) {=} \begin{cases} \frac{p_{n^*}}{1-p_{n^*}}(f^{h_s}(n^*) + t_a) + f^{h_s}(D), & \\ \qquad\qquad\qquad\qquad \textit{if}\, n^* = n_1; & (5.23) \\ f^{h_{n_2}}(D), \qquad\qquad \textit{if}\, n^* = n_2. & (5.24) \end{cases}$$

Proof. We first prove that choosing a node $n \notin h_s$ is a dominated strategy for the interdictor. In fact,

$$\begin{aligned} \text{If } n \notin h_s &\Rightarrow \rho(n) = h_s \\ &\Rightarrow E_d(n \notin h_s, \rho(n)) {=} f^{h_s}(D) \leq E_d(n, \rho(n)) \ \ \forall n \in \mathcal{N}, \end{aligned}$$

since $f^{h_s}(D)$ is the shortest possible expected delivery time. Hence, the interdictor should always choose a node n that is part of a shortest O-to-D path, h_s.

For each $n \in h_s$, we let h_n denote a shortest O-to-D path not containing node n. Then, for $n \in h_s$,

$$\rho(n) {=} \begin{cases} h_s, \ \text{if } \frac{p_n}{1{-}p_n}(f^{h_s}(n){+}t_a){+}f^{h_s}(D){\leq}f^{h_n}(D); & (5.25) \\ h_n, \ \text{otherwise.} & (5.26) \end{cases}$$

Condition (5.25) indicates that U will still choose the shortest path even when the interdictor is located at n, since the expected delivery time of the risky shortest path is still better than the delivery time resulting from choosing the best alternative, i.e., deviating to the shortest path not containing node n. On the other hand, condition (5.26) states that the delay incurred by the presence of the attacker at node $n \in h_s$ leads U to deviate from the shortest path; choosing the best alternative, i.e., the shortest path not containing n.

In this respect, we let $\mathcal{N}_{h_s}$ denote the set of nodes that are part of h_s but are such that $\frac{p_n}{1-p_n}(f^{h_s}(n){+}t_a){+}f^{h_s}(D) \leq f^{h_n}(D)$. $\mathcal{N}_{h_s}$ is formally defined in (5.19).

Hence, the two possible alternatives for the optimal choice of I are n_1 and n_2 defined as:

$$n_1 = \underset{n \in \mathcal{N}_{h_s}}{\operatorname{argmax}} \Big[\frac{p_n}{1-p_n} (f^{h_s}(n) + t_a) + f^{h_s}(D) \Big], \tag{5.27}$$

and

$$n_2 = \underset{n \in h_s \setminus \mathcal{N}_{h_s}}{\operatorname{argmax}} f^{h_n}(D). \tag{5.28}$$

By the definition of n_1 and n_2 in respectively (5.27) and (5.28), U prefers n_1 over any other $n \in \mathcal{N}_{h_s}$, and U prefers n_2 over any other $n \in h_s \setminus \mathcal{N}_{h_s}$.

As a result, if I chooses n_1, the resulting expected delivery time will be:

$$E_d(n_1, \rho(n_1) = h_s) = \frac{p_{n_1}}{1-p_{n_1}} (f^{h_s}(n_1) + t_a) + f^{h_s}(D). \tag{5.29}$$

If I chooses n_2, the resulting expected delivery time is given by

$$E_d(n_2, \rho(n_2) = h_{n_2}) = f^{h_{n_2}}(D). \tag{5.30}$$

The interdictor will, hence, choose the best out of the two alternatives, n_1 or n_2 as follows:

$$n^* = \underset{n \in \{n_1, n_2\}}{\operatorname{argmax}} \Big(E_d\big(n_1, \rho(n_1)\big), E_d\big(n_2, \rho(n_2)\big) \Big), \tag{5.31}$$

which will result in SE stratgies of U and resulting expected delivery times as stated in (5.21)-(5.23).

□

This SE of the game characterizes the optimal interdiction and path selection strategies when the interdictor chooses deterministically the danger point from which to target the UAV. The SE highlights that selecting the shortest path, even if it contains the interdicted node, may still be the optimal path since it may result in an expected delivery time that is lower than all other alternative paths. This can occur, in particular, if the shortest path length, $f^{h_s}(D)$, is significantly shorter than the possible alternatives (as captured by the definition of $\mathcal{N}_{h_s}$ in (5.19).

Next, we analyze the case in which the interdictor chooses a probabilistic interdiction strategy. In that case, we provide the corresponding game formulation and analyze the resulting game equilibrium.

5.4 Game Analysis under Mixed Interdiction Strategies

In this section, we analyze the time-critical network interdiction game under a more general probabilistic choice of interdiction[5]. Here, the interdictor may prefer to choose a probabilistic (i.e. mixed) interdiction strategy to possibly prevent U from predicting their exact actions and, hence, potentially achieving a better outcome.

In this respect, an interdictor's mixed-strategy vector, $\boldsymbol{x} = [x_1, x_2, ..., x_N] \in \mathcal{X}$ specifies the probability, x_n, with which the interdictor plans to launch an attack on the UAV from each node $n \in \mathcal{N}$. Next, we show that when I chooses a mixed interdiction strategy $\boldsymbol{x}$, U's choice of optimal path turns into a Markov decision process (MDP) problem whose transition probabilities result from the choice $\boldsymbol{x}$ by I.

Consider the case in which I had chosen strategy $\boldsymbol{x} \in \mathcal{X}$ and the UAV was at node n, at time t_0, and then decides to go to a neighboring node $j \in \mathcal{N}_g(n)$. As such, U reaches node j at time $t_0 + t(i, j)$, at which point it could be subject to an attack. The probability with which the UAV is successfully attacked at node j, Pr(successfully attacked at node j) can be computed as:

$$\text{Pr}(\text{successfully attacked at node } j) = x_j p_j. \tag{5.32}$$

As a result, if the UAV has reached node i at time t_0 and then decided to go to node j next, it can either reach node j at time $t_0 + t(i, j)$ and not be successfully attacked at j (with probability $1 - x_j p_j$), or it can be brought back to the origin when reaching node j (i.e. if subject to a successful attack) with probability $x_j p_j$. This latter case implies that the UAV would reach node O at time $t_0 + t(i, j) + t_a$ with probability $x_j p_j$. This security problem can then be modeled as an MDP [221] whose transition probabilities depend on the security graph, $\mathcal{G}$, and on the choice $\boldsymbol{x}$ of I. We define the set of states of this MDP to be the set of nodes $\mathcal{N}$ of $\mathcal{G}$. The UAV operator can then decide to go from a node n to any of its neighboring nodes (i.e. next potential states). However, its transition to this state is stochastic, since if the attack is successful, instead of going to a neighboring node, the UAV transitions to state O.

The state transition probabilities denoted by $M\big(i, j; (\boldsymbol{x}, k)\big)$, specifying the probability of transitioning from state i to state j when the attacker chooses a mixed interdiction strategy $\boldsymbol{x}$ and the UAV operator chooses action[6] k (i.e. chooses to move from node i to node $k \in \mathcal{N}_g(i)$) deterministically, is defined as:

$$M\big(i, j; (\boldsymbol{x}, k)\big) = \begin{cases} (1 - x_k p_k), \text{ for } j = k, & (5.33) \\ x_k p_k, \text{ for } j = O, & (5.34) \\ 0, \text{ for } j \in \mathcal{N} \setminus \{O, k\}. & (5.35) \end{cases}$$

[5] Here we note that given the hierarchical structure of our game, considering mixed path selection policies by U would not yield any advantage regarding the achieved expected delivery time as compared to the optimal deterministic path selection policy. As such, we limit our analysis to deterministic path selection.

[6] Hereinafter, in the MDP analyses choosing action $k \in \mathcal{N}_g(i)$ refers to the UAV operator choosing to move its UAV from state (i.e. node) i to a neighboring node $k \in \mathcal{N}_g(i)$.

The instantaneous cost to U (reward to I) from a state transition from i to j when I chooses $\boldsymbol{x}$ and U chooses to move to node k, can be expressed as follows:

$$r\Big(i,j;\big(\boldsymbol{x},k\in\mathcal{N}_g(i)\big)\Big)=\begin{cases} t(i,k), \text{ for } j=k, & (5.36)\\ t(i,k)+t_a, \text{ for } j=O. & (5.37)\end{cases}$$

For every transition between two states, the UAV accumulates additional delivery time as expressed in (5.36) and (5.37), until the UAV reaches D and the game ends. The goal of U is hence to minimize this expected cumulative delivery time. Therefore, the choice of a mixed-strategy by the interdictor, $\boldsymbol{x}$, defines[7] an MDP with transition probabilities as defined in (5.33)-(5.35) and instantaneous reward/cost structure as shown in (5.36) and (5.37).

The goal of U is to choose the best MDP policy to minimize its expected accumulated delivery time. In this regard, a policy $\pi_{\boldsymbol{x}}$ specifies, for each node $n\in\mathcal{N}\setminus\{D\}$, the next node $n'\in\mathcal{N}_g(s)$ to which to go. Hence, at each state n, the set of feasible actions is given by $\mathcal{N}_g(n)$, and a policy constitutes choosing the action to take from each possible state. An optimal policy for U is thus a policy which minimizes the expected cumulative delivery time. We note that, given the state transitions in (5.33)-(5.35), a policy $\pi_{\boldsymbol{x}}$ practically results in one realizable O-to-D path denoted by $h_{\pi_{\boldsymbol{x}}}$. This is due to the fact that under the MDP policy $\pi_{\boldsymbol{x}}$, only the nodes of a certain path will ever be reached. Hence, a policy reduces to a path selection strategy. Given the equivalence between a policy $\pi_{\boldsymbol{x}}$ and its resulting O-to-D path $h_{\pi_{\boldsymbol{x}}}$, we next use the two notations interchangeably depending on whether the emphasis is on a general policy $\pi_{\boldsymbol{x}}$ or on its resulting path $h_{\pi_{\boldsymbol{x}}}$.

We define $E_{\pi_{\boldsymbol{x}}}(s;\boldsymbol{x})$ to be the value of the state s when U follows policy $\pi_{\boldsymbol{x}}$ for the MDP induced by the interdictor's mixed strategy, $\boldsymbol{x}$. In other words, $E_{\pi_{\boldsymbol{x}}}(s;\boldsymbol{x})$ is the expected time that the UAV needs to reach D from s when policy $\pi_{\boldsymbol{x}}$ is followed. Based on the transition probabilities and instantaneous reward structures in (5.33)-(5.37), we can express the values of the states, for a given policy $\pi_{\boldsymbol{x}}$, recursively; as follows:

$$E_{\pi_{\boldsymbol{x}}}(s;\boldsymbol{x})=\sum_{s'\in\{\pi_{\boldsymbol{x}}(s),O\}} M\Big(s,s';\big(\boldsymbol{x},\pi_{\boldsymbol{x}}(s)\big)\Big)\Big[r\big(s,s';(\boldsymbol{x},\pi_{\boldsymbol{x}}(s))\big)+E_{\pi_{\boldsymbol{x}}}(s';\boldsymbol{x})\Big]. \tag{5.38}$$

Of particular interest to our analysis is the value at the origin of the MDP, i.e. $E_{\pi_{\boldsymbol{x}}}(O;\boldsymbol{x})$, which constitutes the expected delivery time when following policy $\pi_{\boldsymbol{x}}$. In this respect, for a given choice $\boldsymbol{x}$ by the interdictor, the goal of the UAV operator is to find a policy $\pi^*_{\boldsymbol{x}}$ which minimizes $E_{\pi_{\boldsymbol{x}}}(O;\boldsymbol{x})$.

To this end, we define $E_{\pi^*_{\boldsymbol{x}}}(s;\boldsymbol{x})$ to be the optimal value at s – the minimum expected time for the UAV to reach D from s – resulting from the choice of optimal policy $\pi^*_{\boldsymbol{x}}$. We can now define the so-called Q-value of each state s, denoted by $Q_{\pi^*_{\boldsymbol{x}}}(s;(\boldsymbol{x},k))$, to be the expected time for the UAV

[7] Hence, hereinafter, we refer to this MDP as the MDP induced by $\boldsymbol{x}$.

to reach D from s when U chooses action k when at state s (i.e. chooses to go to node $k \in \mathcal{N}_g(s)$ when at node s) and then follows the optimal policy $\pi^*_{\boldsymbol{x}}$ afterwards. Hence, $Q_{\pi^*_{\boldsymbol{x}}}(s;(\boldsymbol{x},k))$ will be:

$$Q_{\pi^*_{\boldsymbol{x}}}(s;(\boldsymbol{x},k)){=}\sum_{s'\in\{k,O\}} M\big(s,s';(\boldsymbol{x},k)\big)[r\big(s,s';(\boldsymbol{x},k)\big){+}E_{\pi^*_{\boldsymbol{x}}}(s';\boldsymbol{x})] \tag{5.39}$$

$$={\big(}1{-}x_kp_k\big)\big(t(s,k){+}E_{\pi^*_{\boldsymbol{x}}}(k;\boldsymbol{x})\big){+}x_kp_k\big(t(s,k){+}t_a{+}E_{\pi^*_{\boldsymbol{x}}}(O;\boldsymbol{x})\big). \tag{5.40}$$

The Q-values at each state can be used to derive Bellman's equation for this MDP as follows:

$$E_{\pi^*_{\boldsymbol{x}}}(s;\boldsymbol{x}) = \min_{k\in\mathcal{N}_g(s)} Q_{\pi^*_{\boldsymbol{x}}}(s;(\boldsymbol{x},k)) \tag{5.41}$$

$$= \min_{k\in\mathcal{N}_g(s)} \sum_{s'\in\{k,O\}} M\big(s,s';(\boldsymbol{x},k)\big)[r\big(s,s';(\boldsymbol{x},k)\big) + E_{\pi^*_{\boldsymbol{x}}}(s';\boldsymbol{x})]. \tag{5.42}$$

Based on the recursive definition of the Bellman equation, the expected delivery time achieved for an interdiction strategy $\boldsymbol{x}$ and an MDP policy $\pi_{\boldsymbol{x}}$ inducing a path $h_{\pi_{\boldsymbol{x}}}$=(O, n_1, n_2, n_3, ..., n_r, n_l, n_k, n_m, D), containing $m+2$ ordered nodes, is derived in Proposition 4.

Proposition 4. *The MDP value at the origin, $E_{\pi_{\boldsymbol{x}}}(O;\boldsymbol{x})$, for a mixed interdiction strategy $\boldsymbol{x}$ and MDP policy $\pi_{\boldsymbol{x}}$, inducing path $h_{\pi_{\boldsymbol{x}}} = (O, n_1, n_2, n_3, ..., n_r, n_l, n_k, n_m, D)$, is given by:*

$$\begin{aligned} E_{\pi_{\boldsymbol{x}}}(O;\boldsymbol{x}) = t(n_m, D) + \frac{1}{1-x_Dp_D}\Bigg[& g(n_k,n_m,n_D) \\ & + \frac{1}{1-x_{n_m}p_{n_m}}\Bigg(g(n_l,n_k,n_m) + ... + \frac{1}{1-x_{n_3}p_{n_3}}\Bigg(g(n_1,n_2,n_3) \\ & + \frac{1}{1-x_{n_2}p_{n_2}}\big(g(O,n_1,n_2) + \frac{1}{1-x_{n_1}p_{n_1}} g(O,n_1)\underbrace{\big)\Big)...\Big)\Bigg]}_{m\ brackets}, \end{aligned} \tag{5.43}$$

where $g(.)$ is a function which takes either 2 or 3 inputs (2 or 3 consecutive nodes of a path $h_{\pi_{\boldsymbol{x}}}$, respectively) and which we define as follows (considering k, m, and n to be three consecutive nodes of a path $h_{\pi_{\boldsymbol{x}}}$):

$$g(k,m,n) = x_np_n(t(m,n)+t_a) + t(k,m), \tag{5.44}$$

$$g(m,n) = x_np_n(t(m,n)+t_a). \tag{5.45}$$

Proof. Consider a policy $\pi_{\boldsymbol{x}}$ such that $\pi_{\boldsymbol{x}}(n_i) = n_j$. Based on the transition probabilities in (5.33)-(5.35) and instantaneous reward structures in (5.36) and (5.37), the values of each two consecutive nodes, n_i and n_j (n_j being reached from n_i based on $\pi_{\boldsymbol{x}}$), are such that:

$$E_{\pi_{\boldsymbol{x}}}(n_i;\boldsymbol{x}) = (1 - x_{n_j}p_{n_j})\big(t(n_i,n_j) + E_{\pi_{\boldsymbol{x}}}(n_j;\boldsymbol{x})\big) + x_{n_j}p_{n_j}\big(t(n_i,n_j) + t_a + E_{\pi_{\boldsymbol{x}}}(O;\boldsymbol{x})\big). \tag{5.46}$$

Consider $\pi_{\boldsymbol{x}}$ to induce a certain path $h_{\pi_{\boldsymbol{x}}} = (O, n_1, n_2, n_3, ..., n_r, n_l, n_k, n_m, D)$. The expression in (5.46) can be used to relate the values of each two consecutive nodes of $h_{\pi_{\boldsymbol{x}}}$. As such, knowing that $E_{\pi_{\boldsymbol{x}}}(D;\boldsymbol{x}) = 0$ for each possible policy [8] and using the recursive expression in (5.46) applied for the consecutive nodes of $h_{\pi_{\boldsymbol{x}}}$, the expression of $E_{\pi_{\boldsymbol{x}}}(O;\boldsymbol{x}) = E_{h_{\pi_{\boldsymbol{x}}}}(O;\boldsymbol{x})$ given in (5.43) can be obtained. □

To solve the game, we define the SE in mixed strategies, as follows:

Definition 14. *A strategy pair* $(\boldsymbol{x}^*, \pi^*_{\boldsymbol{x}^*})$ *constitutes a* mixed interdiction Stackelberg equilibrium *(MSE) of the network interdiction game if*

$$\boldsymbol{x}^* = \underset{x\in\mathcal{X}}{\text{argmax}} E_{\pi^*_{\boldsymbol{x}}}(O;\boldsymbol{x}). \tag{5.47}$$

where

$$\pi^*_{\boldsymbol{x}^*} = \underset{\pi_{\boldsymbol{x}^*}\in\mathcal{P}}{\text{argmin}}\, E_{\pi_{\boldsymbol{x}^*}}(O;\boldsymbol{x}^*). \tag{5.48}$$

This MSE can be also equivalently defined in terms of $\boldsymbol{x}^*$ and the optimal path induced by $\pi^*_{\boldsymbol{x}^*}$, i.e., $(\boldsymbol{x}^*, h^* = h_{\pi^*_{\boldsymbol{x}^*}})$.

Next, we derive the MSE strategies in our game.

5.4.1 UAV's Problem Solution

The operator's problem consists of computing the optimal policy (or optimal path) for the MDP induced by $\boldsymbol{x}$. This can be achieved using known methods such as value iteration and policy iteration methods [221]. Indeed, for obtaining the values at each state (i.e. node) resulting from a policy $\pi_{\boldsymbol{x}}$ (known as policy evaluation), $E_{\pi_{\boldsymbol{x}}}(O;\boldsymbol{x})$ can be computed as shown in (5.43) and then used to find $E_{\pi_{\boldsymbol{x}}}(s;\boldsymbol{x})$ for each $s \in \mathcal{S}$ by starting from D (whose value is $E_{\pi_{\boldsymbol{x}}}(D;\boldsymbol{x}) = 0$) and moving backwards while applying (5.46). As such, using policy iteration [221], which is known to converge in finite-time to the optimal policy [221], starting from a certain MDP policy, the policy

[8] $E_{\pi_{\boldsymbol{x}}}(D;\boldsymbol{x}) = 0$ since the expected delivery time starting from D is equal to 0 since the UAV had already reached its destination.

evaluation and policy improvement steps, defined next, can be sequentially taken to converge to the optimal policy.

The policy iteration method follows the three steps below, i.e. 1) policy evaluation, 2) policy improvement, and 3) convergence test.

1. *Policy evaluation:* starting from a certain policy $\pi_{\boldsymbol{x}}^k$, evaluate $E_{\pi_{\boldsymbol{x}}^k}(s;\boldsymbol{x})$ for all $s \in \mathcal{S}$. This can be done as follows:
   (a) Find path $h_{\pi_{\boldsymbol{x}}^k}$ from O-to-D which results from policy $\pi_{\boldsymbol{x}}^k$,
   (b) Knowing $h_{\pi_{\boldsymbol{x}}^k}$, compute $E_{\pi_{\boldsymbol{x}}^k}(O;\boldsymbol{x})$ as shown in (5.43),
   (c) After computing $E_{\pi_{\boldsymbol{x}}^k}(O;\boldsymbol{x})$, and knowing that $E_{\pi_{\boldsymbol{x}}^k}(D;\boldsymbol{x}) = 0$, compute $E_{\pi_{\boldsymbol{x}}^k}(s;\boldsymbol{x})$ for every $s \in \mathcal{S}$ following (5.46).
2. *Policy improvement:* for each $s \in \mathcal{S}$, compute policy $\pi_{\boldsymbol{x}}^{k+1}(s)$, as follows
$$\pi_{\boldsymbol{x}}^{k+1}(s)=\underset{j\in\mathcal{N}_g(s)}{\operatorname{argmin}} \sum_{s'\in\{O,j\}} M(s,s';(\boldsymbol{x},j))(r(s,s';(\boldsymbol{x},j))+E_{\pi^k(\boldsymbol{x})}(s';\boldsymbol{x})). \tag{5.49}$$
3. *Convergence test:* repeat until $\pi^{k+1} = \pi^k$.

Next, we propose an alternative method for identifying U's problem solution which consists of searching over all the possible O-to-D paths. This method is dubbed the all-paths method and can be carried out by the following steps:

1. Find all possible paths, $\mathcal{H}$, from O to D
2. Evaluate $E_h(O;\boldsymbol{x})$ for each path $h \in \mathcal{H}$ using (5.43).
3. Find the optimal path h^* which solves:
$$h^* = \underset{h\in\mathcal{H}}{\operatorname{argmin}}\, E_h(O;\boldsymbol{x}). \tag{5.50}$$
4. Optional step: after computing $E_h(O;\boldsymbol{x})$, and given that $E_h(D;\boldsymbol{x}) = 0$, compute $E_h(s;\boldsymbol{x})$ for every $s \in \mathcal{S}$ as shown in (5.46).

Note that the last step of the all-paths method is not required. It is only included in case one wishes to compute the resulting optimal values at all of the states of the MDP.

The all-paths method does not seek to find the optimal action to be taken from each possible state, but rather an optimal O-to-D path. This equivalently corresponds to determining the next node to go to from only a subset of nodes (which collectively form a path). This approach is practical, since under a certain policy $\pi_{\boldsymbol{x}}$, the nodes that are not part of $h_{\pi_{\boldsymbol{x}}}$ will never be reached.

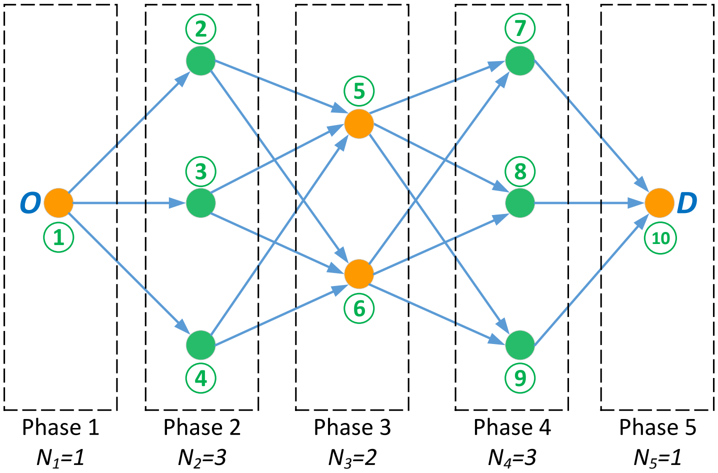

Figure 5.3: Phases-connected security graph with $A = 5$ phases.

Our proposed all-paths method is also guaranteed to converge after $H = |\mathcal{H}|$ iterations. In this respect, if the security graph, $\mathcal{G}$, can be split in phases in which each two consecutive phases form a complete bipartite graph[9] (as is the case in Fig. 5.2 and Fig. 5.3), H grows linearly in the number of nodes, N_i, in a given phase. Indeed, in a phase-connected graph with A phases, the total number of O-to-D paths is given by:

$$H = \prod_{i=1}^{A} N_i. \tag{5.51}$$

For example, in Fig. 5.3, $A = 5$ and $H = 1 \times 3 \times 2 \times 3 \times 1 = 18$.

Hence, for phase-connected $\mathcal{G}$, the number of needed iterations in the all-paths search method grows linearly in the number of nodes in a certain phase and each iteration is search-free and is only limited to arithmetic operations which can be efficiently performed. Here we note that having a phase-connected security graph is a condition that can typically occur in practice. In fact, in the security graph $\mathcal{G}$, the nodes represent danger points from which a cyber-physical attack can be launched against the UAV. These danger points represent locations such as high hills or high buildings which provide line of sight and spatial proximity to the UAV. Hence, when representing $\mathcal{G}$ by an interconnection of phases, this reflects the case in which the UAV goes from one set of danger points to the other (for example between sets of hills and sets of high buildings) with relatively safe conditions in between.

[9] We refer to such graphs as phase-connected graphs

5.4.2 Interdictor's Problem Solution

From the interdictor's side, after predicting the reaction $\pi^*_{\boldsymbol{x}}$ for a chosen interdcition strategy $\boldsymbol{x} \in \mathcal{X}$, I aims at solving the optimization problem defined in (5.47). The main challenge with solving this problem resides in the discontinuous changes in the objective function which can be induced by a slight modification to the chosen strategy $\boldsymbol{x}$. This due to the fact that a minimal change to the chosen $\boldsymbol{x}$ can lead to a complete modification of the resulting optimal reaction MDP policy of U, i.e. $\pi^*_{\boldsymbol{x}}$, leading to discontinuous changes to the objective function. Hence, due to the discontinuity of the objective function in (5.47), finding an exact globally optimal solution to the interdictor's problem may not be guaranteed. The search for such a global optimum can be done using heuristic methods such as pattern search based methods [222].

In its most standard form [222], pattern search methods involve repetitive local exploratory searches and pattern moves. The exploratory searches look for improving local search directions, while pattern moves consist of attempted larger moves in potential enhancing directions. Hence, such a search method is promising for solving I's problem since local exploratory searches can find small perturbations to $\boldsymbol{x}$ which improve the objective function and which may not induce a modification in the resulting optimal MPD policy, $\pi^*_{\boldsymbol{x}}$, while pattern moves allow exploration of changes to $\boldsymbol{x}$ whose magnitudes result in changes to $\pi^*_{\boldsymbol{x}}$, and hence, sudden changes to the objective function.

Hence, by using pattern search based methods[10] an achievable solution to the interdictor's problem can be obtained which leads to what we consider an *achievable MSE* in which the solution of (5.47) is obtained using a pattern search method while the solution of (5.48) is exactly characterized using, for example, the policy iteration method or the all-paths method.

5.5 Game Analysis under Cumulative Prospect Theory

As established in Section 5.3 and Section 5.4, given that the interdiction strategy and the success of a certain launched attack are stochastic, the decision regarding the optimal interdiction and path selection strategies are carried out under uncertainty. Indeed, every chosen interdiction strategy and path selection strategy will give rise to a *prospect*: A set of possible achievable delivery times each of which can occur with a certain probability. In fact, when I chooses $\boldsymbol{x}$ and U chooses path $h = (O, n_1, n_2, n_3, ..., n_r, n_l, n_k, n_m, D)$, and let $k_{n_i} \in \mathbb{N}_0$ be the number of times the UAV is successfully attacked at node $n_i \in h \setminus \{O, D\}$, then the possible achieved delivery times $T'(k_{n_1}, k_{n_2}, ..., k_{n_m})$ and their associated probability of occurrence, $\tau'(k_{n_1}, k_{n_2}, ..., k_{n_m})$, will be given by:

[10] Here, for the numerical solutions parts of our analysis, we use the pattern search method provided as part of the optimization toolbox of MATLAB, which uses a pattern search method that uses an adaptive mesh.

$$T'(k_{n_1},k_{n_2},...,k_{n_m}){=}f^h(D){+}k_{n_1}[f^h(n_1){+}t_a]{+}k_{n_2}[f^h(n_2){+}t_a]{+}...+k_{n_m}[f^h(n_m){+}t_a], \tag{5.52}$$

$$\begin{aligned}\tau'(k_{n_1},k_{n_2},...,k_{n_m}){=}&[(1{-}x_{n_1}p_{n_1})(1{-}x_{n_2}p_{n_2})...(1{-}x_{n_m}p_{n_m})][x_{n_1}p_{n_1}]^{k_{n_1}}[(1{-}x_{n_1}p_{n_1})(x_{n_2}p_{n_2})]^{k_{n_2}}\\ &\times ... \times [(1{-}x_{n_1}p_{n_1})(1{-}x_{n_2}p_{n_2})\times ... \times (1{-}x_{n_k}p_{n_k})x_{n_m}p_{n_m}]^{k_{n_m}}.\end{aligned} \tag{5.53}$$

The expression in (5.52) and (5.53), respectively reduce to (5.1) and (5.2) when considering pure interdiction (i.e. $x_n = 1$ and $x_{n'} = 0$ for all $n \in \mathcal{N} \setminus \{O, D, n\}$).

As such, the previous analyses in Section 5.3 and Section 5.4 have considered that the uncertainty is managed by I and U in a fully rational and objective manner. In other words, possible delivery times are considered to be absolute quantities which are assessed objectively and similarly by both players, and the probabilities of occurrence of these outcomes (for example, the probability of success of a launched attack, p_n) are equally and objectively perceived by I and U. As such, under full rationality, I and U assess a certain pair of strategies $(\boldsymbol{x}, h)$ by computing the expected value of their resulting prospect, i.e., $E_d(\boldsymbol{x}, h)$ and $E_{h_{\pi_{\boldsymbol{x}}}}(O; \boldsymbol{x})$. This full rationality assumption is considered in expected utility theory (EUT) and is widely used in classical game-theoretic (CGT) analyses [146].

However, given the time criticality of the studied drone applications (which must execute certain missions within a target time period), a certain achieved delivery time can be assessed subjectively and differently by U and I with respect to their chosen target delivery times, rather than as an absolute objective quantity. For example, in medical drone delivery applications, an achieved delivery time of $T^o + t^o$ when the target delivery time is T^o is typically observed as a t^o delay whose impact is subjectively assessed based on the criticality of the medical emergency situation. In addition, the perception of probabilities by U and I can be distorted and deviate from the rational objective perception. For example, the risk level of a certain chosen path or the probability of a successful attack can be perceived subjectively and differently by I and U. Indeed, as has been shown in a number of psychological empirical studies as well as behavioral experiments [148, 149], when faced with risk and experiencing uncertainty (similarly to our time-critical network interdiction game), the decision making processes of individuals can significantly deviate from full rationality. Essentially, when making decisions under uncertainty, individuals have been found to subjectively evaluate outcomes and perceive probabilities [148, 149].

Therefore, choosing an optimal strategy does not rely only on the expected value of the prospect it generates but rather on the subjectively assessed value of this prospect, which results from the way a delivery time is individually assessed with respect to the reference delivery time, and the way the different probabilities are subjectively perceived. Hence, the full rationality assumption in CGT cannot account for such subjective assessments of delivery times and distorted perception of probabilities.

To this end, to capture the interdictor's and UAV operator's potential subjective perceptions (i.e. *bounded rationality*), we incorporate the principles of *cumulative prospect theory* [148] in our game formulation. PT is a Nobel prize-winning theory which provides an alternative theory to decision making which has been shown to more accurately model and predict decision makers' subjective behavior, preferences, and valuations, as compared to EUT. Indeed, using PT, the subjective perception of the likelihood of occurrence of a probabilistic delivery time and the subjective evaluation of this delivery time with respect to a reference point becomes central to the decision making processes of I and U.

In a nutshell, considering a prospect $g(\phi_i, \eta_i)$, listing each possible outcome ϕ_i and its probability of occurrence η_i. In our analysis, each ϕ_i is a possible delivery time T' in (5.52) and η_i is its corresponding probability, τ_i', in (5.53). Under PT, the value of an outcome ϕ_i, denoted by $v(\phi_i)$, with respect to a reference point R, is given by [149]:

$$v(\phi_i) = \begin{cases} (\phi_i - R)^{\beta^+}, \text{ if } \phi_i \geq R, & (5.54) \\ -\lambda(-(\phi_i - R))^{\beta^-}, \text{ if } \phi_i < R, & (5.55) \end{cases}$$

where λ is known as the loss multiplier and β^+ and β^- are constant parameters which shape the value function.

Based on the sign of $v(\phi_i)$, g can be split into a negative prospect g^- and positive prospect g^+. For a maximizer (minimizer), the values in g^- correspond to losses (gains) and the values in g^+ correspond to gains (losses). Consider that g^- contains m terms, indexed from $-m$ to -1, and g^+ contains κ terms, indexed from 1 to κ. In addition, consider that each of the two prospects are ranked in ascending order based on the values, $v(\phi_i)$. Under cumulative prospect theory, the valuation of the positive and negative prospects, $V(g^+)$ and $V(g^-)$, are given by [149]:

$$V(g^+) = \sum_{i=1}^{\kappa} \pi_i^+ v(\phi_i), \tag{5.56}$$

$$V(g^-) = \sum_{i=-m}^{-1} \pi_i^- v(\phi_i), \tag{5.57}$$

resulting in the valuation of prospect g, denoted by $V(g)$, and which is given by

$$V(g) = V(g^+) + V(g^-). \tag{5.58}$$

In this regard, π_i^+ and π_i^- are decision weights defined based on the cumulative probability of occurrence of outcome ϕ_i as follows:

$$\pi_i^+ = \omega^+(\sum_{j=i}^{\kappa} \eta_i) - \omega^+(\sum_{j=i+1}^{\kappa} \eta_i), \tag{5.59}$$

$$\pi_i^- = \omega^-(\sum_{j=-m}^{i} \eta_i) - \omega^-(\sum_{j=-m}^{i-1} \eta_i), \tag{5.60}$$

where ω^+ and ω^- are the weighting functions associated with the positive and negative prospects, respectively, and are defined as follows (for a certain objective probability η):

$$\omega^+(\eta) = \frac{\eta^{\gamma^+}}{(\eta^{\gamma^+} + (1-\eta)^{\gamma^+})^{1/\gamma^+}}, \tag{5.61}$$

$$\omega^-(\eta) = \frac{\eta^{\gamma^-}}{(\eta^{\gamma^-} + (1-\eta)^{\gamma^-})^{1/\gamma^-}}, \tag{5.62}$$

where $\gamma^+ \in (0,1]$ and $\gamma^- \in (0,1]$ are known as the rationality parameters. The higher the value of the rationality parameter, the closer are $\omega^+(\eta)$ and $\omega^-(\eta)$ to the rational probability η.

The expressions in (5.59) and (5.60) showcase the way decision weights are formed from cumulative probabilities of outcomes in a prospect. In fact, for a maximizer, $\sum_{j=i}^{\kappa} \eta_i$ corresponds to the probability that the outcome is at least as good as ϕ_i while $\sum_{j=i+1}^{\kappa} \eta_i$ corresponds to the probability that the outcome is strictly better than ϕ_i. Equivalently, $\sum_{j=-m}^{i} \eta_i$ corresponds to the probability that the outcome is at least as bad as ϕ_i while $\sum_{j=-m}^{i-1}$ corresponds to the probability that the outcome is strictly worse than ϕ_i. Hence, these decision weights reflect the subjective perception of the probability of occurrence of the outcomes in a prospect.

Consequently, we will formulate our network interdiction game under cumulative prospect theory (which we call the PT game). We will also split our analysis of the PT game into two parts; the first focusing on pure interdiction strategies and the second on mixed interdiction. For each one of the two cases, we will investigate the resulting PT game as well as define and derive the equilibrium points of these games. In each of the two cases, we first derive the different PT valuations, by I and U, of each prospect which results from a certain pair of interdiction and path selection strategies. Based on these valuations, the equilibrium concepts for the introduced games are defined and then the equilibrium strategies are characterized.

Here, we note that the notations of the constants used in (5.54), (5.55), (5.61), and (5.62), i.e. λ, β^+, β^-, γ^+, and γ^-, will be constituently used in the analyses that ensues but will be indexed by I and U depending on the player to which they refer.

5.6 PT Game Analysis under Pure Strategies

5.6.1 PT Game Formulation under Pure Strategies

As discussed in Section 5.6.1, when U chooses path h and I is located on node $n \in h$, the possible outcomes, T_k, and their associated probability of occurrence, τ_k, for $k \in \mathbb{N}_0$, are as described, respectively, in (5.1) and (5.2). However, as PT predicts, the valuation of these outcomes as well as the perception of their probability of occurrence can be evaluated subjectively and differently by U and I. In this regard, when U chooses a path containing n, the possible outcomes T_k and their probability of occurrence result in the following prospect, $g(n \in h)$, in which the outcomes are ordered from lowest to highest, and is expressed as

$$\begin{aligned} g(n \in h) =& \big(f^h(D), q_n; f^h(D) + (f^h(n) + t_a), (1-q_n)q_n; \\ & \ldots; f^h(D) + k(f^h(n) + t_a), (1-q_n)^k q_n; \ldots\big). \end{aligned} \tag{5.63}$$

The interdictor and the UAV operator evaluate each possible outcome of this prospect subjectively, as shown in (5.54) and (5.55). In this regard, the valuation, v_k^I, that the interdictor gives to the k^{th} possible outcome, $T_k = f^h(D) + k(f^h(n) + t_a)$, is as follows:

$$v_k^I = \begin{cases} (\varDelta I_k)^{\beta_I^+}, \text{if } \varDelta I_k \geq 0, & (5.64) \\ -\lambda_I(-(\varDelta I_k))^{\beta_I^-}, \text{if } \varDelta I_k < 0, & (5.65) \end{cases}$$

where

$$\varDelta I_k = f^h(D) + k(f^h(n) + t_a) - R_I. \tag{5.66}$$

Given that the interdictor aims at maximizing the expected delivery time, achieving an expected delivery time that exceeds its reference expected delivery time (when $\varDelta I_k > 0$), is seen as a gain. On the other hand, when the achieved expected delivery time is lower than the reference point ($\varDelta I_k < 0$), the interdictor evaluates this outcome as a loss and values it accordingly.

Equivalently, the valuation, v_k^U, that the UAV operator gives to the k^{th} possible outcome, T_k, is as follows:

$$v_k^U = \begin{cases} \lambda_U(\varDelta U_k)^{\beta_U^-}, \text{if } \varDelta U_k > 0, & (5.67) \\ -(-(\varDelta U_k))^{\beta_U^+}, \text{if } \varDelta U_k \leq 0, & (5.68) \end{cases}$$

where

$$\varDelta U_k = f^h(D) + k(f^h(n) + t_a) - R_U. \tag{5.69}$$

Since U aims at minimizing the expected delivery time, $\varDelta U_k \geq 0$ is evaluated as a loss since it reflects the case in which the expected delivery time exceeds the target delivery time (i.e. U's reference point R_U). On the other hand, $\varDelta U_k < 0$ is viewed as a gain since it reflects the case in which the expected delivery time is below the target delivery time.

Next, based on PT principles, we derive the valuations that I and U give to each possible choice of pair of pure interdiction and path selection strategies (n, h). We denote these valuations by $V_I(n, h)$ and $V_U(n, h)$ for, respectively, I and U.

Proposition 5. *The cumulative prospect-theoretic valuation that I assigns to a strategy pair* (n, h) *is given by*

$$V_I(n,h) = \begin{cases} V_I(g_I(n \in h)), \text{ if } n \in h; & (5.70) \\ V_I(g_I(n \notin h)), \text{ if } n \notin h. & (5.71) \end{cases}$$

with

$$\begin{aligned} V_I(g_I(n \in h)) =& \sum_{i=0}^{k_I^-} -\lambda_I(-\varDelta I_i)^{\beta_i^-}\left(\omega_I^-\left(1-p_n^{i+1}\right)-\omega_I^-\left(1-p_n^i\right)\right) \\ &+\sum_{i=k_I^+}^{\infty}(\varDelta I_i)^{\beta_I^+}\left[\omega_I^+\left((p_n)^i\right)-\omega_I^+\left((p_n)^{i+1}\right)\right], \end{aligned} \tag{5.72}$$

where k_I^- *and* k_I^+ *are such that:* $\varDelta I_k < 0$ *for* $k \leq k_I^-$, $\varDelta I_k > 0$, *for* $k > k_I^+$, *and* $k_I^+ = k_I^- + 1$;

and

$$V_I(g_I(n \notin h)) = \begin{cases} (f^h(D)-R_I)^{\beta_I^+}, \text{ if } f^h(D) \geq R_I; \\ -\lambda_I(-(f^h(D)-R_I))^{\beta_I^-}, \text{if } f^h(D) < R_I. \end{cases} \tag{5.73}$$

Proof. We first start by considering the case in which $n \in h$. In this case, incorporating I's valuation of each possible outcome, based on (5.64) and (5.65), in prospect $g(n \in h)$, leads to the following prospect, $g_I(n \in h)$:

$$\begin{aligned} g_I(n \in h) = \Big(& -\lambda_I(-\varDelta I_0)^{\beta_I^-}, q_n; -\lambda_I(-\varDelta I_1)^{\beta_I^-}, (1-q_n)q_n; \ldots; -\lambda_I(-\varDelta I_{k_I^-})^{\beta_I^-}, (1-q_n)^{k_I^-} q_n; \\ & (\varDelta I_{k_I^+})^{\beta_I^+}, (1-q_n)^{k_I^+} q_n; \ldots; (\varDelta I_{k_I})^{\beta_I^+}, (1-q_n)^{k_I} q_n; \ldots \Big), \end{aligned} \tag{5.74}$$

such that $\varDelta I_k < 0$, for $k \leq k_I^-$, and $\varDelta I_k > 0$, for $k > k_I^+$; while $\varDelta I_k$ is as defined in (5.66) for $k \in \{0, 1, ..., k_I^-, k_I^+, ..., \infty\}$..

$g_I(n \in h)$ can be further split into a negative prospect, $g_I^-(n \in h)$, which includes the elements of $g_I(n \in h)$ with $\mathit{\Delta} I_k < 0$ (i.e. for $k \in \{0, ..., k_I^-\}$), and a positive prospect, $g_I^+(n \in h)$, which includes the elements of $g_I(n \in h)$ with $\mathit{\Delta} I_k > 0$ (i.e. for $k \geq k_I^+$). The negative prospect includes the outcomes that I values as losses, while the positive prospect includes outcomes that I values as gains. $g_I^-(n \in h)$ and $g_I^+(n \in h)$ are expressed as:

$$g_I^-(n \in h)=\Big(-\lambda_I(-\mathit{\Delta} I_0)^{\beta_I^-}, q_n; -\lambda_I(-\mathit{\Delta} I_1)^{\beta_I^-}, (1-q_n)q_n; \ldots; -\lambda_I(-\mathit{\Delta} I_{k_I^-})^{\beta_I^-}, (1-q_n)^{k_I^-} q_n\Big). \tag{5.75}$$

$$g_I^+(n \in h)=\Big((\mathit{\Delta} I_{k_I^+})^{\beta_I^+}, (1-q_n)^{k_I^+} q_n; \ldots; (\mathit{\Delta} I_{k_I})^{\beta_I^+}, (1-q_n)^{k_I} q_n; \ldots\Big). \tag{5.76}$$

We next consider the way I values this prospect by incorporating not only its subjective valuation of outcomes but also its cumulative weighting of the probability of occurrence of each of these outcomes. We let $V_I(g_I(n \in h))$ denote the PT value that I gives to prospect $g_I(n \in h)$, which results from the PT valuation of the negative and positive components of $g_I(n \in h)$,

$$V_I(g_I(n \in h)) = V_I(g_I^-(n \in h)) + V_I(g_I^+(n \in h)). \tag{5.77}$$

$$\begin{aligned} V_I(g_I^-(n \in h)) =& -\Big[\lambda_I(-\mathit{\Delta} I_0)^{\beta_I^-}\Big]\Big[\omega_I^-(q_n) - 0\Big] - \Big[\lambda_I(-\mathit{\Delta} I_1)^{\beta_I^-}\Big]\Big[\omega_I^-\big(q_n+(1-q_n)q_n\big) - \omega_I^-(q_n)\Big] - \\ & ... - \Big[\lambda_I(-\mathit{\Delta} I_{k_I^-})^{\beta_I^-}\Big]\Big[\omega_I^-\big(\sum_{i=0}^{k_I^-} q_n(1-q_n)^i\big) - \omega_I^-\big(\sum_{i=0}^{k_I^- -1} q_n(1-q_n)^i\big)\Big], \end{aligned} \tag{5.78}$$

where $\mathit{\Delta}_i$ is as defined in (5.66) for $i \in \{0, 1, ..., k_I^-\}$.

Hence,

$$V_I(g_I^-(n \in h)) = \sum_{i=0}^{k_I^-}\Bigg[- \lambda_I\Big((-\mathit{\Delta} I_i)^{\beta_i^-}\Big)\Big(\omega_I^-\big(\sum_{j=0}^{i} q_n(1-q_n)^j\big) - \omega_I^-\big(\sum_{j=0}^{i-1} q_n(1-q_n)^j\big)\Big)\Bigg]. \tag{5.79}$$

However, based on geometric series:

$$\sum_{j=0}^{i} q_n(1-q_n)^j = 1 - (1-q_n)^{i+1} = 1 - p_n^{i+1}, \tag{5.80}$$

and

$$\sum_{j=0}^{i-1} q_n(1-q_n)^j = 1 - p_n^i. \tag{5.81}$$

Replacing (5.80) and (5.81) in (5.79) results in

$$V_I(g_I^-(n\in h)) = \sum_{i=0}^{k_I^-} -\lambda_I(-\Delta I_i)^{\beta_i^-}\Big(\omega_I^-\big(1-p_n^{i+1}\big)-\omega_I^-\big(1-p_n^i\big)\Big). \tag{5.82}$$

A similar analysis can be carried out to obtain the expression of $V_I(g_I^+(n\in h))$. In this regard,

$$\begin{aligned} V_I(g_I^+(n\in h)) = & \Big[(\Delta I_{k_I^+})^{\beta_I^+}\Big]\Big[\omega_I^+\big(\sum_{i=k_I^+}^{\infty}(1-q_n)^i q_n\big)-\omega_I^+\big(\sum_{i=k_I^+ +1}^{\infty}(1-q_n)^i q_n\big)\Big]+\dots \\ & +\Big[(\Delta I_{k_I})^{\beta_I^+}\Big]\Big[\omega_I^+\big(\sum_{i=k_I}^{\infty}(1-q_n)^i q_n\big)-\omega_I^+\big(\sum_{i=k_I+1}^{\infty}(1-q_n)^i q_n\big)\Big]+\dots \qquad (5.83) \\ = & \sum_{i=k_I^+}^{\infty}(\Delta I_i)^{\beta_I^+}\Big[\omega_I^+\big(\sum_{j=i}^{\infty}(1-q_n)^j q_n\big) - \omega_I^+\big(\sum_{j=i+1}^{\infty}(1-q_n)^j q_n\big)\Big]. \qquad (5.84) \end{aligned}$$

In addition,

$$\begin{aligned} \sum_{j=i}^{\infty}(1-q_n)^j q_n = & q_n\Big(\sum_{j=0}^{\infty}(1-q_n)^j - \sum_{j=0}^{i-1}(1-q_n)^j\Big) \\ = & q_n\Big(\frac{1}{1-(1-q_n)} - \frac{1-(1-q_n)^i}{1-(1-q_n)}\Big) = (1-q_n)^i = p_n^i. \qquad (5.85) \end{aligned}$$

Hence, the result in (5.85) can be used to simplify the expression in (5.84) leading to

$$V_I(g_I^+(n\in h)) = \sum_{i=k_I^+}^{\infty}(\Delta I_i)^{\beta_I^+}\Big[\omega_I^+\big((p_n)^i\big)-\omega_I^+\big((p_n)^{i+1}\big)\Big]. \tag{5.86}$$

Hence, computing $V_I(g_I^-(n\in h))$ and $V_I(g_I^+(n\in h))$ as in (5.82) and (5.86), respectively, allows computation of the value that I assigns to prospect $g(n\in h)$, resulting from choosing a node n

that is part of path h taken by U. This computation can be done as shown in (5.77) and results in

$$\begin{aligned} V_I(g_I(n \in h)) = & \sum_{i=0}^{k_I^-} -\lambda_I(-\mathit{\Delta} I_i)^{\beta_i^-} \left(\omega_I^-\left(1-p_n^{i+1}\right)-\omega_I^-\left(1-p_n^i\right)\right) \\ & + \sum_{i=k_I^+}^{\infty} (\mathit{\Delta} I_i)^{\beta_I^+} \left[\omega_I^+\left((p_n)^i\right)-\omega_I^+\left((p_n)^{i+1}\right)\right], \end{aligned} \tag{5.87}$$

where $k_I^+ = k_I^- + 1$.

Now, we consider the case in which $n \notin h$. When the chosen path h taken by the UAV does not include the interdiction node n, the resulting delivery time does not result in a probabilistic prospect but is rather deterministic and equal to $f^h(D)$ with a probability equal to 1. This deterministic prospect is formally represented as

$$g(n \notin h) = (f^h(D), 1). \tag{5.88}$$

As PT predicts, this achieved delivery time, when $n \notin h$, is subjectively valued by I depending on whether it is larger than its target delivery time R_I (gain scenario) or smaller than its target delivery time (loss scenario). Hence, the value that I associates to prospect $g_I(n \notin h)$, denoted by $V_I(g_I(n \notin h))$, is:

$$V_I(g_I(n \notin h)) = \begin{cases} (f^h(D)-R_I)^{\beta_I^+}, \text{if } f^h(D) \geq R_I; \\ -\lambda_I(-(f^h(D)-R_I))^{\beta_I^-}, \text{if } f^h(D) < R_I. \end{cases} \tag{5.89}$$

Hence, the valuation, $V_I(n, h)$, that the interdictor assigns to a strategy pair (n, h), in which the interdictor is located at node n and U takes path h, is given by

$$V_I(n,h) = \begin{cases} V_I(g_I(n \in h)), \text{ if } n \in h; & (5.90) \\ V_I(g_I(n \notin h)), \text{ if } n \notin h. & (5.91) \end{cases}$$

□

Proposition 6. *The cumulative prospect-theoretic valuation that U assigns to a strategy pair (n, h) is given by*

$$V_U(n,h) = \begin{cases} V_U(g_U(n \in h)), \textit{ if } n \in h; & (5.92) \\ V_U(g_U(n \notin h)), \textit{ if } n \notin h. & (5.93) \end{cases}$$

with

$$
\begin{aligned}
V_U(g_U(n \in h)) = &\sum_{i=0}^{k_U^-} -(-\mathit{\Delta} U_i)^{\beta_U^+}\left(\omega_U^+(1-p_n^{i+1})-\omega_U^+(1-p_n^{i})\right) \\
&+\sum_{i=k_U^+}^{\infty} \lambda_U(\mathit{\Delta} U_i)^{\beta_U^-}\Big(\omega_U^-\left((p_n)^i\right)-\omega_U^-\left(p_n^{(i+1)}\right)\Big), \qquad (5.94)
\end{aligned}
$$

where k_U^- and k_U^+ are such that: $\mathit{\Delta} U_k < 0$ for $k \leq k_U^-$, $\mathit{\Delta} U_k > 0$ for $k \geq k_U^+$, and $k_U^+ = k_U^- + 1$;

and

$$
V_U(g_U(n \notin h)) = \begin{cases} -(-(f^h(D) - R_U))^{\beta_U^+}, \text{ if } f^h(D) \leq R_U; \\ \lambda_U(f^h(D) - R_U)^{\beta_U^-}, \text{ if } f^h(D) > R_U. \end{cases} \qquad (5.95)
$$

Proof. We first start with the case in which $n \in h$. Incorporating U's valuation of each possible outcome, based on (5.67) and (5.68), in prospect $g(n \in h)$, leads to prospect $g_U(n \in h)$ defined as follows:

$$
\begin{aligned}
g_U(n \in h) = \Big(&-(-\mathit{\Delta} U_0)^{\beta_U^+}, q_n; -(-\mathit{\Delta} U_1)^{\beta_U^+}, (1-q_n)q_n; ...; -(-\mathit{\Delta} U_{k_U^-})^{\beta_U^+}, (1-q_n)^{k_U^-}q_n; \\
&\lambda_U(\mathit{\Delta} U_{k_U^+})^{\beta_U^-}, (1-q_n)^{k_U^+}q_n; ...; \lambda_U(\mathit{\Delta} U_{k_U})^{\beta_U^-}, (1-q_n)^{k_U}q_n; ...\Big), \qquad (5.96)
\end{aligned}
$$

such that $\mathit{\Delta} U_k < 0$ for $k \leq k_U^-$ and $\mathit{\Delta} U_k > 0$ for $k \geq k_U^+$; while $\mathit{\Delta} U_k$ is as defined in (5.69) for $k \in \{0, 1, ..., k_U^-, k_U^+, ..., \infty\}$.

Prospect $g_U(n \in h)$ can be split into a negative (for $\mathit{\Delta} U_k \leq 0$) and a positive prospect (for $\mathit{\Delta} U_k > 0$), denoted by $g_U^-(n \in h)$ and $g_U^+(n \in h)$, respectively. In this case, the negative prospect represents a gain for the UAV operator, since it corresponds to delivery times that are shorter than the target delivery time, while a positive prospect is a loss for the UAV operator, since it corresponds to delivery times that are longer than the target delivery time. The negative and positive prospects are then defined as

$$
g_U^-(n \in h) = \Big(-(-\mathit{\Delta} U_0)^{\beta_U^+}, q_n; ...; -(-\mathit{\Delta} U_{k_U^-})^{\beta_U^+}, (p_n)^{k_U^-}q_n\Big) \qquad (5.97)
$$

and

$$
g_U^+(n \in h) = \Big(\lambda_U(\mathit{\Delta} U_{k_U^+})^{\beta_U^-}, (p_n)^{k_U^+}q_n; ...; \lambda_U(\mathit{\Delta} U_{k_U})^{\beta_U^-}, (p_n)^{k_U}q_n; ...\Big). \qquad (5.98)
$$

The PT valuation that U assigns to $V_U(g_U^-(n \in h))$ can be computed as follows:

$$
\begin{aligned}
V_U(g_U^-(n\in h)) &= \sum_{i=0}^{k_U^-}\Big[-(-\mathit{\Delta}U_i)^{\beta_U^+}\Big(\omega_U^+\big(\sum_{j=0}^{i}(p_n)^j q_n\big) - \omega^+\big(\sum_{j=0}^{i-1}(p_n)^j q_n\big)\Big)\Big] \\
&= \sum_{i=0}^{k_U^-} -(-\mathit{\Delta}U_i)^{\beta_U^+}\big(\omega_U^+(1-p_n^{i+1}) - \omega_U^+(1-p_n^i)\big),
\end{aligned} \tag{5.99}
$$

where the second equality holds since $\sum_{j=0}^{i-1}(p_n)^j q_n = 1 - p_n^i$, as has been shown in (5.81).

In addition, the PT valuation that U assigns to $V_U(g_U^+(n\in h))$ can be computed as follows:

$$
\begin{aligned}
V_U(g_U^+(n\in h)) &= \sum_{i=k_U^+}^{\infty}\Big[\lambda_U(\mathit{\Delta}U_i)^{\beta_U^-}\Big(\omega_U^-\big(\sum_{j=i}^{\infty}(p_n)^j q_n\big) - \omega_U^-\big(\sum_{j=i+1}^{\infty}(p_n)^j q_n\big)\Big)\Big] \\
&= \sum_{i=k_U^+}^{\infty}\lambda_U(\mathit{\Delta}U_i)^{\beta_U^-}\Big(\omega_U^-\big((p_n)^i\big) - \omega_U^-\big(p_n^{(i+1)}\big)\Big),
\end{aligned} \tag{5.100}
$$

where the second equality holds since $\sum_{j=i}^{\infty}(p_n)^j q_n = p_n^i$ as shown in (5.85).

Therefore,

$$
\begin{aligned}
V_U(g_U(n\in h)) &= V_U(g_U^-(n\in h)) + V_U(g_U^+(n\in h)) \\
&= \sum_{i=0}^{k_U^-} -(-\mathit{\Delta}U_i)^{\beta_U^+}\big(\omega_U^+(1-p_n^{i+1}) - \omega_U^+(1-p_n^i)\big) \\
&\quad + \sum_{i=k_U^+}^{\infty}\lambda_U(\mathit{\Delta}U_i)^{\beta_U^-}\Big(\omega_U^-\big((p_n)^i\big) - \omega_U^-\big(p_n^{(i+1)}\big)\Big),
\end{aligned} \tag{5.101}
$$

where $k_U^+ = k_U^- + 1$.

Now, we consider the case in which $n \notin h$ resulting in a deterministic prospect $g(n \notin h) = (f^h(D), 1)$. This deterministic prospect is valued by U as a gain, in case $f^h(D) \leq R_U$, and as a loss in case $f^h(D) > R_U$. Hence, the valuation, $V_U(g(n \notin h))$, that U assigns to $g(n \notin h)$ is:

$$
V_U(g_U(n\notin h)) = \begin{cases} -(-(f^h(D)-R_U))^{\beta_U^+}, & \text{if } f^h(D) \leq R_U; \\ \lambda_U(f^h(D)-R_U)^{\beta_U^-}, & \text{if } f^h(D) > R_U. \end{cases} \tag{5.102}
$$

Hence, the valuation, $V_U(n,h)$, that U assigns to a strategy pair (n,h), in which the interdictor is located at node n and U takes path h, is given by

$$
V_U(n,h) = \begin{cases} V_U(g_U(n\in h)), & \text{if } n \in h; \qquad (5.103) \\ V_U(g_U(n\notin h)), & \text{if } n \notin h. \qquad (5.104) \end{cases}
$$

□

As shown in (5.72) and (5.94), $V_I(g(n \in h))$ and $V_U(g(n \in h))$ correspond to infinite summations, i.e. infinite series. Hence, to compare between possible pairs of strategies (n, h), based on their valuations $V_I(n, h)$ and $V_U(n, h)$, and identify the equilibrium strategy pair, it is necessary for these sums to converge. We next show in Proposition 7 and Proposition 8 that $V_I(g(n \in h))$ and $V_U(g(n \in h))$ are convergent series.

Proposition 7. *$V_I(g(n \in h))$ is a convergent series.*

Proof. For proving the convergence of $V_I(g(n \in h))$, we next prove that $V_I(g_I^+(n \in h))$, defined in (5.86), converges. In this regard, we prove that $V_I(g_I^+(n \in h))$, which is composed of positive terms, converges using what is know as the *ratio test*. Following the ratio test, for a series $\sum_{n=1}^{\infty} a_n$ with positive terms a_n, L is defined as $L = \lim\limits_{n\to\infty} |\frac{a_{n+1}}{a_n}|$. In this respect, if $L < 1$, then $\sum_{n=1}^{\infty} a_n$ converges.

As such, we refer to the k^{th} term of $V_I(g_I^+(n \in h))$ by $V_k^{I^+}$, which is given by

$$V_k^{I^+} = (\mathit{\Delta} I_k)^{\beta_I^+}\left[\omega_I^+\left((p_n)^k\right) - \omega_I^+\left((p_n)^{k+1}\right)\right]. \tag{5.105}$$

where

$$\omega_I^+(p_n^k) = \frac{p_n^{k\gamma_I^+}}{(p_n^{k\gamma_I^+} + (1 - p_n^k)^{\gamma_I^+})^{1/\gamma_I^+}}. \tag{5.106}$$

In this respect,

$$L = \lim_{k\to\infty} \frac{V_{k+1}^{I+}}{V_k^{I+}} = \frac{p_n^{(k+1)\gamma_I^+} - p_n^{(k+2)\gamma_I^+}}{p_n^{k\gamma_I^+} - p_n^{(k+1)\gamma_I^+}} = \frac{p_n^{\gamma_I^+} - p_n^{2\gamma_I^+}}{1 - p_n^{\gamma_I^+}} = p_n^{\gamma_I^+} < 1$$
$$\Rightarrow V_I(g_I^+(n \in h)) \text{ converges } \Rightarrow V_I(g(n \in h)) \text{ converges.}$$

□

Proposition 8. *$V_U(g(n \in h))$ is a convergent series.*

Proof. To prove the convergence of $V_U(g(n \in h))$, we prove that $V_U(g_U^+(n \in h))$, defined in (5.100), converges using the ratio test (similarly to the test carried out in Proposition 7).

As such, we denote the k^{th} term of $V_U(g_U^+(n \in h))$ by $V_k^{U^+}$, which is given by

$$V_k^{U^+} = \lambda_U(\mathit{\Delta} U_k)^{\beta_U^-}\left[\omega_U^-\left((p_n)^k\right) - \omega_U^-\left((p_n)^{k+1}\right)\right]. \tag{5.107}$$

where

$$\omega_U^-(p_n^k) = \frac{p_n^{k\gamma_U^-}}{(p_n^{k\gamma_U^-} + (1 - p_n^k)^{\gamma_U^-})^{1/\gamma_U^-}}. \tag{5.108}$$

In this respect,

$$L = \lim_{k\to\infty} \frac{V_{k+1}^{U+}}{V_k^{U+}} = p_n^{\gamma_I^-} < 1$$
$$\Rightarrow V_U(g_U^+(n \in h)) \text{ converges } \Rightarrow V_U(g(n \in h)) \text{ converges.}$$

□

Hence, under PT, the pure-strategy equilibrium of the game is based on the personal valuations, $V_I(n,h)$ and $V_U(n,h)$, that I and U respectively assign to the prospect resulting from the choice of any strategy pair (n,h). This is in contrast to the game under full rationality in which both players assess a strategy pair equally and objectively based on the resulting expected delivery time, $E_d(n,h)$. As such, under PT, the game becomes a nonzero-sum game which introduces additional challenges for identifying the equilibrium strategies. In this regard, we next identify and analyze the SE of our PT game.

5.6.2 PT Game Equilibrium in Pure Strategies

Equivalently to the analysis in Section 5.3.2, U can optimally react to a decision n that had been taken by I. However, under the PT game, this optimal reaction is based on the valuation $V_U(n,h)$ rather than the expected delivery time $E_d(n,h)$. In this PT game, we denote the choice of a path $h \in \mathcal{H}$ by U, as an optimal reaction to a node $n \in \mathcal{N}$ that had been chosen by I, by $\rho^{\text{PT}}(n)$. $\rho^{\text{PT}}(n)$ is formally defined as:

$$\rho^{\text{PT}}(n) = \underset{h\in\mathcal{H}}{\operatorname{argmin}}\, V_U(n,h), \tag{5.109}$$

where $V_U(n,h)$ is as derived in Proposition 6.

Equivalently to the SE for the fully rational game in Definition 13, an SE for the PT game (SE-PT), is defined as follows.

Definition 15. *A strategy pair* $(\tilde{n}^*, \tilde{h}^*)$ *constitutes a* Stackelberg equilibrium of the PT game *if*

$$V_I(\tilde{n}^*, \tilde{h}^* = \rho^{PT}(\tilde{n}^*)) \geq V_I(n, \rho^{PT}(n)) \textit{ for all } n \in \mathcal{N}, \tag{5.110}$$

where $V_I(n,h)$ *is as defined in (*5.70*) and (*5.71*) for, respectively,* $h \supset n$ *(i.e.* $n \in h$*) and* $n \notin h$*, and* $\rho^{PT}(n)$ *is as defined in (*5.127*).*

As such, the interdictor's problem corresponds to choosing $\tilde{n}^*$ which solves:

$$\tilde{n}^* = \underset{n\in\mathcal{N}}{\operatorname{argmax}}\, V_I(n, \rho^{\text{PT}}(n)). \tag{5.111}$$

Following a similar logic used for the derivation of the SE in Theorem 9, the SE-PT can be analytically characterized as shown in Theorem 10.

Theorem 10. *The interdictor's SE-PT strategy, $\tilde{n}^*$, is given by:*

$$\tilde{n}^* = \underset{n \in \{m_1, m_2\}}{\operatorname{argmax}} \Big(V_I(m_1, \rho^{PT}(m_1)), V_I(m_2, \rho^{PT}(m_2)) \Big), \tag{5.112}$$

where

$$m_1 = \underset{n \in \mathcal{M}_{h_s}}{\operatorname{argmax}} V_I(n \in h_s), \tag{5.113}$$

$$\mathcal{M}_{h_s} = \{n \in h_s | V_U(n \in h_s) \leq V_U(n, h_n)\}, \tag{5.114}$$

h_n is the shortest O-to-D path not containing node n, and

$$m_2 = \underset{n \in h_s \backslash \mathcal{M}_{h_s}}{\operatorname{argmax}} V_I(n \notin h_n). \tag{5.115}$$

The resulting UAV operator's SE-PT strategy is given by

$$\tilde{h}^* = \rho^{PT}(\tilde{n}^*) = \begin{cases} h_s, \text{ if } \tilde{n}^* = m_1; & (5.116) \\ h_{m_2}, \text{ if } \tilde{n}^* = m_2. & (5.117) \end{cases}$$

Proof. The proof follows similar steps as the proof of Theorem 9. For convenience, a sketch of the proof is provided next. The complete details of the proof can be generated by following the steps of the proof of Theorem 9.

U's response to a choice $n \in h_s$ by I will either be h_s or h_n. I always has an incentive to choose $n \in h_s$, since otherwise, $\rho^{\mathrm{PT}}(n) = h_s$, which results in the worst possible $V_I(n, h)$ to the interdictor. However, choosing an $n \in h_s$ might also lead U to deviate from h_s and choose the best alternative h_n. Hence, I can split the nodes in h_s into two sets, $\mathcal{M}_{h_s}$ and $\mathcal{N} \setminus \mathcal{M}_{h_s}$. The nodes in $\mathcal{M}_{h_s}$ consist of the nodes of h_s which are such that, even when I is located at an $n \in \mathcal{M}_{h_s}$, U still prefers taking path h_s. This will lead to the valuation $V_I(n \in h_s)$ for the interdictor. On the other hand, choosing a node $n \in \mathcal{N} \setminus \mathcal{M}_{h_s}$ leads U to choosing path h_n instead of h_s. This will result in the valuation $V_I(n \in h_s, h_n \neq h_s)$ for the interdictor.

Hence, m_1 and m_2 in (5.113) and (5.113) represent the best node that I can choose from each of the two sets, $\mathcal{M}_{h_s}$ and $\mathcal{N} \setminus \mathcal{M}_{h_s}$, respectively. As such, $\tilde{n}^*$ in (5.112) corresponds to choosing the best of these two alternatives, and $\tilde{h}^*$ in (5.116) and (5.117) correspond to choosing the best reaction ρ^{PT} by U to the choice made by I. □

Hence, Theorem 10 analytically characterizes the SE of the PT game, which can be compared to the SE of the conventional game derived in Theorem 9. This comparison enables us to analyze the effect of the players' subjective PT valuations and decision weights on their chosen equilibrium strategies. Indeed, a main component of the choice of the SE and and SE-PT strategies is the characterization of sets $\mathcal{N}_{h_s}$, in (5.19), and $\mathcal{M}_{h_s}$, in (5.114). By comparing (5.19) and (5.114), we can see that $\mathcal{N}_s$ relies on the comparison between $\frac{p_n}{1-p_n}(f^{h_s}(n) + t_a) + f^{h_s}(D)$ and $f^{h_n}(D)$ for each $n \in h_s$. On the other hand, $\mathcal{M}_{h_s}$ relies on comparing $V_U(n \in h_s)$, which can be obtained from (5.94), with $V_U(n, h_n)$, which can be obtained from (5.95). Hence, this difference in $\mathcal{N}_{h_s}$ and $\mathcal{M}_{h_s}$ enable possible deviation of the SE-PT strategies from the SE strategies.

Next, we formulate, analyze, and characterize equilibrium solutions to the PT game considering mixed interdiction strategies.

5.7 PT Game Analysis under Mixed Interdiction Strategies

5.7.1 PT Game formulation under Mixed Interdiction

In Section 5.4, we introduced and analyzed the time-critical network interdiction game resulting from a probabilistic (i.e. mixed) choice of interdiction strategies. In this regard, the analysis in Section 5.4 considered fully rational objective players. Next, we incorporate the concepts and principles of PT into the mixed-interdiction game formulation.

Consider the case in which I chooses $\boldsymbol{x}$ and U chooses a policy that induces path $h = (O, n_1, n_2, n_3, ..., n_r, n_l, n_k, n_m, D)$. Then, the resulting possible delivery times, $T'(k_{n_1}, k_{n_2}, ..., k_{n_m})$, and their associated probability of occurrence, $\tau'(k_{n_1}, k_{n_2}, ..., k_{n_m})$, as given by (5.52) and (5.53) where $k_{n_i} \in \mathbb{N}_0$ is the number of times the UAV is successfully attacked at a node $n_i \in h \backslash \{O, D\}$.

Hence, the interdiction strategy $\boldsymbol{x}$, by I, and response path h, by U, result in a prospect $\mathit{\Gamma}(\boldsymbol{x}, h)$ in which each outcome $T'(k_{n_1}, k_{n_2}..., k_{n_m})$ occurs with probability $\tau'(k_{n_1}, k_{n_2}..., k_{n_m})$. Under PT, rather than relying on the expected value of this prospect to compare strategy pairs $(\boldsymbol{x}, h) \in \mathcal{X} \times \mathcal{H}$, each of I and U generates a personal valuation of this prospect. As a result, their choices of optimal mixed interdiction and path selection strategies are based on these PT valuations.

In this regard, given (5.52) and (5.53), as well as the value and weighting functions introduced in (5.54), (5.55), (5.61), and (5.62), we can generate the valuations assigned by I and U, $\mathit{\Xi}_I(\boldsymbol{x}, h)$ and $\mathit{\Xi}_U(\boldsymbol{x}, h)$, to prospect $\mathit{\Gamma}(\boldsymbol{x}, h)$ by following the steps introduced in Section 5.5 and applied in Section 5.6.1.

In this respect, we next provide detailed derivations of $\mathit{\Xi}_I(\boldsymbol{x}, h)$, and $\mathit{\Xi}_U(\boldsymbol{x}, h)$.

Interdictor's PT Valuation of $\mathit{\Gamma}(\boldsymbol{x}, h)$

Starting with the interdictor's PT valuation of $\mathit{\Gamma}(\boldsymbol{x}, h)$, I values each outcome $T'(k_{n_1}, k_{n_2}..., k_{n_m})$ of prospect $\mathit{\Gamma}(\boldsymbol{x}, h)$ based on its reference point R_I. Therefore, the valuation that I assigns to

$T'(k_{n_1},k_{n_2}...,k_{n_m})$, denote by $\xi_I(k_{n_1},k_{n_2}...,k_{n_m})$, is:

$$\xi_I(k_{n_1},k_{n_2}...,k_{n_m})=\begin{cases}-\lambda_I(-(T'(k_{n_1},k_{n_2},...,k_{n_m})-R_I))^{\beta_I^-}, \\ \text{ if } T'(k_{n_1},k_{n_2}...,k_{n_m}) < R_I; \\ (T'(k_{n_1},k_{n_2},...,k_{n_m})-R_I)^{\beta_U^+}, \\ \text{ if } T'(k_{n_1},k_{n_2}...,k_{n_m}) \geq R_I. \end{cases} \tag{5.118}$$

Based on their signs, the different $\xi_I(k_{n_1},k_{n_2}...,k_{n_m})$ can be split into (and sorted from low to high) into a negative vector and a positive vector, denoted respectively by Γ_I^- and Γ_I^+. In this respect, Γ_I^- contains κ_I^- elements while Γ_I^+ contain an infinite number of elements. We denote the first element of Γ_U^+ by $\Gamma_I^+(\kappa_I^+)$ where $\kappa_I^+ = \kappa_I^- + 1$. We let $\Gamma_U^+(i)$ and $\Gamma_I^+(i)$ denote generic elements of Γ_U^- and Γ_U^+, respectively.

In addition, we let $\hat{\tau}_k^-$ and $\hat{\tau}_k^+$ denote the probabilities of occurrence of elements $\Gamma_I^-(k)$ and $\Gamma_I^+(k)$, respectively. Therefore, the elements of Γ_I^- and Γ_I^+ with their associated probabilities constitute the negative and positive portions of $\Gamma(\boldsymbol{x},h)$, as valued by I, denoted by $\Gamma_I^-(\boldsymbol{x},h)$ and $\Gamma_I^+(\boldsymbol{x},h)$.

The valuations by I of Γ_I^- and Γ_I^+, denoted respectively by $\Xi_I^-(\Gamma_I^-)$ and $\Xi_I^+(\Gamma_I^+)$, can be computed as follows:

$$\Xi_I^-(\Gamma_I^-) = \sum_{i=1}^{\kappa_I^-} \Gamma_I^-(i)\Big[\omega_I^-\Big(\sum_{j\leq i}\hat{\tau}_j\Big) - \omega_I^-\Big(\sum_{j<i}\hat{\tau}_j\Big)\Big]. \tag{5.119}$$

$$\Xi_I^+(\Gamma_I^+) = \sum_{i=\kappa_I^+}^{\infty} \Gamma_I^+(i)\Big[\omega_I^+\Big(\sum_{j\geq i}\hat{\tau}_j\Big) - \omega_I^+\Big(\sum_{j>i}\hat{\tau}_j\Big)\Big]. \tag{5.120}$$

Therefore, the valuation, $\Xi_I(\boldsymbol{x},h)$, that I assigns to prospect $\Gamma(\boldsymbol{x},h)$ resulting from the strategy pair $(\boldsymbol{x},h))$ is

$$\Xi_I(\boldsymbol{x},h) = \Xi_I^-(\Gamma_I^-) + \Xi_I^+(\Gamma_I^+). \tag{5.121}$$

In an equivalent manner, the UAV operator's PT valuation of $\Gamma(\boldsymbol{x},h)$ can be computed, as shown next.

UAV Operator's PT Valuation of $\Gamma(\boldsymbol{x},h)$

With regard to the UAV operator, each outcome $T'(k_{n_1},k_{n_2}...,k_{n_m})$ of prospect $\Gamma(\boldsymbol{x},h)$ is valued based on U's reference point R_U. In this respect, the valuation that U assigns to $T'(k_{n_1},k_{n_2}...,k_{n_m})$, which we denote by $\xi_U(k_{n_1},k_{n_2}...,k_{n_m})$, is as follows:

$$\xi_U(k_{n_1},k_{n_2}...,k_{n_m})=\begin{cases}-(-(T'(k_{n_1},k_{n_2},...,k_{n_m})-R_U))^{\beta_U^+}, \\ \text{ if } T'(k_{n_1},k_{n_2}...,k_{n_m})\leq R_U; \\ \lambda_U(T'(k_{n_1},k_{n_2},...,k_{n_m})-R_U)^{\beta_U^-}, \\ \text{ if } T'(k_{n_1},k_{n_2}...,k_{n_m}) > R_U. \end{cases} \tag{5.122}$$

The different $\xi_U(k_{n_1},k_{n_2}...,k_{n_m})$ can be split into two vectors (with sorted elements from low to high) based on their signs. We denote the negative vector by $\mathit{\Gamma}_I^-$ and the positive vector by $\mathit{\Gamma}_I^+$. $\mathit{\Gamma}_U^-$ will have κ_U^- elements and we let $\mathit{\Gamma}_U^-(k)$ denote the k^{th} element of $\mathit{\Gamma}_U^-$. On the other hand, $\mathit{\Gamma}_U^+$ has an infinite number of elements. We denote the first element of $\mathit{\Gamma}_U^+$ by $\mathit{\Gamma}_U^+(\kappa_U^+)$ and we let $\mathit{\Gamma}_U^+(k)$ denote the k^{th} element of $\mathit{\Gamma}_U^+$.

We let $\tilde{\tau}_k^-$ denote the probability of occurrence of element $\mathit{\Gamma}_U^-(k)$ of $\mathit{\Gamma}_U^-$, while $\tilde{\tau}_k^+$ denote the probability of occurrence of element $\mathit{\Gamma}_U^+(k)$ of $\mathit{\Gamma}_U^+$. As such, the elements of $\mathit{\Gamma}_U^-$ and $\mathit{\Gamma}_U^+$, and their associated probabilities, respectively form the negative and positive portions of $\mathit{\Gamma}(\boldsymbol{x},h)$, denoted by $\mathit{\Gamma}_U^-(\boldsymbol{x},h)$ and $\mathit{\Gamma}_U^+(\boldsymbol{x},h)$.

The valuation, $\mathit{\Xi}_U^-(\mathit{\Gamma}_U^-)$, of the negative prospect, $\mathit{\Gamma}_U^-$, can be computed as follows:

$$\mathit{\Xi}_U^-(\mathit{\Gamma}_U^-)=\sum_{i=1}^{\kappa_U^-}\mathit{\Gamma}_U^-(i)\Big[\omega_U^+\Big(\sum_{j\leq i}\tilde{\tau}_j\Big)-\omega_U^+\Big(\sum_{j<i}\tilde{\tau}_j\Big)\Big]. \tag{5.123}$$

In addition, the valuation, $\mathit{\Xi}_U^+(\mathit{\Gamma}_U^+)$, of the positive prospect, $\mathit{\Gamma}_U^+$, can be computed as follows:

$$\mathit{\Xi}_U^+(\mathit{\Gamma}_U^+)=\sum_{i=\kappa_U^+}^{\infty}\mathit{\Gamma}_U^+(i)\Big[\omega_U^-\Big(\sum_{j\geq i}\tilde{\tau}_j\Big)-\omega_U^-\Big(\sum_{j>i}\tilde{\tau}_j\Big)\Big]. \tag{5.124}$$

Thus, the valuation, $\mathit{\Xi}_U(\boldsymbol{x},h)$, that U assigns to prospect $\mathit{\Gamma}(\boldsymbol{x},h)$ is:

$$\mathit{\Xi}_U(\mathit{\Gamma}(\boldsymbol{x},h))=\mathit{\Xi}_U^-(\mathit{\Gamma}_U^-)+\mathit{\Xi}_U^+(\mathit{\Gamma}_U^+). \tag{5.125}$$

Based on $\mathit{\Xi}_I(\boldsymbol{x},h)$ and $\mathit{\Xi}_U(\boldsymbol{x},h)$, the equilibrium of the PT game under mixed interdiction can be defined and characterized as shown next.

5.7.2 PT Game Equilibrium under Mixed Interdiction

The definition of the SE-PT equilibrium introduced in Definition 15 can be extended to the mixed interdiction case to form a *PT mixed interdiction Stackelberg equilibrium* (MSE-PT) defined in Definition 16.

Definition 16. *A strategy pair* $(\tilde{\boldsymbol{x}}^*, \tilde{h}^*_{\tilde{\boldsymbol{x}}^*})$ *constitutes a* PT mixed interdiction Stackelberg equilibrium *of the network interdiction game if*

$$\varXi_I(\tilde{\boldsymbol{x}}^*, \tilde{h}^*_{\tilde{\boldsymbol{x}}^*} = \tilde{\rho}^{PT}(\tilde{\boldsymbol{x}}^*)) \geq \varXi_I(\boldsymbol{x}, \tilde{\rho}^{PT}(\boldsymbol{x}))\, \textit{for all}\; n \in \mathcal{N}, \tag{5.126}$$

where $\tilde{\rho}^{PT}(\boldsymbol{x})$ *is the optimal reaction of* U *to* $\boldsymbol{x}$ *and is given by:*

$$\tilde{\rho}^{PT}(\boldsymbol{x}) = \operatorname*{argmin}_{h \in \mathcal{H}} \varXi_U(\boldsymbol{x}, h). \tag{5.127}$$

In this regard, our solution approach presented in Section 5.7 and which enabled deriving the MSE of the game (under full rationality) can be also applied to derive the MSE-PT of the PT game. Indeed, characterizing the MSE-PT requires solving U's problem in (5.127) as well as I's problem given in (5.126). In this regard, the all-paths method proposed in Section 5.4.1 can guarantee solving U's problem as shown in Lemma 3.

Lemma 3. *The all-paths method is guaranteed to find* $\tilde{\rho}(\boldsymbol{x})$ *for each interdiction strategy* $\boldsymbol{x} \in \mathcal{X}$.

Proof. Finding $\tilde{\rho}(\boldsymbol{x})$ corresponds to identifying the path h which solves:

$$h = \operatorname*{argmin}_{h \in \mathcal{H}} \varXi_U(\boldsymbol{x}, h). \tag{5.128}$$

As such, by following steps 1 to 3 of the all-paths method, and considering $\varXi_U(\boldsymbol{x}, h)$ instead of $E_h(O; \boldsymbol{x})$, the all-paths method performs an exhaustive search over all possible O-to-D paths and returns path h which results in the minimum $\varXi_U(\boldsymbol{x}, h)$; and hence solves (5.128). □

The interdictor's problem corresponds to solving the following optimization problem.

$$\tilde{\boldsymbol{x}}^* = \operatorname*{argmax}_{x \in \mathcal{X}} \varXi_I(\boldsymbol{x}, \tilde{\rho}^{\text{PT}}(\boldsymbol{x})). \tag{5.129}$$

Similarly to I's problem in Section 5.4.2, obtaining an exact global solution to I's PT problem in (5.129) cannot be guaranteed due to the non-convexity and discontinuity of the objective function stemming from the sudden changes to $\tilde{\rho}^{\text{PT}}(\boldsymbol{x})$ which can be triggered by minimal changes to $\boldsymbol{x}$. Hence, for obtaining a solution to (5.129), we propose using a pattern search based method, as discussed in Section 5.4.2.

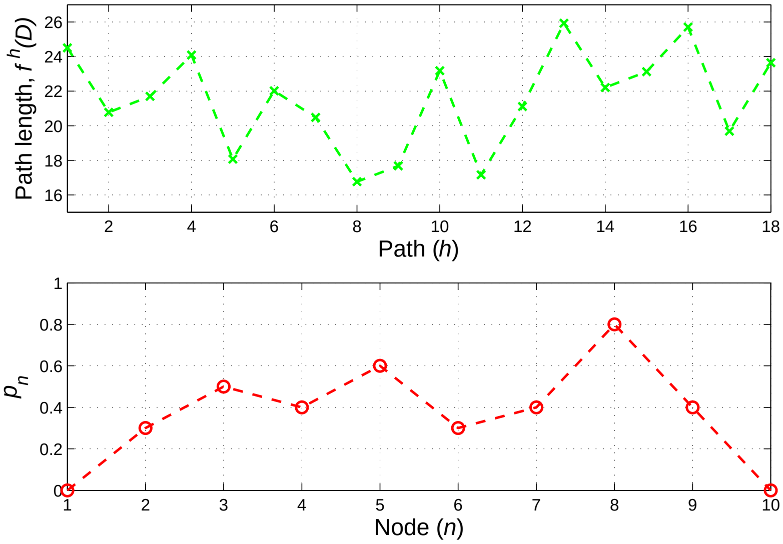

Figure 5.4: Paths lengths, $f^h(D)$, and node risk probabilities, p_n.

5.8 Numerical Results

For performing numerical analyses, we consider the graph shown in Fig. 5.2 which is composed of $N = 10$ nodes and $E = 18$ edges. For ease of reference, we number the 18 paths, from 1 to 18, as follows: $[1, 2, ..., 18] \triangleq [(2,5,7), (2,5,8), (2,5,9), (2,6,7), (2,6,8), (2,6,9), (3,5,7), (3,5,8), (3,5,9), (3,6,7), (3,6,8), (3,6,9), (4,5,7), (4,5,8), (4,5,9), (4,6,7), (4,6,8), (4,6,9)]$. Here, given that node 1 (O) and node 10 (D) are part of each path, and for convenience, a path $(1, i, j, k, 10)$ is referred to by (i, j, k). In addition, the travel times t_i, for $i \in \{1, ..., 18\}$, in Fig. 5.2 have been drawn from a uniform distribution in the interval $[2, 8]$; which resulted in $[t_1, t_2, ..., t_{18}] \triangleq [6.89, 3.46, 7.58, 4.1, 3.18, 3.51, 5.7, 4.84, 4.11, 6.99, 5.51, 5.3, 7.5, 3.72, 6.54, 6.52, 4.28, 5.41]$. We then chose the attack success probabilities as $\boldsymbol{p}= [0, 0.3, 0.5, 0.4, 0.6, 0.3, 0.4, 0.8, 0.4, 0]$. The length of each path h, $f^h(D)$, and the risk probability at each node, p_n, are shown in Fig. 5.4. Fig. 5.4 shows that path 8, i.e. $(3, 5, 8)$, is the shortest path followed by paths 11, i.e. $(3, 6, 8)$, and path 9, $(3, 5, 9)$; while node 8 is the most risky node followed by nodes 5 and 3, respectively. The re-handling and processing time is considered to be $t_a = 5$. Moreover, regarding the PT parameters of I and U, unless stated otherwise, we consider $R_I = R_U = 20$, $\lambda_I = \lambda_U = 2.5$, $\beta_I^- = \beta_I^+ = \beta_U^- = \beta_U^+ = 0.6$, and $\gamma_I^- = \gamma_I^+ = \gamma_U^- = \gamma_U^+ = 0.5$.

We will first take the reference points (which represent, for example, a target delivery time) of both players to be equal to R, i.e. $R_I = R_U = R$, and ranging from 10 to 35. The resulting equilibrium interdiction strategies (i.e. I's equilibrium strategies) are shown in Fig. 5.5, and U's equilibrium strategies are shown in Fig. 5.6. Fig. 5.5 shows that the MSE interdiction strategy, $\boldsymbol{x}^*$, focuses solely on nodes 5, 8, and 9, (with $x_5^* = 0.48$, $x_8^* = 0.31$, and $x_9^* = 0.21$) which are nodes of significant risk (especially nodes 5 and 8 with $p_5 = 0.6$ and $p_8 = 0.8$) and each one of these nodes is at least part of one of the three shortest paths, i.e. paths 8, 11, and 9. In addition, U's

MSE strategy, h, corresponds to choosing path 12, which is composed of nodes 3, 6, and 9. Given that nodes 3 and 6 are not attacked by I at the MSE, and that $p_9 = 0.4$ and $x_9^* = 0.2$, path 12 is a relatively safe path. The players' MSE strategies lead to an MSE expected delivery time that is equal to around 23, as shown in Fig. 5.7.

Fig. 5.5 highlights the difference between I's MSE-PT interdiction strategies, $\tilde{\boldsymbol{x}}^*$, and the MSE interdiction strategies at the different values of R. Fig. 5.5 shows the shift with an increase in R in the PT interdiction strategy, $\tilde{\boldsymbol{x}}^*$, from mainly targeting the nodes of the last phase before node D (i.e. nodes 7, 8, and 9), at $R = 10$, to a more spread out attack strategy targeting a larger number of nodes, at $R = 35$. In fact, at small values of R, such as $R = 10$, all possible delivery times fall above R. Hence, all possible outcomes are valued by I as gains. Since the PT valuation function, $v_I(.)$ in (5.54) and (5.54), leads I to be risk averse in gains, choosing nodes 7, 8, and 9 is appealing since any O-to-D path is guaranteed to pass by at least one of these nodes. Clearly, this choice of $\tilde{\boldsymbol{x}}^*$ is a risk averse choice that guarantees a sure gain. However, when R increases, some of the possible delivery times will fall below R. Hence, for a choice $\boldsymbol{x}$ by I, and h by U, some of the outcomes will correspond to gains and some to losses leading I to drift away from a mere risk averse strategy.

In Fig. 5.6, we show the different MSE-PT strategies of U for the different values of R. Fig. 5.6 shows that at $R = 10$, U chooses the shortest path, i.e. path 8, at the MSE-PT. This is due to the fact that, for such a small reference point R, all possible delivery times are greater than R and are, hence, seen as losses by U. Hence, due to the concavity of the value function for outcomes greater than R_U, and since U is a minimizer, the benefit from any reduction in losses exceeds the damage caused by an increase in losses of the same magnitude (i.e. this PT property is known as risk seeking in losses). Hence, taking the shortest path (even if it is risky up to a certain extent) becomes more appealing to U. When R increases, U's MSE-PT strategy will drift away from the shortest path, particularly at values of R that are high enough to enable certain possible delivery times to fall below the reference delivery time, R, leading to outcomes that are valued as gains.

Fig. 5.7 shows the resulting expected delivery times, at the MSE and MSE-PT, for the different values of R. Clearly, for low values of R, the MSE-PT results in a lower expected delivery time than the MSE. However, for relatively high values of R, the MSE-PT results in an expected delivery time that is higher than the expected delivery time at the MSE. In fact, as shown in Fig. 5.7, the percentage difference in expected delivery time at the MSE-PT compared to the MSE is -7.5% at $R = 15$ and $+14.4\%$ at $R = 30$. Indeed, since at low values of R, I takes a risk averse non-aggressive attack strategy, as shown in Fig. 5.5), and U chooses a risk-seeking shortest path, as shown in Fig. 5.6, this leads to achieving a relatively short expected delivery time since this shortest path (i.e. path 8) is not heavily targeted by I at the MSE-PT. However, for higher values of R, I considers more aggressive interdiction strategies and U considers safer paths which results in expected delivery times that are higher at the MSE-PT than at the MSE. In addition, the results in Fig. 5.7 show that at the MSE-PT, except for $R = 30$ and $R = 35$, U was not able to achieve an expected delivery time that is below its target reference delivery time. However, at the MSE, U's expected delivery time is lower than its target delivery time for $R \geq 25$. Hence, selecting strategies based on PT valuations is, based on this comparison, disadvantageous to U.

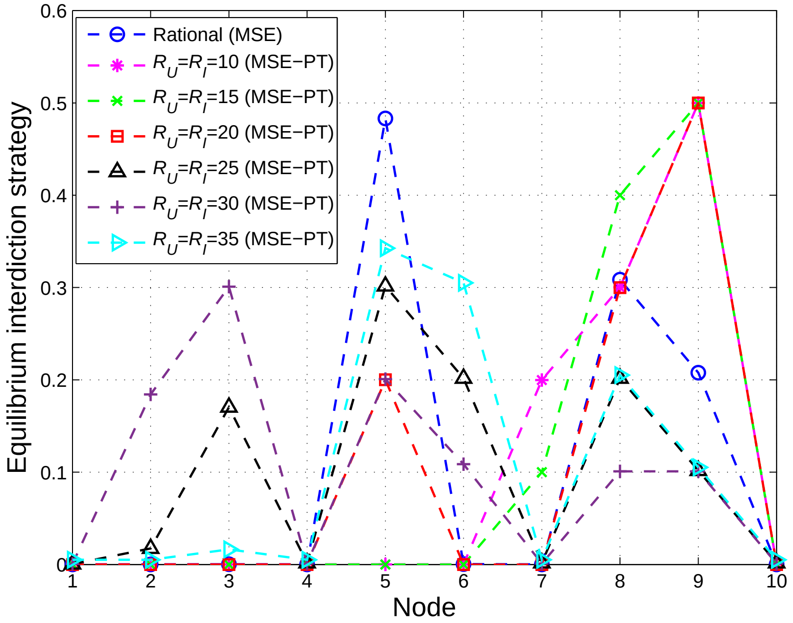

Figure 5.5: Equilibrium interdiction strategy for different $R = R_I = R_U$.

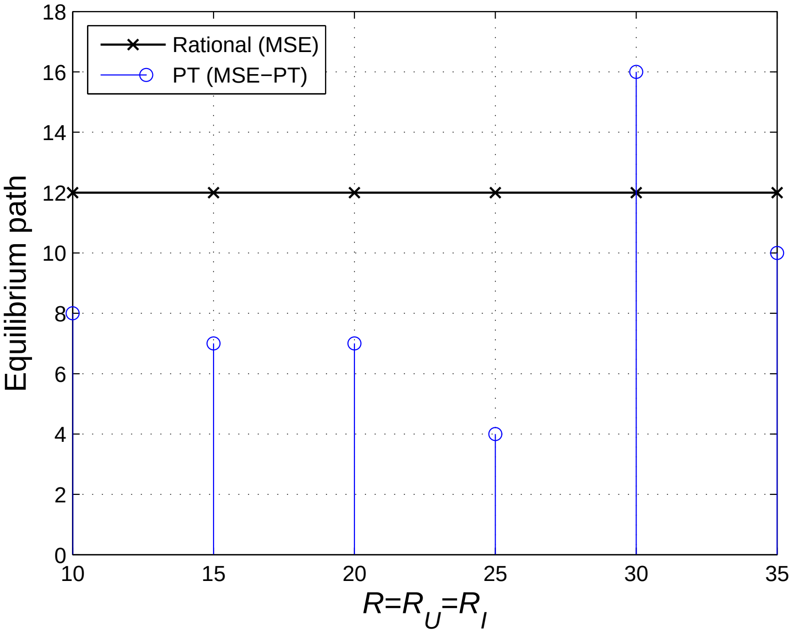

Figure 5.6: U's equilibrium path selection strategy for different $R = R_I = R_U$.

Hereinafter, to characterize the effect of the various PT parameters on the resulting equilibrium strategies and outcomes, we consider the interdictor to be fully rational (i.e. $R_i = 0$, $\lambda_I = 1$,

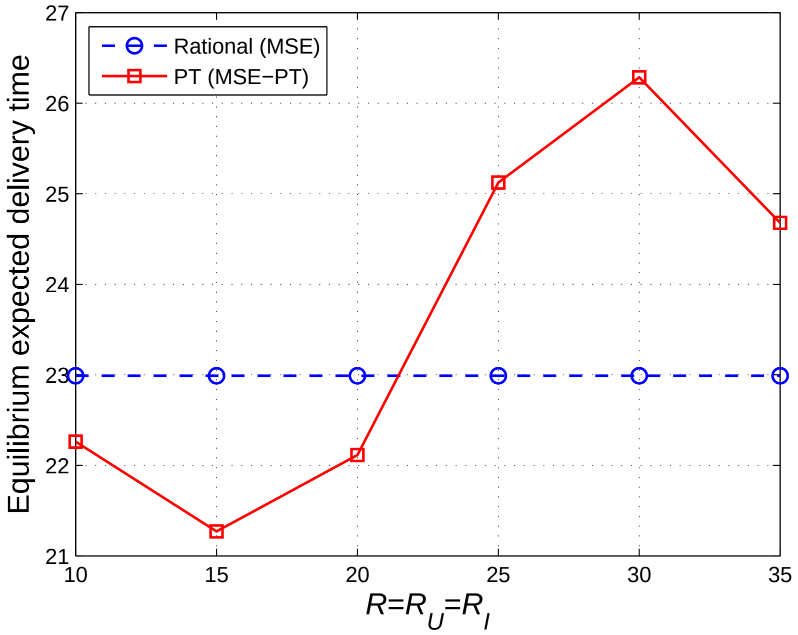

Figure 5.7: Expected delivery time for different $R = R_I = R_U$.

$\beta_I^- = \beta_I^+ = 1$, and $\gamma_I^- = \gamma_I^+ = 1$), while U values outcomes and performs probability weighting following cumulative prospect theory, with PT parameters similar to the ones used in the previous simulations, unless stated otherwise. We first study the effect of varying the rationality parameters of U, i.e. γ_U^- and γ_U^+, on the MSE-PT and then study the effects of varying U's loss parameter λ_U. First, we consider $\gamma_U = \gamma_U^- = \gamma_U^+$, and we let γ_U take the following values: 0.25, 0.3, 0.35, 0.5, 0.75, and 0.9.

Fig. 5.8 shows that the MSE-PT interdiction strategy approaches its MSE strategy at higher values of γ_U. However, one can see that I's MSE-PT strategy does not completely coincide with its MSE even for high values of γ_U. This is due to the fact that even when U's probability weighting is closer to full rationality, the way U values the possible game outcomes (i.e. the possible delivery times) is based on its reference point R_U and value function. Hence, even with a closely rational probability weighting, U's MSE-PT may not equal its MSE strategy. This can, indeed, be seen from Fig. 5.9, which shows that even for $\gamma_U = 0.9$, U's MSE-PT strategy is different than its MSE strategy.

Fig. 5.9 shows the way in which U's MSE-PT strategy changes with an increase in γ_U. In this regard, at lower values of γ_U, U's MSE-PT strategy consists of path 9, i.e. $(3, 5, 9)$, while at higher values of γ_U, U's MSE-PT strategy shifts to choosing path 11, i.e $(3, 6, 8)$. As can be seen from Fig. 5.8, at lower values of γ_U, I's optimal strategy is focused on nodes 5 and 8 making path 9, chosen by U at the MSE-PT, highly risky. However, U still chooses this path, at the MSE-PT, since at such low values of γ_U, U's valuation of probabilities is highly distorted. In fact, the weighting functions $\omega_U^+(.)$ and $\omega_U^-(.)$ flatten for lower values of γ_U. Hence, U would assess different paths

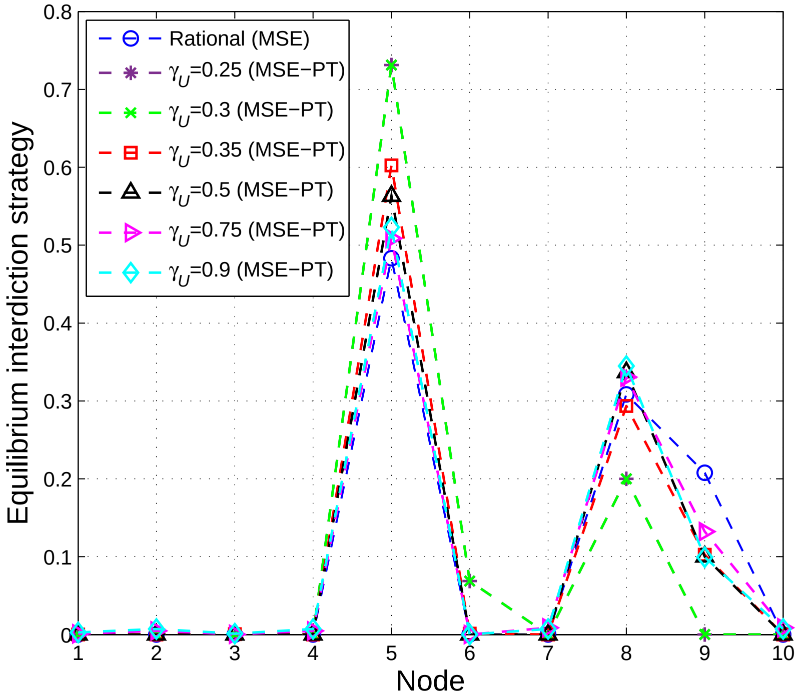

Figure 5.8: I's equilibrium interdiction strategy for different values of $\gamma_U = \gamma_U^- = \gamma_U^+$.

as almost equally risky leading U to choose path 9. However, when γ_U increases, U's perception of probabilities becomes more rational. Hence, for these values of γ_U, U can observe that path 9 is highly risky and chooses instead the safer path 11, composed of nodes $(3, 6, 8)$ which are not attacked with a high probability by I at the MSE-PT.

Fig. 5.10 shows the resulting expected delivery times at the MSE and at the MSE-PT for the various values of γ_U. From Fig. 5.10, we can see that the MSE-PT strategies result in expected delivery times that are longer than the expected delivery time achieved at the MSE. Indeed, for $\gamma_U = 0.25$, the percentage difference between the expected delivery time at the MSE-PT and that at the MSE goes up to $+21.5\%$. The reason is that, as shown in Fig. 5.9, for low values of γ_U, U admits a risky MSE-PT strategy leading to high expected delivery times. However, with an increase in γ_U, the shift in U's MSE-PT strategy allows achieving better expected delivery times; which are, however, still longer than the MSE expected delivery time. Fig. 5.10 also shows an expected delivery time labeled "Rational response". This corresponds to U choosing a rational strategy in response to I's MSE-PT strategy. In other words, rational response corresponds to choosing the path strategy h^* which solves (5.50) for $\boldsymbol{x} = \tilde{\boldsymbol{x}}^*$. In this scenario, I assumes that U admits PT valuations and would, hence, choose its MSE-PT strategy, $\tilde{\boldsymbol{x}}^*$. However, if U is rather rational, it can take advantage of its knowledge of $\tilde{\boldsymbol{x}}^*$ to achieve a better expected delivery time. Indeed, the rational response of U consists of choosing path 11, for $\gamma_U = 0.25$ and $\gamma_U = 0.3$, and path 12, for the higher values of γ_U, which result in achieving expected delivery times that are shorter than the expected delivery

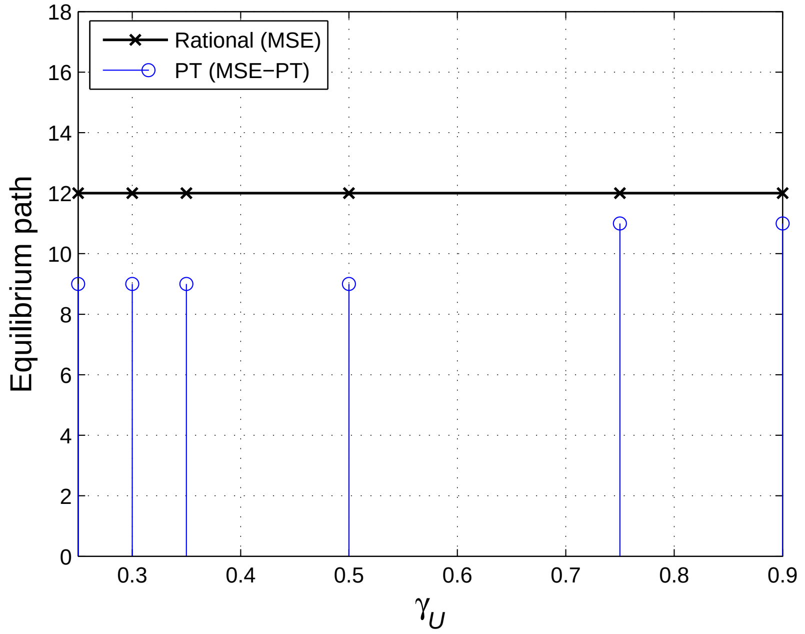

Figure 5.9: U's equilibrium path selection strategy for different values of $\gamma_U = \gamma_U^- = \gamma_U^+$.

times at the MSE-PT and the MSE, as shown in Fig. 5.10. In fact, as can be seen from Fig. 5.10, at $\gamma_U = 0.25$, choosing the rational response strategy (which corresponds to choosing path 11) allows U to achieve an expected delivery time that is 30.3% lower than the expected delivery time achieved at the MSE-PT.

Fig. 5.11 shows the resulting expected delivery times at the MSE and at the MSE-PT, for the various values of $\lambda_U \in \{1, 2.5, 5\}$. Fig. 5.11 also shows the expected delivery time achieved when U plays the rational response strategy as a reaction to I choosing its MSE-PT strategy. Fig. 5.11 shows that the MSE-PT strategies chosen at the different values of λ_U result in an expected delivery time that is only slightly higher than the one achieved at the MSE. At higher values of λ_U, this difference in expected delivery times decreases. Indeed, at $\lambda_U = 1$, the percentage difference between the MSE-PT and the MSE expected delivery times is $+4.14\%$ while this difference drops to only 1.3% at $\lambda_U = 5$. However, when U plays a rational response strategy, in response to I's MSE-PT strategy (which consists of choosing path 12 for all the three values of λ_U, i.e. 1, 2.5 and 5), U can achieve an expected delivery time that is up to 11% lower than the expected delivery time achieved at the MSE.

5.9 Summary

In this chapter, we have introduced a novel mathematical framework for studying the cyber-physical security of time-critical UAV applications, such as drone delivery systems and anti-drone

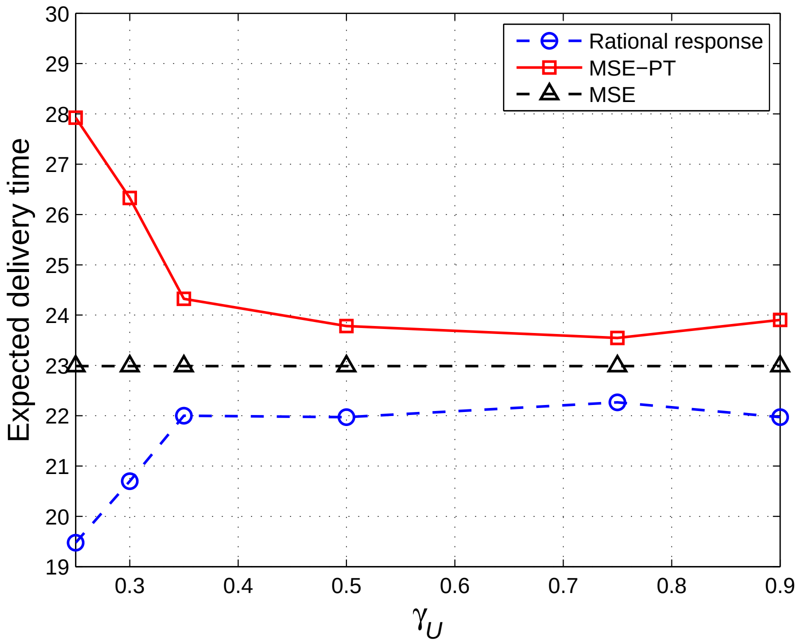

Figure 5.10: Expected delivery time a) when U plays a rational response to I's MSE-PT strategy, b) at the MSE, and c) at the MSE-PT for different values of $\gamma_U = \gamma_U^- = \gamma_U^+$.

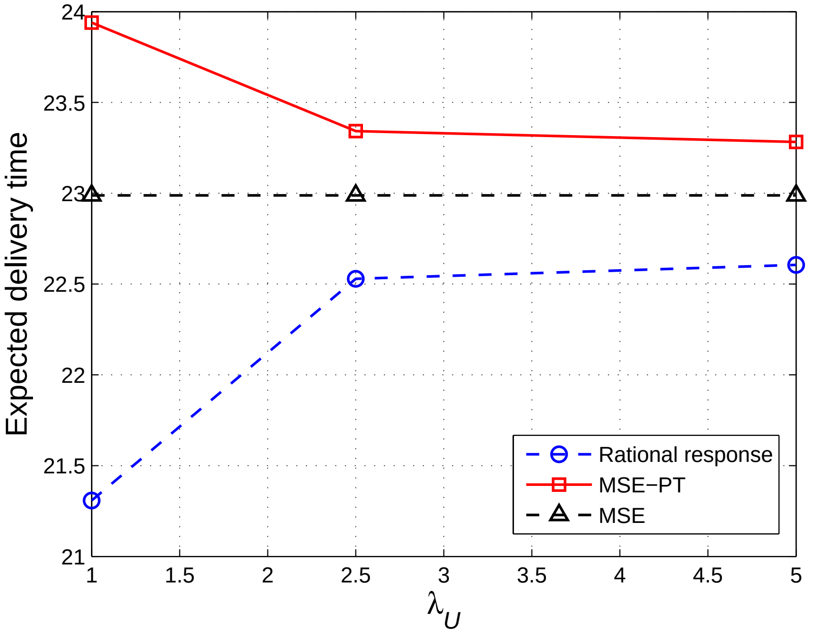

Figure 5.11: Expected delivery time a) when U plays a rational response to I's MSE-PT strategy, b) at the MSE, and c) at the MSE-PT, for different values of λ_U.

systems. We have modeled the problem using a network interdiction game between the UAV operator and the interdictor, while considering that either of which is malicious and the other is benign. In addition, we have incorporated principles from cumulative prospect theory in the game formulation to account for the players' potential subjectivity and bounded rationality. In this regard, under pure strategies – for the fully rational game and the cumulative prospect-theoretic game, we have derived the Stackelbeg equilibrium of the game. In addition, under mixed-strategies, for the PT and fully rational games, we have characterized the solutions to the optimization problems of the UAV operator and interdictor and proposed solution algorithms for obtaining these solutions. Simulation results have highlighted the effects of the cumulative prospect-theoretic parameters of the players on the resulting game outcomes and equilibrium strategies. In this regard, the results have shown that the subjectivity of the players is in most results disadvantageous to the UAV operator leading to delays in the expected delivery time which can surpass the target delivery time predefined by the UAV operator.

Chapter 6

Diffusion of Threats in Cyber-Physical Systems

6.1 Introduction

Cyber-physical systems are characterized by a tight interconnection between the physical system and its underlying information and communication layers. Such a cyber-physical interconnection allows the diffusion of attacks and threats from the cyber layer to the physical system, and from the physical system to the cyber realm. As such, understanding such threat propagation is vital for securing these CPSs.

Even though a large number of works, as surveyed in Section 1.2, have recently focused on studying CPSs security such as in [29, 52, 79, 102, 117, 120, 127, 223], no previous works have focused on such detrimental propagation of threats while devising optimal defense mechanisms which are cognizant of potential smart strategic attackers which aim at exploiting such diffusion possibilities to penetrate the system and inflict a wide-scale damage to the CPS.

The main contribution of this chapter is to develop a general framework for analyzing CPS security – accounting for the propagation of threats throughout the system – in the presence of a strategic attacker and defender. Given a general CPS model, the problem is formulated as a zero-sum game between the attacker and defender that are interacting over the cyber side of the CPS. In this game, the attacker aims at launching cyber attacks on a number of cyber nodes of the CPS to damage some of the physical components by capitalizing on the diffusion of failures from the cyber to the physical components. In contrast, the defender aims at defending a number of cyber nodes to stop such attacks. Since the attacker and defender can have different computational abilities and levels of knowledge of the CPS, we propose a novel approach to capture such disparate cognitive levels inspired by the behavioral framework of *cognitive hierarchy theory* [224]. Our proposed framework considers that the defender can be faced, in practical situations, with an attacker possessing one of various possible levels of computational abilities and knowledge depth. Thus, choosing a

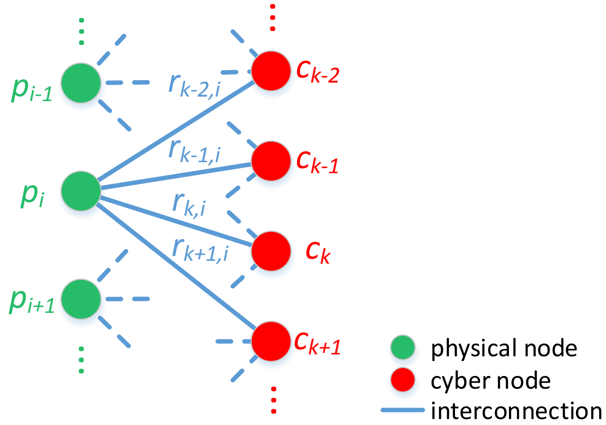

Figure 6.1: Cyber-Physical Interconnection.

defense strategy while always assuming that the attacker is a very complex strategic thinker, as in conventional games [102, 127], is not always optimal. Hence, our bounded rationality framework assumes that the defender can be faced with an attacker than can have one of many *levels of thinking* reflecting the level of sophistication of its used strategy. To solve this game, we characterize the various levels of thinking of the attacker and accordingly derive its optimal strategy. Moreover, the optimal strategy of the defender is chosen to be the one that maximizes its expected payoff given a probability distribution of the attacker's thinking levels.

As a case study, we consider a wide area protection scenario in the smart grid. In this study, we focus on the economic effects that a false disconnection of a transmission line can have on the system. Our numerical results over the PJM-5 bus system show that the defender can have an incentive to deviate from its Nash equilibrium strategy knowing that the attacker can be acting with bounded rationality. Moreover, these results also showcase the effect that the probability of facing each attacker level has on the optimal attack and defense strategies.

The rest of this chapter is organized as follows. Section 6.2 introduces our general CPS security model as well as the proposed game with bounded rationality. Section 6.3 presents a case study focusing on wide area protection of the smart grid illustrating our proposed model and game while Section 6.4 presents a summary of the chapter.

6.2 System Model and Game Formulation

Consider a CPS composed of N_c cyber and N_p physical nodes that are strongly interdependent. Let $\mathcal{C}$ and $\mathcal{P}$ be, respectively, the sets of cyber and physical nodes. In this model, security breaches can spread from the cyber to the physical realms. As illustrated in Fig. 6.1, we let $r_{c,p}$ be the interconnection between a cyber node $c \in \mathcal{C}$ and a physical node $p \in \mathcal{P}$. In fact, control laws governing the operation of the physical system depend on local and remote data collected by cyber nodes. Such data is sent via communication channels to a supervisory control and data acquisition system which, in turn, sends control signals back to the cyber nodes initiating a control action over the physical nodes. In this regard, $r_{c,p}$ is a weight that captures the effect of the data sent by cyber node c on the control action over physical node p. Accordingly, from a security perspective, $r_{c,p}$ represents the probability that p fails due to corrupt data sent by c. Hereinafter, we use "failed node" to refer to a cyber node sending corrupt data. This failure of c can be due to a cyber attack on this node or to other reasons such as a software bug or a misconfiguration. Hence, $r_{c,p}$ can be expressed as $r_{c,p} = \Pr(p\,\text{fails}\,|\,c\,\text{has failed})$, while $\sum_{c\in\mathcal{C}} r_{c,p} = 1$.

Let π_p be the probability of failure of $p \in \mathcal{P}$ due to failures of a number of cyber nodes, and κ_c the probability of failure of one of the cyber nodes $c \in \mathcal{C}$. Accordingly, π_p will be given by

$$\pi_p = \sum_{c=1}^{N_c} r_{c,p}\kappa_c. \tag{6.1}$$

We denote by $\boldsymbol{R}$ the matrix of interconnections between cyber and physical nodes, and $\boldsymbol{\pi} = [\pi_1, ..., \pi_{N_p}] \in \mathbb{R}^{N_p}$ and $\boldsymbol{\kappa} = [\kappa_1, ..., \kappa_{N_c}] \in \mathbb{R}^{N_c}$ the failure probability vectors of the physical and cyber nodes, respectively. Accordingly, (6.1) can be rewritten in matrix form as follows:

$$\boldsymbol{\pi} = \boldsymbol{\kappa}\boldsymbol{R}. \tag{6.2}$$

Each physical node p is associated with a cost of failure f_p. Hence, the expected total loss to the system, E_f, is given by:

$$E_f = \sum_{p=1}^{N_p} \pi_p f_p. \tag{6.3}$$

6.2.1 Game Formulation

In the absence of attacks, the probability of failure of each cyber node is typically small and is only due to the presence of software bugs or misconfiguration by, for example, maintenance personnel. Thus, under no cyber attacks $\boldsymbol{\kappa} \approx \mathbf{0}$ and, thus, $\boldsymbol{\pi} \approx \mathbf{0}$. However, when a cyber node c is attacked, the probability of failure of this node goes up to $\kappa_c = 1$. As a result, as seen from (6.2), this attack increases the risk of failure of the physical components that are interconnected to c thus increasing E_f as per (6.3). On the other hand, defending c protects it from failures in which case $\kappa_c = 0$ even when c_k is attacked[1]. For example, if an attacker induces a malware over a cyber node, when this node is defended, the malware is detected and eliminated.

[1] Attack and defense are assumed to be always successful such that an attack on c will certainly lead to its failure while defending c leads to its non-failure.

The attacker hence aims at maximizing E_f while the defender, which is the system operator, aims at minimizing it. To analyze the optimal decision making of each of the attacker and defender, we formulate a noncooperative zero-sum game [146] $\varXi = \langle \mathcal{I}, (\mathcal{S}_i)_{i\in\mathcal{I}}, (U_i)_{i\in\mathcal{I}} \rangle$. Here, $\mathcal{I} = \{d, a\}$ is the set of players: defender (d) and attacker (a). $\mathcal{S}_i$ is the set of actions available to player $i \in \mathcal{I}$ which consists of choosing a subset of cyber nodes to defend or attack. Let n_d and n_a be the number of nodes that can be, respectively, defended by the defender and attacked by the attacker. Then, we have $|\mathcal{S}_d| = \binom{N_c}{n_d}$ and $|\mathcal{S}_a| = \binom{N_c}{n_a}$. U_i is the utility function of player $i \in \mathcal{I}$ and is such that for $s_i \in \mathcal{S}_i$,

$$U_d(s_d, s_a) = -U_a(s_d, s_a) = -E_f, \tag{6.4}$$

where E_f is given by (6.3).

6.2.2 Solution Concept

The most commonly adopted equilibrium concept for such static noncooperative games is the Nash equilibrium [146] (NE); as defined in Chapter 2 and reintroduced next. In this regard, let $\gamma_i \in \varGamma_i$ be a probability distribution over the strategy set of player i where $\varGamma_i$ is the set of all possible such distributions. Thus, $\gamma_i(s)$ represents the probability of player i choosing strategy $s \in \mathcal{S}_i$ while $\sum_{s\in\mathcal{S}_i} \gamma_i(s) = 1$. Accordingly, each player's expected utility is given by:

$$\begin{aligned}\bar{U}_d(\boldsymbol{\gamma}_d, \boldsymbol{\gamma}_a) &= -\bar{U}_a(\boldsymbol{\gamma}_d, \boldsymbol{\gamma}_a)\\ &= -\sum_{s_d\in\mathcal{S}_d}\sum_{s_a\in\mathcal{S}_a} \gamma_d(s_d)\gamma_a(s_a)U_a(s_d, s_a).\end{aligned} \tag{6.5}$$

A best response strategy of a rational player i, γ_i^*, is one that maximizes its expected utility facing its opponent's strategy, γ_{-i}:

$$\bar{U}_i(\gamma_i^*, \gamma_{-i}) \geq \bar{U}_i(\gamma_i, \gamma_{-i})\ \forall \gamma_i \in \varGamma_i. \tag{6.6}$$

When every player plays a best response strategy against its opponent's strategy, the game reaches an equilibrium. Thus, the strategy profile $(\gamma_i^*, \gamma_{-i}^*)$ is a NE of the game when $\forall i \in \mathcal{I}$ [146]:

$$\bar{U}_i(\gamma_i^*, \gamma_{-i}^*) \geq \bar{U}_i(\gamma_i, \gamma_{-i}^*)\ \forall \gamma_i \in \varGamma_i. \tag{6.7}$$

6.2.3 Notion of Bounded Rationality

The NE as defined in (6.7) assumes that both players are *strategic thinkers, act rationally, and have complete knowledge of the game*. However, when faced with risk and uncertainty, individuals are known to deviate from full rational behavior[2] [161].

[2] Even in the case of automated attack and defense, the high required computational ability and short time to act can lead to taking sub-optimal decisions.

In fact, (6.7) requires every player to anticipate the exact cost, f_p, caused to the system due to the loss of each physical component $p \in \mathcal{P}$. With this knowledge, the attacker (defender) can rank the physical components based on the magnitude of their associated f_p. Accordingly, each player can maximize (minimize) the harm caused to the system taking into consideration the defense (attack) strategy that can be adopted by the opponent. However, cyber-physical systems are known to be very complex systems. Thus, obtaining such an exact ranking of the costs caused by the loss of every component, f_p, is highly complex. As a result, in practice, the attacker and defender can build their own perception of the vector of incurred losses $\boldsymbol{f}$, denoted as $\hat{\boldsymbol{f}}^i$ for $i \in \mathcal{I}$, then take action accordingly. However, $\hat{\boldsymbol{f}}^i$ can differ from $\boldsymbol{f}$. Moreover, the attacker and defender can have different computational capabilities and thus can generate a different $\hat{\boldsymbol{f}}^i$ based on their skill and computational levels. Thus, by following its own perception, a player can deviate from full rationality while choosing its optimal strategy. Consequently, this bounded rationality can lead to deviations from the NE strategies.

To model such bounded rationality, we categorize each player based on its *level of thinking* which is defined by how close is its perception $\hat{\boldsymbol{f}}^i$ to the actual $\boldsymbol{f}$. Thus, high level thinkers are more intelligent, have better knowledge, and superior computational ability, allowing them to generate a closer perception to the real $\boldsymbol{f}$. Such a notion is inspired from the behavioral framework of *cognitive hierarchy theory* (denoted here by CH) [224] – defined in Section 2.5.2 – in which it is shown that human players assume that they have the highest level of thinking, denoted by level K, and that their opponents' levels of thinking are distributed over lower levels $0, ..., K-1$. In a CH model, level 0 thinkers choose an action randomly from their strategy space while higher level thinkers employ more advanced levels of reasoning to choose their strategies. To model the proportion of level k thinkers for $k \in \{0, ..., K-1\}$, a Poisson distribution, $\alpha(k)$, with mean and variance denoted by λ is usually assumed [224]:

$$\alpha(k) = \frac{e^{-\lambda}\lambda^k}{k!}. \tag{6.8}$$

Given that the defender in our model is the system operator, it can anticipate with full certainty $\boldsymbol{f}$. In contrast, the attacker might have a distorted $\hat{\boldsymbol{f}}$ which reflects its level of thinking and, as a result, its chosen strategy. The defender, hence, has to choose its optimal strategy while anticipating the possibility of facing an attacker that can fall in any category k with a probability $\alpha(k)$.

As a result, the knowledge that the defender has about potential types of the attacker that it can face can give an incentive for the defender to deviate from its NE strategy. In fact, this anticipation of the various attacker types would change the best response strategy of the defender from the NE strategy which assumes that the defender faces only a fully rational attacker. Moreover, since the attacker acts with bounded rationality based on its thinking level, this attacker chooses the strategy that it perceives to be optimal based on its own perception following from its $\hat{\boldsymbol{f}}$. Thus, the attacker also has an incentive to deviate from the NE strategy. Consequently, our bounded rationality framework showcases how in practical situations attackers and defenders can deviate from the fully rational NE.

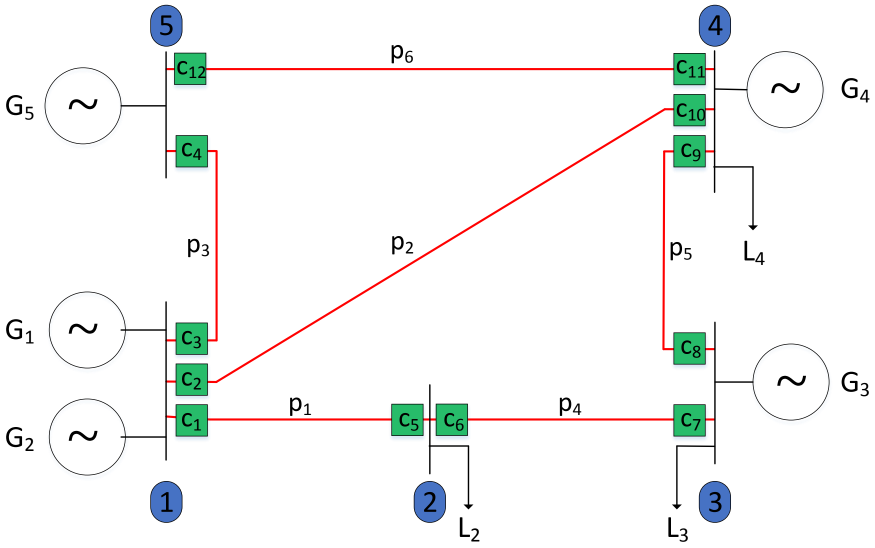

Figure 6.2: PJM 5-bus System

To give more elaboration of our proposed CPS model, game formulation, and bounded rationality framework, we next analyze in detail a case study focusing on the concept of wide area protection of a smart grid with energy markets implications.

6.3 Wide Area Protection in the Smart Grid

6.3.1 Smart Grid Wide Area Monitoring and Protection

In a smart grid, the concept of wide area monitoring, protection, and control relies on system-wide information sent from a collection of cyber nodes to generate protective actions affecting the status (i.e. connectivity) of the system's physical components to prevent the propagation of large disturbances [7]. The extent to which the information sent by every cyber node affects the status of each physical component can follow our proposed model in Section 6.2.

Consider the PJM 5-bus system shown in Fig. 6.2. This test system comprises 5 generator units and 3 loads. All data pertaining to this test system are available in [225]. The cyber nodes $\mathcal{C} \triangleq \{c_1, ..., c_{12}\}$ collect real time data from around the system and send them to the SCADA. The SCADA processes the data, detects possible disturbances, and sends, in this event, protection actions requiring the disconnection of a transmission line to stop the propagation of the disturbance. The transmission lines, $\mathcal{P} \triangleq \{p_1, ..., p_6\}$, constitute the physical nodes of the system.

Accordingly, one of the purposes of this wide protection concept is to disconnect physical components, such as transmission lines, to stop the propagation of a detected disturbance. This is known as disturbance isolation. When the protection system successfully isolates a disturbance, as per its design requirements, the underlying protection scheme is known to be "dependable" [226]. In addition, the protection system is required to be "secure" which dictates that the system takes protective actions *only* in the event of occurrence of anomalies [226]. Thus, falsely disconnecting a component of the system during normal operation is seen as a security breach.

To this end, a malicious attacker can target the security of the system by compromising a number of cyber nodes n_a and manipulating their sent data, to falsely trip a certain transmission line. Here, $\boldsymbol{\kappa} = [\kappa_1, ..., \kappa_{12}]$ is the failure probability vector of the 12 cyber nodes (i.e. probability of a cyber node sending false data) and $\boldsymbol{\pi} = [\pi_1, ..., \pi_6]$ is the vector of probabilities of a false disconnection of a transmission line due to one, or multiple, failures in the cyber system. The degree up to which a failure on the cyber side leads to a disconnection of a transmission line is captured by the matrix $\boldsymbol{R}$ in (6.2). Locally collected data give, naturally, a better indication of the real-time operating state of a transmission line and hence have the most significant effect on the decision of disconnecting that line. Based on this observation, we build $\boldsymbol{R}$ as follows. As shown in Fig. 6.2, each transmission line is affected by data sent from 12 cyber nodes 2 of which are locally connected to it. These local cyber nodes equally share a 50% effect on the decision to disconnect the line while the other 50% is split equally between the 10 remaining cyber nodes. As a result, $\boldsymbol{R}$, such that $\boldsymbol{\pi} = \boldsymbol{\kappa R}$, is represented as follows[3]:

$$r_{i,j} = \begin{cases} 0.25, & \text{if } c_i \text{ is locally connected to } p_j, \\ 0.05, & \text{otherwise.} \end{cases}$$

Next, we focus on the cost of loss, f_{p_i}, of each physical component $p_i \in \mathcal{P}$. A wrongful disconnection of a transmission line can have detrimental effects on the operation and stability of a power system. For example, the 1965 blackout of the Northeast region of the United States and the Ontario province of Canada was caused by a false trip of a transmission line [227]. As a result of such incidents, power system operators adopted what is known as the "$n-1$ security criterion" which requires the system to preserve its normal state of operation after the loss of one of its n components [122]. Based on this reinforced security requirement, a loss of one transmission line does not, typically, affect the safety of a system under low stress operating conditions. Thus, we will focus on another key effect of a false disconnection of a transmission line, namely, the economic effect.

The economic dispatch of the smart grid is based on the solution of an optimal power flow (OPF) problem. A typical OPF problem formulation [228] is an optimization problem aiming at minimizing the total generation cost of the system subject to a set of equality and inequality constraints reflecting the system's operational requirements and physical limits.

To this end, consider V^0 to be the value function of the original OPF problem, i.e. without loss of any transmission line, and V^{p_i} to be the value function of the OPF with loss of transmission line

[3] We use this representation of $\boldsymbol{R}$ as a numerical example of our proposed model. Nonetheless, other numerical representations could have also been equally adopted without affecting the validity of our model and underlying analyses.

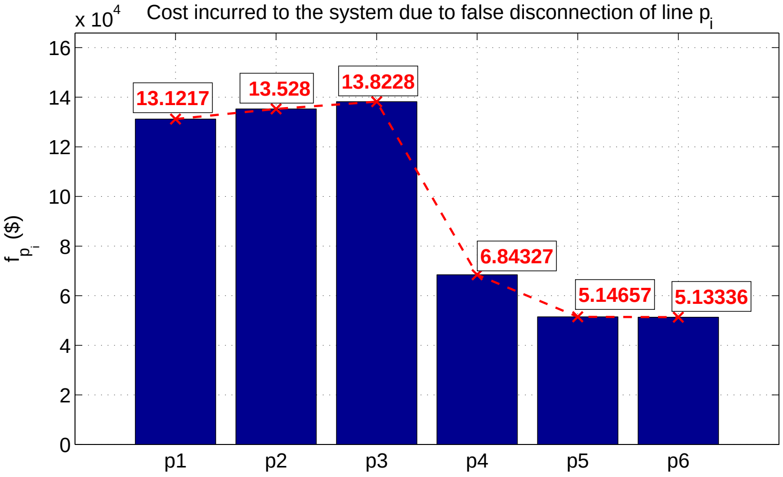

Figure 6.3: Cost to the system incurred by the loss of each transmission line as expressed in (6.9).

$p_i \in \mathcal{P}$. The value function of the OPF problem reflects the total cost of generation spent to meet the load and is normally expressed in \$ per hour. Moreover, consider T^{p_i} (expressed in hours) to be the time needed to bring back p_i into operation and CR^{p_i} (expressed in \$) to be the cost of repair of p_i. Then, f_{p_i} will be given by:

$$f_{p_i} = (V^{p_i} - V^0)T^{p_i} + CR^{p_i}. \tag{6.9}$$

6.3.2 Numerical Results

For the considered PJM 5-bus system, to calculate $f_{p_i}\ \forall p_i \in \mathcal{P}$, we run the optimal power flow seven different times to compute $\{V_0, V^{p_1}, ..., V^{p_6}\}$. Also, we consider that every disconnected transmission line needs 12 hours and costs $\$80,000$ to be brought back into operation[4]. The results are shown in Fig. 6.3. As can be seen from Fig. 6.3, disconnecting p_3 incurs the highest cost to the system ($\$131,220$) followed by p_2, p_1, p_4, p_5 and p_6, respectively.

In our case analysis, we consider that the attacker (defender) aims at attacking (defending) a given transmission line, $p_i \in \mathcal{P}$, by compromising (securing) the two cyber nodes that have the most effect on this line. In other words, for the considered game, the strategy space of the defender and attacker can be defined as follows: $\mathcal{S}_d = \mathcal{S}_a = \{(c_1, c_5), (c_2, c_{10}), (c_3, c_4), (c_6, c_7), (c_8, c_9), (c_{11}, c_{12})\}$. This corresponds to choosing to defend/attack one of the lines in $\mathcal{P}$. Thus, equivalently, $\mathcal{S}_d = \mathcal{S}_a = \{p_1, p_2, p_3, p_4, p_5, p_6\}$.

[4] Such numbers are used as an example and are usually specific to the system and to the line's voltage level and length.

Table 6.1: Attacker's Payoff $U_a(s_i^d, s_j^a)$, [Unit: $\$1,000$]

a d	p_1	p_2	p_3	p_4	p_5	p_6
p_1	-38.82	-141.22	-142.30	-116.71	-110.49	-110.44
p_2	-139.60	-38.69	-142.17	-116.58	-110.35	-110.31
p_3	-139.50	-140.99	-38.59	-116.48	-110.26	-110.21
p_4	-141.82	-143.31	-144.40	-40.92	-112.58	-112.53
p_5	-142.39	-143.88	-144.96	-119.37	-41.48	-113.10
p_6	-142.39	-143.88	-144.97	-119.37	-113.15	-41.49

The defender and attacker aim at maximizing their expected utility functions, $\bar{U}_i$, given by (6.5). The payoff $U_d(s_d, s_a)$ of the defender for the different $s_d \in \mathcal{S}_d$ and $s_a \in \mathcal{S}_a$ is presented in Table 6.1 in which the row player is the defender and the column player is the attacker[5]. The payoff of the attacker for the different strategy combinations is the negative of that of the defender given that the game is of zero-sum type.

When both players are strategic thinkers and have complete information of the game, the NE in (6.7) can be found using the von Neumann indifference principle [146]. Applying the von Neumann indifference principle we get the following equilibrium results:

$$\boldsymbol{\gamma}_d^* = [0.2931, 0.3034, 0.3107, 0.0842, 0.0047, 0.0040], \tag{6.10}$$

$$\boldsymbol{\gamma}_a^* = [0.1276, 0.1244, 0.1222, 0.1922, 0.2167, 0.2169]. \tag{6.11}$$

This optimal strategy leads to $\bar{U}_d = -\$110,240$ and $\bar{U}_a = \$110,240$.

On the other hand, as explained previously, the NE assumes that both attacker and defender act strategically and have complete information of the game. However, computing $\boldsymbol{f}$ requires the solution of an OPF which is a complicated optimization problem [229] that requires complete knowledge of the system. The complexity of finding the solution of the OPF in practical applications is thoroughly discussed in [229]. To this end, since the defender is the system operator, it has complete knowledge of the system and has the computational tools that are developed specifically for the solution of the system's OPF. On the other hand, the attacker might not have neither the full knowledge of the system nor the computational capabilities to solve the OPF and compute $f_{p_i} \, \forall p_i \in \mathcal{P}$. In this case, the attacker must build a perception of the ranking of f_{p_i}, for different $p_i \in \mathcal{P}$, to assess which attack strategy is the most harmful to the system. Thus, playing an NE defense strategy against an assumed fully rational attacker might not be an optimal strategy given that the attacker can deviate from its NE strategy due to its bounded rationality.

[5] The defender always has a negative payoff even when the attack is blocked. In fact, with no attack, $\boldsymbol{\pi}^c \neq \mathbf{0}$ since cyber node c_k can fail due to a software bug or misconfiguration. In our numerical analysis we take $\pi_j^c = 1/12 \, \forall j = 1, ..., 12$ prior to attack and defense. $\boldsymbol{\pi}^c$ is small but not equal $\mathbf{0}$.

By applying the proposed model of Section 6.2.3, we can investigate deviations from the NE due to the bounded rationality of the attacker. To this end, we consider that the attacker can take one of three types reflecting three different "thinking levels" as described in Section 6.2.3. A *level 0* attacker, denoted by l_0, is one that chooses an attack strategy randomly (following a uniform distribution) from its strategy set $\mathcal{S}_a$. A *level 1* attacker, denoted by l_1, cannot generate OPF solutions but can observe the power flow on each line (requires eavesdropping rather than solving the computationally demanding OPF). Hence, an attacker l_1 builds a perception of the most harmful line to attack based on the level of power flow on every line. A more loaded line, p_i, is associated with a larger $\hat{f}_{p_i}$. Thus, an l_1 attacker targets the line that is the most loaded. A *level 2* attacker, denoted by l_2, is considered to have full knowledge of the system and high computational ability and can hence solve the OPF and compute $f_{p_i}\,\forall p_i \in \mathcal{P}$. Thus, l_2 can compute the exact $\boldsymbol{f}$ and attacks the line p_i with highest f_{p_i}.

In our model, the defender performs the highest thinking level since it has the capability and knowledge to think strategically. In fact, through historical data, the defender can build an anticipation about the potential thinking levels that an attacker may perform. Thus, the defender anticipates what the attack strategy can be, based on a distribution of possible attacker's types, and plays a best response defense strategy that maximizes its expected payoff. On the other hand, the attacker may not be able to acquire such accurate knowledge about what the defender's strategy may be. Thus, the attacker forms a perception of the harm that its attack can have. Then, the attacker bases its attack on this perception since it assumes that the defender is equally likely to defend any of the cyber nodes. In other words, the attacker assumes the defender to be a level 0 thinker.

Next, we compute the best response strategy of the defender when faced with an attacker belonging to one of the three types. $\gamma_a^{l_k}$ corresponds to attacker l_k's attack strategy while $\gamma_d^{l_k}$ denotes the best response of the defender against this strategy.

To this end, we first consider l_0 which chooses a line to attack randomly. Thus, its strategy is given by $\gamma_a^{l_0}(s_a) = 1/6\,\forall s_a \in \mathcal{S}_a$. To determine the best response of the defender facing an l_0 attacker, we show, in Fig. 6.4, the expected utility of the defender when choosing each of its possible strategies. By checking the values of the achieved expected utility when defending a line p_i (dashed line in Fig. 6.4), one can see that the best response of the defender against an l_0 attacker is to choose to defend p_3. That is, $\gamma_d^{l_0}(p_3) = 1$ and $\gamma_d^{l_0}(p_j) = 0\,\forall p_j \neq p_3$ which results in $\bar{U}_d^{l_0}(\gamma_d^{l_0}, \gamma_a^{l_0}) = -\bar{U}_a^{l_0}(\gamma_d^{l_0}, \gamma_a^{l_0}) = -\$109,340$.

Considering the case of an l_1 attacker, its bounded rationality dictates attacking the line carrying the highest power flow since a disconnection of such a line is perceived to cause the highest harm to the system. Let $\boldsymbol{\omega}$ be the vector of power flows over lines $\{p_1, ..., p_6\}$ with no disconnection of any of these lines. Running an OPF of the PJM 5-bus system results in the following flows expressed in MW: $\boldsymbol{\omega} = [252.38, 187.87, 230.25, 49.21, 24.95, 238.5]$. Given that p_1 bears the highest power flow, $\gamma_a^{l_1}$ consists of attacking line p_1 with probability equals to 1. Based on Table 6.1, the defender's best response against $\gamma_a^{l_1}$ is to choose to defend line p_1 with probability 1 ($\gamma_d^{l_1}(p_1) = 1$). These defense and attack strategies result in $\bar{U}_d^{l_1}(\gamma_d^{l_1}, \gamma_a^{l_1}) = -\bar{U}_a^{l_1}(\gamma_d^{l_1}, \gamma_a^{l_1}) = -\$38,830$.

In contrast to l_1, an l_2 attacker has the ability and the knowledge to solve the OPF and characterize

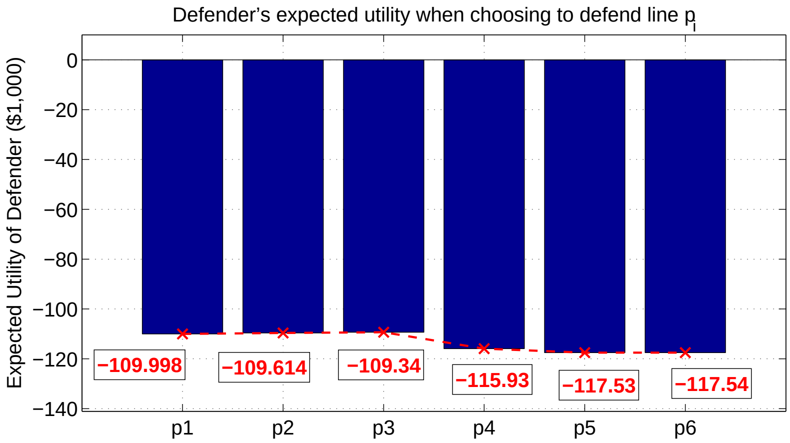

Figure 6.4: Defender's expected utility when defending one of the lines $p_i \in \mathcal{P}$ facing an l_0 attacker.

the line with highest f_{p_i}. As shown in Fig. 6.3, line p_3's loss is the most harmful. Hence, $\gamma_a^{l_2}$ consists of attacking line p_3 with probability 1. The best response of the defender to this strategy can be obtained from Table 6.1 and consists of defending p_3 with a probability 1 ($\gamma_d^{l_2}(p_3) = 1$). These defense and attack strategies result in $\bar{U}_d^{l_2}(\gamma_d^{l_2}, \gamma_a^{l_2}) = -\bar{U}_a^{l_2}(\gamma_d^{l_2}, \gamma_a^{l_2}) = -\$38,590$.

Given that the defender might be faced with an attacker from any of the three types, it aims to devise an optimal strategy that achieves the best expected utility facing the possible three types. The probability that the attacker is of level l_k is given by $\alpha(k)$ which can follow, for example, the distribution in (6.8) or any other distribution which can, for example, be obtained from any empirical analyses or historical data. Here, rather than assuming the distribution in (6.8), we focus on the case in which the ratio of probabilities of level $k+1$ to level k is a constant and we denote this ratio by τ. Thus, $\alpha(1)/\alpha(0) = \alpha(2)/\alpha(1) = \tau$. Using this relation and noting that $\alpha(0) + \alpha(1) + \alpha(2) = 1$, we can express $\alpha(0)$ as: $\alpha(0) = 1/(1 + \tau + \tau^2)$.

From our derived best response expressions, $\gamma_d^{l_0}$, $\gamma_d^{l_1}$ and $\gamma_d^{l_2}$, we know that the defender would defend line p_3 when faced with an l_0 or l_2 attacker while the defender would defend line p_1 when faced with an l_1 attacker. Given the defined probabilities of each attacker's type, we can calculate the expected payoff of the defender when faced with an attacker $l_k \triangleq \alpha(0)l_0 + \alpha(1)l_1 + \alpha(2)l_2$. This latter notation means that l_k corresponds to a combination of types l_0, l_1 and l_2 with probability $\alpha(0), \alpha(1)$ and $\alpha(2)$, respectively. Following from the expressions of $\bar{U}_d^{l_0}$, $\bar{U}_d^{l_1}$ and $\bar{U}_d^{l_2}$ as well as from Table 6.1, the expected utility of the defender when defending p_1 and p_3 can be expressed as follows:

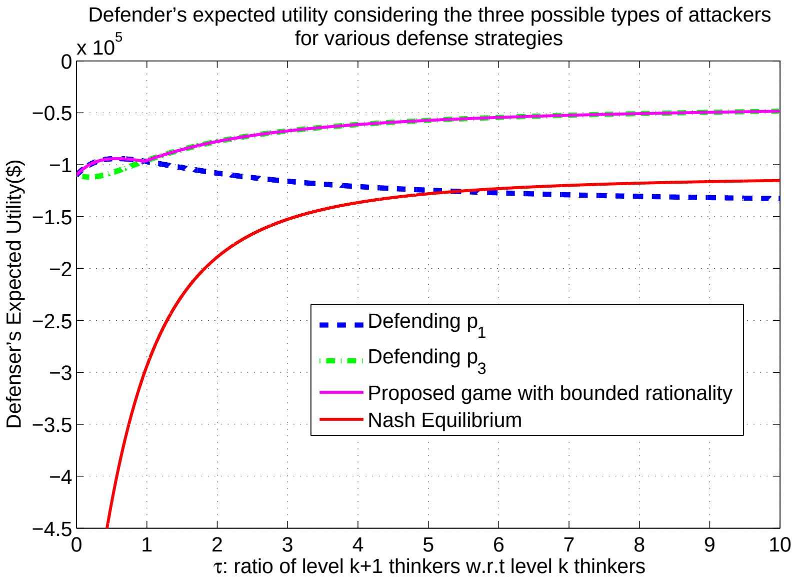

Figure 6.5: Defender's expected utility when facing an attacker which can be of types l_0, l_1, and l_2.

$$\begin{aligned}
\bar{U}_d(p_1, l_k) &= \alpha(0)\bar{U}_d(p_1, l_0) + \alpha(1)\bar{U}_d(p_1, l_1) + \alpha(2)\bar{U}_d(p_1, l_2)\\
&= -109.998\alpha(0) - 38.823\alpha(1) - 142.302\alpha(2)\\
&= -109.998\alpha(0) - 38.823\alpha(0)\tau - 142.302\alpha(0)\tau^2\\
\bar{U}_d(p_3, l_k) &= -109.336\alpha(0) - 139.489\alpha(1) - 38.823\alpha(2)\\
&= -109.336\alpha(0) - 139.489\alpha(0)\tau - 38.823\alpha(0)\tau^2
\end{aligned}$$

As a result, the defender picks p_1 when $\bar{U}_d(p_1, l_k) > \bar{U}_d(p_3, l_k)$, picks p_3 when $\bar{U}_d(p_1, l_k) < \bar{U}_d(p_3, l_k)$, and is indifferent when $\bar{U}_d(p_1, l_k) = \bar{U}_d(p_3, l_k)$. Thus, the defender chooses the strategy, $\gamma_d^{l_k *}$ which results in $\bar{U}_d^*(\gamma_d^{l_k *}, l_k) = \max\big(\bar{U}_d(p_1, l_k), \bar{U}_d(p_3, l_k)\big)$.

Fig. 6.5 shows the optimal expected utility achieved by the defender when playing $\gamma_d^{l_k *}$ for an increasing ratio τ. Fig. 6.5 shows that the defender achieves a better expected utility, $\bar{U}_d^*$, when playing $\gamma_d^{l_k *}$ against $\gamma_a^{l_k}$ as compared to the NE utility achieved when choosing γ_d^*, in (6.10), against $\gamma_a^{l_k}$. Thus, given that the attacker can act with bounded rationality in security applications, accounting for this bounded rationality has achieved a better payoff for the defender as compared to playing the NE strategy. For $\tau = 0.5$, the defender achieves a 78% increase in its expected utility by choosing $\gamma_d^{l_k *}$ instead of γ_d^*. This increase drops to 67% for $\tau = 1$ and 55% for $\tau = 5$. The value of τ gives an indication about the probability of having a lower or higher level attacker. In fact, $\tau < 1$ indicates that a low level attacker is more probable while $\tau > 1$ indicates that a higher level attacker is more probable. Thus, the general trend shows that when the probability of a high level attacker increases, the gain from deviating from the NE defense strategy decreases.

Moreover, it can be seen from Fig. 6.5, that the defender's optimal strategy is to defend p_1 for approximately $\tau < 1$ and defend p_3 for $\tau > 1$. This implies that when it is more probable to face a low level attacker, the defender optimally defends against the targeted line, p_1. In contrast, when facing a more intelligent attacker is more probable, $\tau > 1$, the defender's optimal strategy is to defend p_3 which is the most probable target of a high level attacker.

6.4 Summary

In this chapter, we studied the security of the smart grid in the presence of an attacker and defender. We have first introduced a general CPS security model showing how attacks can propagate from the cyber to the physical system. We have then formulated the interaction between attacker and defender using a game-theoretic model. In addition, we have introduced a bounded rationality framework inspired by cognitive hierarchy theory that is suitable to model the limited levels of thinking of the attacker. We have applied our framework to the concept of wide area protection of the smart grid and its energy markets implications. We have shown that when considering bounded rationality of the attacker, the defender can achieve a better protection of the system. We have also shown that when the cognitive level of the attacker increases, the gain from deviating from the NE defense strategy decreases.

Chapter 7

Distributed Storage for Enhanced Smart Grid Resilience

7.1 Introduction

The emerging concept of microgrids (MGs) will play a major role in the modernization of the power grid. Microgrids are small-scale local power grids which are, typically, composed of renewable generation units, storage devices, and energy consumers [230]. MGs are managed by various MG operators (MGOs) and can operate in either connected or islanded modes, and are expected to bring forth innovative solutions for the smart grid by enhancing power management and providing energy reserves via storage.

Indeed, the storage capability of MGs can be used to assist in the energy management of the smart grid as investigated by a number of recent works [231–233]. However, more recently, there has been considerable interest in using the storage abilities of MGs to enhance the resilience of the smart grid against emergency events such as natural disasters or cyber-physical security breaches. In this regard, various academic, industrial, and federal reports [234–236] have proposed leveraging the MGs' storage capacity to mitigate the effect of loss of generation during emergencies by meeting the smart grid's most critical loads. Indeed, distributed storage and generation units, the integral constituents of MGs, have played an essential role in preserving the operation of hospitals and police stations, as well as fire fighting and rescue services centers in many recent emergency situations in the United States [236]. For instance, this has been the case during natural disasters such as hurricanes Katrina and Rita, and the wildfires which interrupted the transmission of electricity to parts of Utah in 1995 and 2003, as well as in the 2003 North American Northeast blackout [236]. In addition to the various reports in [234–236] that encourage the use of MG storage to enhance grid resilience, other works such as [237] and [238] have also investigated the issues related to power quality that might arise when a critical load is supplied by MG energy sources. However, there is a lack of works that analyze the willingness and ability of MGOs to participate in covering the power grid's critical loads.

To this end, in order to leverage the distributed storage units across MGs, the power companies must offer significant financial incentives for the MGOs to keep a portion of their energy surplus in storage for potential emergency use. The MGOs are hence faced with the choice of selling their excess at the current market price, or storing it and potentially selling it at the significantly higher emergency price, in the future. Moreover, given the fact that the energy bought in case of emergency is limited, competition will arise between the different MGOs who seek to take advantage of the incentives offered by the power company for emergency energy.

In this regard, game theory [147] can be used to model the interdependency between MGOs and predict the outcomes of their competitive behavior. In fact, game-theoretic analysis has been a popular tool for understanding the interactions between storage owners in smart grid energy management [231–233]. However, these works do not investigate the aforementioned scenarios in which storage is used for improving resilience. Moreover, these works typically rely on games with complete information, which are not practical for smart grid scenarios.

Another key drawback of existing game-theoretic analysis is the assumption that all players are rational and thus seek to maximize their expected utilities in a similar objective manner. In a real-life application however, as observed by the experimental studies in [148] and [149], the behavior of individuals can deviate considerably from the rational principles of conventional game theory. In this regard, the framework of *prospect theory* (PT) [148] can be used to model the non-rational behavior of MGOs in the presence of uncertainty such as renewable energy sources [164], and its impact on the ability of MGs to meet the power grid's critical load.

The main contribution of this chapter is to propose a new framework for analyzing the storage strategy of MGOs in order to enhance smart grid resilience. In this regard, we formulate a non-cooperative Bayesian game between multiple MGOs to account for the incomplete information of each MGO regarding the excess of energy of its opponents. In this game, each MGO must choose a portion of its MG's energy excess to store so as to maximize a utility function that captures the tradeoff between selling at the current market price and potentially selling in the future at a significantly higher emergency energy price. In contrast to conventional game theory, we develop a prospect-theoretic framework that models the behavior of MGOs when faced with the uncertainty of their opponents' stored energy, which stems from the presence of intermittent renewable energy sources. In particular, we account for each MGO's valuation of its gains and losses with respect to its own individual utility evaluation perspective, as captured via the PT framing effect [148] by a utility reference point. This reference point represents a utility that an individual MGO anticipates and it originates from previous experiences and future aspirations of profits, which can differ in between MGOs [149].

For this proposed game, we derive the closed-form expression for the Bayesian Nash equilibrium (BNE) for the classical game-theoretic scenario and interpret this equilibrium under different conditions. For the PT case, we propose a best response algorithm that allows the MGOs to reach a BNE in a decentralized fashion. Simulation results highlight the difference in MGO behavior between the fully rational case of classical game theory (CGT) and the prospect-theoretic scenario. Indeed, for certain reference points, MGOs choose to store more energy under PT compared to CGT, while the case is reversed for other reference points where MGOs noticeably reduce their

MGs' stored energy. In addition, the impact of the reference point is found to be more prominent as the emergency price increases. The power company must therefore quantify the subjective behavior of the MGOs before choosing the optimal emergency energy price, in order to meet the critical load at minimal cost.
The rest of this chapter is organized as follows. Section 7.2 presents the system model and provides the Bayesian game formulation. Section 7.3 presents the game solution under classical game theory, while Section 7.4 introduces the game solution under prospect theory. Section 7.5 presents and interprets a set of simulation results; while Section 7.6 concludes the chapter.

We note that the results presented in this chapter are based on a collaborative work with Mr. Georges El Rahi. In this regard, the co-authors have equally contributed to this work in terms of the problem formulation as well as the presented mathematical models, derivations, and results.

7.2 System Model and Bayesian Game Formulation

7.2.1 System Model

Consider a large-scale smart grid managed by a power company that integrates a set $\mathcal{N}$ of N microgrids, each of which is managed by an MG operator. Microgrids are small-scale distribution grids which typically include renewable generation units, storage devices, and energy consumers. Each MG operator manages all energy trades conducted by its own MG. Each MG $n \in \mathcal{N}$, managed by its MGO n, includes a storage unit with capacity $Q_{n,\max}$ which can be used to store the excess of energy produced. Given the intermittent nature of renewable energy sources, each MG's energy surplus $Q_n \in [0, Q_{n,\max}]$ is unknown beforehand and will vary over time. A positive Q_n indicates that an MG has extra energy while $Q_n = 0$ indicates that no surplus is available. Given an amount of energy surplus, Q_n, an MGO n has the option of selling this stored energy to the grid at the corresponding retail price, ρ, or saving it for later use in case of emergency, for improved resilience. In this regard, each MGO will choose a portion $\alpha_n \in [0, 1]$ of its MG's Q_n to store and will consequently sell the rest. In case of emergency or blackout, the power company will purchase the stored energy to cover a certain required critical load L_c, until normal power supply is restored.

In order to increase the resilience of the power grid against emergency events, the power company will encourage the MGOs to store part of their MGs' excess by offering a price ρ_c per unit of stored energy purchased in case of emergency. Typically, ρ_c must be significantly larger than ρ to incentivize the MGOs to store the excess. If the total stored energy exceeds the needed L_c, the power company will no longer purchase the entire energy stored by each MG.

Let $\boldsymbol{\alpha}$ and $\boldsymbol{Q}$ be the vectors that represent, respectively, the storage strategy and the available energy surpluses of all the MGOs in the set $\mathcal{N}$. In this respect, when $\boldsymbol{\alpha}^{\intercal}\boldsymbol{Q} > L_c$, the power company will purchase, from each MG n, an amount of energy D_n given by:

$$D_n = \left(\alpha_n Q_n - \frac{\boldsymbol{\alpha}^\intercal \boldsymbol{Q} - L_c}{N}\right)^+, \tag{7.1}$$

where $(q)^+ = \max(0, q)$. $\boldsymbol{\alpha}^\intercal \boldsymbol{Q} - L_c$ is the amount by which the total stored energy exceeds the required L_c. Let θ be the expected probability of an emergency event occurring. Then, each MGO n will choose its optimal storage strategy α_n to optimize the following utility function:

$$U_n(\boldsymbol{\alpha}, \boldsymbol{Q}) = \begin{cases} \rho\left(Q_n - \alpha_n Q_n\right) + \theta\rho_c\alpha_n Q_n, & \text{if } \boldsymbol{\alpha}^\intercal \boldsymbol{Q} \leq L_c, \\ \rho\left(Q_n - \alpha_n Q_n\right) + \theta\rho_c D_n, & \text{otherwise.} \end{cases} \tag{7.2}$$

Note that, when $\theta\rho_c < \rho$, the MGOs will have no incentive to store their MGs' excess and, hence, they will sell all the available surplus at the current market price. Thus, hereinafter, we restrict our analysis to the case $\theta\rho_c > \rho$. As seen from (7.2), the driving factor in determining an MGO's optimal strategy is the total energy stored by its opponents. In fact, as $\boldsymbol{\alpha}^\intercal \boldsymbol{Q} - L_c$ increases, so will the amount of stored energy which will not be bought in case of emergency. Indeed, the MGO could have instead sold that energy at the current market price and made a profit. Given this trade-off between selling at the current market price and storing the excess for a potentially higher profit in case of emergency, each MGO aims at maximizing its utility function by choosing the optimal storage strategy α_n, while also accounting for the actions of its opposing MGs.

Each MGO is typically fully aware of the presence of all N MGs in the power grid and knows the size of their storage devices. In addition, each MGO knows the exact amount of energy excess available to its own MG. However, an MGO cannot determine the energy excess of other MGs. In fact, obtaining such information is not possible especially given the intermittent renewable energy sources and the time-varying nature of energy consumption. Each MGO thus assumes the excess of energy Q_m of other MGs to be a random variable that follows a certain probability distribution function $f_n(Q_m)$ over $[0, Q_{m,\text{max}}]$ where $m \in \mathcal{N} \setminus \{n\}$. We refer to Q_n as the *type* of MGO n and, to $f_n(Q_m)$, as MGO n's *belief* of another MGO m's type. In fact, when MGO n chooses a certain storage strategy α_n, it is uncertain of the profit it will gain. This uncertainty stems from its incomplete information regarding the type of its opponents, originating from the intermittent renewable energy and the time-varying nature of energy consumption, as well as from randomness of an emergency event.

Given the competition over the financial incentives offered by the power company for emergency energy, the MGOs' actions and utility are highly interdependent thus motivating a game-theoretic approach [147]. In addition, given the incomplete information of the opponents' excess of energy that directly affects the MGOs' utility, each MGO will maximize its expected utility given its own beliefs $f_n(Q_m)$. MGO n's expected utility, $E_n(\boldsymbol{\alpha}, Q_n)$, will therefore be given by

$$E_n(\boldsymbol{\alpha}, Q_n) = \mathbb{E}_{\boldsymbol{Q}_{-n}}\left[U_n(\boldsymbol{\alpha}, \boldsymbol{Q})\right], \tag{7.3}$$

where $\boldsymbol{Q}_{-n}$ is the vector that represents the energy excess of all MGs in the set $\mathcal{N} \setminus \{n\}$. The strategic interactions between the various MGOs under incomplete information can be modeled using Bayesian game models [147].

7.2.2 Bayesian Game Formulation

We formulate a static noncooperative Bayesian game [147] between the different MGOs in the set $\mathcal{N}$. In this game, each MGO seeks to maximize its expected utility given its beliefs of its opponents' energy excess by choosing its optimal storage strategy. Since the decisions on the portion of energy to store are coupled, as captured by (2), we adopt a game-theoretic approach. Formally, we define a strategic game $\Xi = \{\mathcal{N}, \{\mathcal{A}_n\}_{n\in\mathcal{N}}, \{\mathcal{T}_n\}_{n\in\mathcal{N}}, \{\mathcal{F}_n\}_{n\in\mathcal{N}}, \{U_n\}_{n\in\mathcal{N}}\}$ where $\mathcal{N}$ is the set of all MGOs, $\mathcal{A}_n$ is the action space which represents the possible storage strategies of each player n, $\mathcal{T}_n$ is the set of types of MGOs that represent the possible energy surplus for each their MGs, $\mathcal{F}_n$ is the set of beliefs of player n represented by the probability distributions of each of its opponents' types, and U_n is the utility function of player n defined in (7.2). In order to find the solution of the proposed game, we first define the two key concepts of *best response strategy* and *Bayesian Nash equilibrium.*

Definition 17. *The set of* best response strategies *of an MGO $n \in \mathcal{N}$ to the strategy profile $\boldsymbol{\alpha}_{-n}$, $r(\boldsymbol{\alpha}_{-n})$, is defined as*

$$r_n(\boldsymbol{\alpha}_{-n}) = \{\alpha_n^* \in \mathcal{A}_n | \mathbb{E}_{\boldsymbol{Q}_{-n}}\left[U_n(\alpha_n^*, \boldsymbol{\alpha}_{-n}, \boldsymbol{Q})\right] \geq \mathbb{E}_{\boldsymbol{Q}_{-n}}\left[U_n(\alpha_n, \boldsymbol{\alpha}_{-n}, \boldsymbol{Q})\right], \forall \alpha_n \in \mathcal{A}_n\},$$

where $\boldsymbol{\alpha}_{-n}$ is the vector that represents the storage strategy of all MGOs in the set $\mathcal{N} \setminus \{n\}$.

In other words, when the strategies of the opponents are fixed to $\boldsymbol{\alpha}_{-n}$, any best response strategy would maximize player n's expected utility, given its beliefs $\mathcal{F}_n$ of its opponents' types. In our analysis, we assume that an MGO's belief $f_n(Q_m)$ over its opponent's energy surplus follows a uniform distribution over the domain $[0, Q_{m,\text{max}}]$. We next define the concept of a pure strategy Bayesian Nash equilibrium.

Definition 18. *A strategy profile $\boldsymbol{\alpha}^*$ is said to be a* pure strategy Bayesian Nash equilibrium *if every MGO's strategy is a best response to the other MGOs' strategies, i.e.*

$$\alpha_n^* \in r_n(\boldsymbol{\alpha}_{-n}^*) \, \forall n \in \mathcal{N}. \tag{7.4}$$

In the proposed game, at the BNE, no MGO n, can increase its expected utility by unilaterally deviating from its storage strategy α_n^*.

In what follows, we will derive closed-form expressions of the BNEs for the case in which two MGs are located in the proximity of the critical load. In fact, power supply to the critical load from distant MGs might not be feasible due to transmission barriers and significant power losses. As such, given these limitations and the scale of a given microgrid, the analysis for two MGs will be quite representative.

7.3 Two-Player Game Solution under Classical Game-Theoretic Analyses

For the case in which two MGs ($N = 2$) are capable of supplying the critical load, the expected utility of MGO 1 given its belief of MGO 2's type can be written as

$$E_1(\boldsymbol{\alpha}, Q_1) = \int_0^{Q_{2,\max}} U_1(\boldsymbol{\alpha}, \boldsymbol{Q}) f_1(Q_2) dQ_2, \tag{7.5}$$

where $\boldsymbol{\alpha} = [\alpha_1 \ \alpha_2]$ and $\boldsymbol{Q} = [Q_1 \ Q_2]$. For the two-MG case, we have

$$U_1(\boldsymbol{\alpha}, \boldsymbol{Q}) = \begin{cases} \rho Q_1 \left(1 - \alpha_1\right) + \theta \rho_c \alpha_1 Q_1 & \text{if } \alpha_2 \leq \frac{L_c - \alpha_1 Q_1}{Q_2}, \\ \rho Q_1 \left(1 - \alpha_1\right) + \theta \rho_c D_1 & \text{otherwise.} \end{cases} \tag{7.6}$$

Next, we assume that neither of the MGs owns a large enough storage device to fully supply the critical load on its own. Under this assumption, D_1 will be given by

$$D_1 = \alpha_1 Q_1 - \frac{1}{2} \left(\alpha_1 Q_1 + \alpha_2 Q_2 - L_c\right). \tag{7.7}$$

In order to find the solution of the proposed game, we first derive the best response strategy of each player which we then use to compute the different BNEs.

7.3.1 Best Response Strategies

The best response strategy of each MGO is characterized next. In fact, we present the following propositions that analyze MGO 1's best response for different values of α_2.

Proposition 9. *The best response of MGO* 1*, for* $\alpha_2 \in \left[0, \frac{L_c - Q_1}{Q_{2,max}}\right]$*, is given by* $r_1(\alpha_2) = 1$*. MGO* 1 *thus maximizes its expected utility by storing its MG's entire energy excess.*

Proof. For $\alpha_2 \leq \frac{L_c - Q_1}{Q_{2,\max}}$, the total stored energy is below the critical load for all types of MGO 2 and all strategies of MGO 1 since $\alpha_2 Q_{2,\max} + Q_1 \leq L_c$. Thus, MGO 1's best response is to store its entire energy excess which is fully sold in case of emergency. In fact, here, $E_1(\boldsymbol{\alpha}, Q_1) = U_1(\boldsymbol{\alpha}, \boldsymbol{Q}) = \rho \left(Q_1 - \alpha_1 Q_1\right) + \theta \rho_c \alpha_1 Q_1$ since $U_1(\boldsymbol{\alpha}, \boldsymbol{Q})$ is independent of Q_2 for this case, as seen in (7.6). $E_1(\boldsymbol{\alpha}, Q_1)$ is clearly an increasing function, given that $\rho_c \theta > \rho$, which is maximized at its upper boundary ($\alpha_1 = 1$). Thus $r_1(\alpha_2) = 1$ for $\alpha_2 \in \left[0, \frac{L_c - Q_1}{Q_{2,\max}}\right]$. □

Proposition 10. *The best response of MGO* 1*, for* $\alpha_2 \in \left[\frac{L_c - Q_1}{Q_{2,max}}, 1\right]$*, is given by*

$$r_1(\alpha_2) = \begin{cases} \frac{L_c\rho_c\theta + (\rho_c\theta - 2\rho)\alpha_2 Q_{2,max}}{Q_1\rho_c\theta}, & \textit{if } \left[\frac{2\rho}{\rho_c\theta} - 1\right]\alpha_2 > \frac{L_c - Q_1}{Q_{2,max}}, \\ 1, & \textit{if } \left[\frac{2\rho}{\rho_c\theta} - 1\right]\alpha_2 \leq \frac{L_c - Q_1}{Q_{2,max}}. \end{cases} \tag{7.8}$$

Proof. For the proof of Proposition 2, first, we analyze the expected utility of MGO 1, for $\alpha_1 \in \left[0, \frac{L_c - \alpha_2 Q_{2,\max}}{Q_1}\right]$ and $\alpha_1 \in \left[\frac{L_c - \alpha_2 Q_{2,\max}}{Q_1}, 1\right]$, with $\alpha_2 \in \left[\frac{L_c - Q_1}{Q_{2,\max}}, 1\right]$.

a) For $\alpha_1 \in \left[0, \frac{L_c - \alpha_2 Q_{2,\max}}{Q_1}\right]$, the total energy stored is below the critical load L_c for all possible types of MGO 2. Here, MGO 1's expected utility is given by

$$E_{1,2a}(\boldsymbol{\alpha}, Q_1) = \rho\left(Q_1 - \alpha_1 Q_1\right) + \theta\rho_c\alpha_1 Q_1.$$

$E_{1,2a}$ is a strictly increasing function given that $\theta\rho_c > \rho$, hence, it is maximized at its upper boundary $\alpha^*_{1,2a} = \frac{L_c - \alpha_2 Q_{2,\max}}{Q_1}$.

b) For $\alpha_1 \in \left[\frac{L_c - \alpha_2 Q_{2,\max}}{Q_1}, 1\right]$, given MGO 2's strategy, the total energy stored is above the critical load for certain types of MGO 2. MGO 1's expected utility is given by

$$E_{1,2b}(\boldsymbol{\alpha}, Q_1) = \int_0^A U_1(\boldsymbol{\alpha}, \boldsymbol{Q}) f(Q_2) dQ_2 + \int_A^{Q_{2,\max}} U_1(\boldsymbol{\alpha}, \boldsymbol{Q}) f(Q_2) dQ_2, \tag{7.9}$$

with $A = \frac{L_c - \alpha_1 Q_1}{\alpha_2}$ which follows from (5). Under this assumption, $f_1(Q_2) = 1/Q_{2,\max}$ over its domain and $E_{1,2b}$ is now given by

$$\begin{aligned} E_{1,2b}(\boldsymbol{\alpha}, Q_1) = \frac{1}{Q_{2,\max}} \int_0^A \left[\rho\left(Q_1 - \alpha_1 Q_1\right) + \theta\rho_c\alpha_1 Q_1\right] dQ_2 + \\ \frac{1}{Q_{2,\max}} \int_A^{Q_{2,\max}} \left[\rho\left(Q_1 - \alpha_1 Q_1\right) + \frac{1}{2}\theta\rho_c\left(\alpha_1 Q_1 - \alpha_2 Q_2 + L_c\right)\right] dQ_2. \end{aligned} \tag{7.10}$$

By taking the second derivative of (7.10) with respect to the decision variable α_1, we get

$$\frac{\partial E_{1,2b}}{\partial^2 \alpha_1} = -\frac{Q_1^2 \rho_c \theta}{2\alpha_2 Q_{\max,2}}.$$

The function is strictly concave given that its second derivative is strictly negative. The optimal solution is, hence, obtained by the necessary and sufficient optimality condition given by

$$\frac{\partial E_{1,2b}}{\partial \alpha_1} = 0. \tag{7.11}$$

(7.11) has a unique solution which is given by

$$\alpha_{1,r} = \frac{L_c\rho_c\theta + (\rho_c\theta - 2\rho)\alpha_2 Q_{2,\max}}{Q_1\rho_c\theta}.$$

Given that $E_{1,2b}$ is a strictly concave function and that α_1 is restricted to $\left[\frac{L_c-\alpha_2Q_{2,\max}}{Q_1}, 1\right]$, $\alpha^*_{1,2b}$ will be

$$\alpha^*_{1,2b} = \begin{cases} \frac{L_c-\alpha_2Q_{2,\max}}{Q_1}, & \text{if } \alpha_{1,r} < \frac{L_c-\alpha_2Q_{2,\max}}{Q_1}, \\ \alpha_{1,r}, & \text{if } \alpha_{1,r} \in \left[\frac{L_c-\alpha_2Q_{2,\max}}{Q_1} \quad 1\right], \\ 1, & \text{if } \alpha_{1,r} > 1. \end{cases} \tag{7.12}$$

In fact, $\alpha_{1,r}$ is the optimal solution for $E_{1,2b}$ if it belongs to the feasible region of $E_{1,2b}$. On the other hand, if $\alpha_{1,r}$ is larger than the upper bound, then $E_{1,2b}$ is a strictly increasing function over the feasibility set and is maximized at its upper bound $\alpha^*_{1,2b} = 1$. Finally, if $\alpha_{1,r}$ is smaller than the domain's lower bound $\frac{L_c-\alpha_2Q_{2,\max}}{Q_1}$, then $E_{1,2b}$ is a strictly decreasing function over the feasibility set and is maximized at its lower bound. However, the condition $\alpha_{1,r} < \frac{L_c-\alpha_2Q_{2,\max}}{Q_1}$ cannot be satisfied for $\rho_c\theta > \rho$, and thus $\frac{L_c-\alpha_2Q_{2,\max}}{Q_1}$ cannot be the maximizer of $E_{1,2b}$. We can thus rewrite (7.12) as

$$\alpha^*_{1,2b} = \begin{cases} \alpha_{1,r}, & \text{if } \left[\frac{2\rho}{\rho_c\theta} - 1\right]\alpha_2 > \frac{L_c-Q_1}{Q_{2,\max}}, \\ 1, & \text{if } \left[\frac{2\rho}{\rho_c\theta} - 1\right]\alpha_2 \leq \frac{L_c-Q_1}{Q_{2,\max}}. \end{cases} \tag{7.13}$$

We first note that $E_{1,2a} = E_{1,2b}$ for $\alpha_1 = \frac{L_c-\alpha_2Q_{2,\max}}{Q_1}$ which is the maximizer of $E_{1,2a}$. However, as previously discussed, $E_{1,2b}$ cannot be maximized at $\frac{L_c-\alpha_2Q_{2,\max}}{Q_1}$. Thus, the maximizer of MGO 1's expected utility, for $\alpha_2 \in \left[\frac{L_c-Q_1}{Q_{2,\max}}, 1\right]$, belongs to the domain $\left[\frac{L_c-\alpha_2Q_{2,\max}}{Q_1}, 1\right]$. In other words, $r_1(\alpha_2) = \alpha^*_{1,2b}$ for $\alpha_2 \in \left[\frac{L_c-Q_1}{Q_{2,\max}}, 1\right]$. □

Given the previous propositions, an MGO's best response strategy is thus summarized in the following theorem.

Theorem 11. *The best response strategy of MGO* 1*,* $r_1(\alpha_2)$*, is given by*

$$r_1(\alpha_2) = \begin{cases} 1, & \textit{if } \alpha_2 \le \frac{L_c - Q_1}{Q_{2,\mathit{max}}}, \\ \alpha_{1,r}, & \textit{if } \alpha_2 > \frac{L_c - Q_1}{Q_{2,\mathit{max}}} \textit{ and } \left[\frac{2\rho}{\rho_c\theta} - 1\right]\alpha_2 > \frac{L_c - Q_1}{Q_{2,\mathit{max}}}, \\ 1, & \textit{if } \alpha_2 > \frac{L_c - Q_1}{Q_{2,\mathit{max}}} \textit{ and } \left[\frac{2\rho}{\rho_c\theta} - 1\right]\alpha_2 \le \frac{L_c - Q_1}{Q_{2,\mathit{max}}}. \end{cases} \tag{7.14}$$

MGO 2*'s best response strategy* $r_2(\alpha_1)$ *is derived similarly and is the same as (*7.14*) but with indices* 1 *and* 2 *interchanged.*

Proof. The proof follows from Propositions 1 and 2. □

7.3.2 Derivation and Interpretation of the Game Equilibria

Given the MGOs' best response function in (7.14), we will compute all possible BNEs for this game. We will then derive and interpret the conditions needed for each BNE to exist.

Theorem 12. *The proposed MGO game admits four possible Bayesian Nash equilibria for different conditions that relate the MG parameters,* Q_n *and* $Q_{n,\mathit{max}}$*, with power grid parameters* ρ*,* ρ_c*,* θ*, and* L_c*. The strategy profiles (*α_1^*, α_2^**), that constitute the four BNEs, are the following:*
1) First BNE: (1,1).
2) Second BNE: $\left(1, \dfrac{L_c\rho_c\theta + (\rho_c\theta - 2p)Q_{1,\mathit{max}}}{Q_2\rho_c\theta}\right)$.
3) Third BNE: $\left(\dfrac{L_c\rho_c\theta + (\rho_c\theta - 2p)Q_{2,\mathit{max}}}{Q_1 p_c\theta}, 1\right)$.
4) Fourth BNE: $\left(\alpha_{1,4}^*, \alpha_{2,4}^*\right)$ *is the strategy profile that constitute the fourth BNE, where*

$$\alpha_{1,4}^* = \frac{-L\rho_c\theta(Q_2\rho_c\theta - 2Q_{2,\mathit{max}}\rho + Q_{2,\mathit{max}}\rho_c\theta)}{Q_{1,\mathit{max}}Q_{2,\mathit{max}}\left(4\rho^2 + \rho_c^2\theta^2 - 4\rho\rho_c\theta\right) - Q_1Q_2\rho_c^2\theta^2},$$
$$\alpha_{2,4}^* = \frac{-L\rho_c\theta(Q_1\rho_c\theta - 2Q_{\mathit{max},1}\rho + Q_{1,\mathit{max}}\rho_c\theta)}{Q_{1,\mathit{max}}Q_{2,\mathit{max}}\left(4\rho^2 + \rho_c^2\theta^2 - 4\rho\rho_c\theta\right) - Q_1Q_2\rho_c^2\theta^2}.$$

Proof. The strategy profiles of the BNEs are derived by solving the set of best-response equations, $\alpha_1^* = r_1(\alpha_2^*)$ and $\alpha_2^* = r_2(\alpha_1^*)$, for the different possible combinations of the best response strategies. □

The conditions under which each BNE is defined are further summarized and interpreted next.

First BNE

the strategy profile (1,1) constitutes a BNE of the proposed game if any of the following four conditions is satisfied:

a) $L_c \geq Q_{2,\max} + Q_1$ and $L_c \geq Q_{1,\max} + Q_2$. Here, each MGO is aware that the total stored energy is below the critical load, regardless of the type and strategy of its opponent.

b) $L_c \geq Q_{2,\max} + Q_1$ and $\frac{2\rho}{\rho_c\theta} - 1 \leq \frac{L_c - Q_2}{Q_{1,\max}} < 1$. Here, MGO 1 knows that the total stored energy is always below the critical load regardless of the type and strategy of its opponent. On the other hand, MGO 2 is aware that part of its MG's stored energy might not be sold in case of emergency. However, ρ_c is large enough compared to ρ to satisfy the condition under which MGO 2 stores its MG's entire excess.

c) $\frac{2\rho}{\rho_c\theta} - 1 \leq \frac{L_c - Q_1}{Q_{2,\max}} < 1$ and $L_c \geq Q_{1,\max} + Q_2$. The analysis of this condition is the same as condition b) with the order of the players reversed.

d) $\frac{2\rho}{\rho_c\theta} - 1 \leq \frac{L_c - Q_1}{Q_{2,\max}} < 1$ and $\frac{2\rho}{\rho_c\theta} - 1 \leq \frac{L_c - Q_2}{Q_{1,\max}} < 1$. In this case, both MGOs are aware that part of their stored energy might not be sold. However, ρ_c is large enough compared to ρ to satisfy the conditions for which both MGOs store their MGs' entire excess.

Second BNE

the strategy profile $\left(1, \frac{L_c\rho_c\theta + (\rho_c\theta - 2p)Q_{1,\max}}{Q_2\rho_c\theta}\right)$ constitutes a BNE of the proposed game if any of the following two conditions are satisfied:

a) $L_c \geq \frac{L_c\rho_c\theta + (\rho_c\theta - 2p)Q_{1,\max}}{Q_2\rho_c\theta} Q_{2,\max} + Q_1$ and
$\frac{2\rho}{\rho_c\theta} - 1 > \frac{L_c - Q_2}{Q_{1,\max}}$. In this case, MGO 1 knows that given MGO 2's storage strategy, the total stored energy is always below the critical load. Meanwhile, MGO 2 is aware that, given MGO 1's strategy, the total stored energy might exceed the critical load and part of its stored energy might not be sold in case of emergency. MGO 2 will not store the entire excess given that ρ_c is not large enough compared to ρ.

b) $\left[\frac{2\rho}{\rho_c\theta} - 1\right] \frac{L_c\rho_c\theta + (\rho_c\theta - 2\rho)Q_{1,\max}}{Q_2\rho_c\theta} \leq \frac{L_c - Q_1}{Q_{2,\max}}$,
$\frac{L_c - Q_1}{Q_{2,\max}} < \frac{L_c\rho_c\theta + (\rho_c\theta - 2\rho)Q_{1,\max}}{Q_2\rho_c\theta}$ and $\frac{2\rho}{\rho_c\theta} - 1 > \frac{L_c - Q_2}{Q_{1,\max}}$. Here, both MGOs know that given their opponent's strategy, part of their MG's stored energy might not be sold. The emergency price ρ_c is large enough compared to ρ to satisfy the condition for which MGO 1 stores the entire excess, however, it is not large enough for MG 2 to fully store its MG's entire excess.

Third BNE

The interpretation of the third BNE is similar to that of the second but with index 1 swapped with 2.

Fourth BNE

The strategy profile $\left(\alpha^*_{1,4}, \alpha^*_{2,4}\right)$, defined in Theorem 2, constitutes a BNE which is obtained by solving the set of equations $\alpha^*_1 = \alpha_{1,r}$ and $\alpha^*_2 = \alpha_{2,r}$, in the case where the following condition is satisfied:

a) $\alpha^*_{2,4}\left[\frac{2\rho}{\rho_c\theta} - 1\right] > \frac{L_c - Q_1}{Q_{2,\max}}$ and $\alpha^*_{1,4}\left[\frac{2\rho}{\rho_c\theta} - 1\right] > \frac{L_c - Q_2}{Q_{1,\max}}$.

Under this condition, both MGOs know that given their opponent's strategy, part of their MG's stored energy might not be sold. The emergency price ρ_c is not large enough to satisfy the conditions under which either MGO stores the entire excess.

Our previous analysis assumes that all MG operators are fully rational and their behavior can thus be modeled using classical game-theoretic analysis. However, this assumption might not hold true in a real smart grid, given that the operators of the MGs might have different subjective valuations of the payoffs gained from selling their energy surplus. Next, we will use the framework of prospect theory [148] to model the behavior of MGOs when faced with such uncertainty and subjectivity of profits, stemming from the presence of renewable energy and the uncertainty it imposes on the volume of energy surplus that other MGOs generate.

7.4 Prospect-Theoretic Analyses

In a classical noncooperative game, a player evaluates an objective expected utility. However, in practice, individuals tend to subjectively perceive their utility when faced with uncertainty [148]. In our model, an MGO's uncertainty originates from the presence of renewable energy and the uncertainty it imposes on the volume of energy surplus that the opposing MGOs generate. In fact, an MGO is uncertain of the portion of its MG's stored energy that will be sold in case of emergency, which is directly related to the energy surplus available to its opponents. Since MGOs are humans, they will perceive the possible profits of energy trading, in terms of gains and losses.

This motivates the application of PT to account for the MGO's subjectivity while choosing the optimal energy portion to store. PT is a widely used tool for understanding human behavior when faced with uncertainty of alternatives. In our analysis, we will inspect the effect of the key notion of utility framing from prospect theory. Utility framing states that a utility is considered a gain if it is larger than the reference point, while it is perceived as a loss if it is smaller than that reference point. We define R_n as the reference point of a given MGO n. The choice of R_n can be different between MGOs as it reflects personal expectations of profit from selling the energy surplus. In this regard, a certain profit, r, originating from a particular energy trade, will be perceived differently by an MGO used to reaping larger profits as opposed to an MGO that usually generates lower profits. In fact, an MGO n with historically high profits would have a high reference point, $R_n > r$, and will hence consider r to be a loss, whereas, an MGO m with relatively low historical profits would have a lower reference point, $R_m < r$ and would hence consider r to be a gain. Consequently, to model this subjective perception of losses and gains we need to redefine the utility function of the MGOs using PT framing [149]:

$$V\left(U_n\left(\boldsymbol{\alpha}, \boldsymbol{Q}\right)\right) = \begin{cases} \left(U_n(\boldsymbol{\alpha}, \boldsymbol{Q}) - R_n\right)^{\beta+} & \text{if } U_n(\boldsymbol{\alpha}, \boldsymbol{Q}) > R_n, \\ -\lambda_n \left(R_n - U_n(\boldsymbol{\alpha}, \boldsymbol{Q})\right)^{\beta^-} & \text{if } U_n(\boldsymbol{\alpha}, \boldsymbol{Q}) < R_n, \end{cases} \tag{7.15}$$

where $0 < \beta^- \leq 1, 0 < \beta^+ \leq 1$ and $\lambda \geq 1$.

$V(\cdot)$ is the framing value function that is concave in gains and convex in losses with a larger slope for losses than for gains [149]. In fact, PT studies show that the aggravation that an individual feels for losing a sum of money is greater than the satisfaction associated with gaining the same amount [148], which explains the introduction of the loss multiplier λ_n. In addition, the framing principle states that an individual's sensitivity to marginal change in its utility diminishes as we move further away from the reference point, which explains the introduction of the gain and loss exponents β^+ and β^-.

It is important to note that, as an MGO chooses to store a larger portion α of its MG's energy, its potential payoffs will now span a larger range of values. In other words, as an MGO stores more energy, it will now have the possibility to make higher expected profits by selling more in case of emergency. On the other hand, by storing more energy, the MGO risks making less profit whenever its opponent has also stored a significant part of its own energy. These probable payoffs are related to the type of the opponent. In fact, the MGO would get a maximum profit for the case in which the opponent's type is small, i.e. the opponent did not have a significant energy surplus. For the case in which the opponent's type is large, a significant part of an MG's stored energy will not be sold in case of emergency, resulting in lower possible payoffs for its MGO, compared to smaller values of α. This concept is key in our PT analysis, given that payoffs are evaluated through comparison to the reference point. Similarly to our analysis for the CGT case, we will first derive the best response strategy of the MGOs.

Proposition 11. *The best response of MGO* 1 *under PT, for* $\alpha_2 \in \left[0, \frac{L_c - Q_1}{Q_{2,max}}\right]$*, is to store its entire energy excess, similarly to the classical game theory analysis.*

Proof. As seen from Proposition 1, for $\alpha_2 \in \left[0, \frac{L_c - Q_1}{Q_{2,\text{max}}}\right]$, $U_1(\boldsymbol{\alpha}, \boldsymbol{Q})$ is an increasing function over its domain. Given that the framing function $V(\cdot)$ is an increasing function as well, MGO 1's expected utility, $E_{1,\text{PT}}(\boldsymbol{\alpha}, Q_1) = V\left(U_1\left(\boldsymbol{\alpha}, \boldsymbol{Q}\right)\right)$, is thus maximized at its upper boundary of $\alpha_1 = 1$. □

We next derive the expected utility of MGO 1 under PT for $\alpha_2 \in \left[\frac{L_c-Q_1}{Q_{2,\max}}, 1\right]$. MG 1's expected utility for $\alpha_2 \in \left[\frac{L_c-Q_1}{Q_{2,\max}}, 1\right]$ takes different values for $\alpha_1 \in \left[0, \frac{L_c-\alpha_2 Q_{2,\max}}{Q_1}\right]$ and $\alpha_1 \in \left[\frac{L_c-\alpha_2 Q_{2,\max}}{Q_1}, 1\right]$:

Proposition 12. *For* $\alpha_1 \in \left[0, \frac{L_c-\alpha_2 Q_{2,max}}{Q_1}\right]$ *and* $\alpha_2 \in \left[\frac{L_c-Q_1}{Q_{2,max}}, 1\right]$*, MGO 1's expected utility under PT,* $E_{PT,1,2a}$*, is given by*

$$E_{PT,1,2a}(\boldsymbol{\alpha}, Q_1) = \begin{cases} -\lambda_1 \left(R_1 - U_{1,2a}\right)^{\beta_1^-} & \text{if } \alpha_1 \leq B, \\ \left(U_{1,2a} - R_1\right)^{\beta_1^+} & \text{if } \alpha_1 > B, \end{cases} \tag{7.16}$$

where $U_{1,2a} = \rho\left(Q_1 - \alpha_1 Q_1\right) - \theta\rho_c\alpha_1 Q_1$*, and* $B = \frac{R_1-\rho Q_1}{Q_1(\rho_c\theta-\rho)}$.

Proof. In Proposition 4, Equation (7.16) follows from the fact that for $\alpha_1 \leq B$, the original utility, $U_{1,2a}$, is below the reference point R_1 and is thus perceived as a loss. On the other hand, it is considered as a gain for $\alpha_1 > B$. □

Proposition 13. *For* $\alpha_1 \in \left[\frac{L_c-\alpha_2 Q_{2,max}}{Q_1}, 1\right]$ *and* $\alpha_2 \in \left[\frac{L_c-Q_1}{Q_{2,max}}, 1\right]$*, player 1's expected utility under PT is given by*

$$E_{PT,1,2b}(\boldsymbol{\alpha}, Q_1) = I_1 + I_2, \tag{7.17}$$

where

$$I_1 = \begin{cases} -\dfrac{\lambda_1(L_c - \alpha_1 Q_1)}{\alpha_2 Q_{max,2}} \left[R_1 - U_{I,1}\right]^{\beta_1^-} & \text{if } \alpha_1 \leq B, \\ \dfrac{L_c - \alpha_1 Q_1}{\alpha_2 Q_{max,2}} \left[U_{I,1} - R_1\right]^{\beta_1^+} & \text{if } \alpha_1 > B, \end{cases} \tag{7.18}$$

$$U_{I,1} = \rho\left(Q_1 - \alpha_1 Q_1\right) + \theta\rho_c\alpha_1 Q_1, \tag{7.19}$$

$$I_2 = \begin{cases} M_l \left[\left(R_1 - U_{max,2}\right)^{\beta_1^-+1} - \left(R_1 - U_{A,2}\right)^{\beta_1^-+1}\right] & \text{if } C_1, \\ M_g \left[\left(U_{r,2} - R_1\right)^{\beta_1^++1} - \left(U_{A,2} - R_1\right)^{\beta_1^++1}\right] + & \\ M_l \left[\left(R_1 - U_{max,2}\right)^{\beta_1^-+1} - \left(R_1 - U_{r,2}\right)^{\beta_1^-+1}\right] & \text{if } C_2, \\ M_g \left[\left(U_{max,2} - R_1\right)^{\beta_1^++1} - \left(U_{A,2} - R_1\right)^{\beta_1^++1}\right] & \text{if } C_3, \end{cases} \tag{7.20}$$

$M_g = \dfrac{-2}{\left(\beta_1^+ + 1\right)\rho_c\theta\alpha_2}$, $M_l = \dfrac{-2\lambda_1}{\left(\beta_1^- + 1\right)\rho_c\theta\alpha_2}$,
$U_{max,2} = \rho\left(Q_1 - \alpha_1 Q_1\right) + \frac{1}{2}\theta\rho_c\left(\alpha_1 Q_1 + L_c - Q_{2,max}\right)$,
$U_{A,2} = \rho\left(Q_1 - \alpha_1 Q_1\right) + \frac{1}{2}\theta\rho_c\left(\alpha_1 Q_1 + L_c - A\right)$, $A = \frac{L_c-\alpha_1 Q_1}{\alpha_2}$, *and*

$U_{r,2} = \rho\left(Q_1 - \alpha_1 Q_1\right) + \frac{1}{2}\theta\rho_c\left(\alpha_1 Q_1 + L_c - Q_{2,r}\right)$, *where* $Q_{2,r}$ *is given in (7.25).*

Conditions C_1, C_2, *and* C_3 *are given by*

$$C_1 : \alpha_1 \leq B, \tag{7.21}$$

$$C_2 \ : \ \alpha_1 \ > \ B \ \textit{and} \ Q_1\left(\theta\rho_c - 2\rho\right)\alpha_1 \ \leq \ \theta\rho_c\alpha_2 Q_{\textit{max},2} \ - \ L_c\rho_c\theta \ - \ 2\rho Q_1 \ + \ 2R_1, \tag{7.22}$$

$$C_3 \ : \ \alpha_1 \ > \ B \ \textit{and} \ Q_1\left(\theta\rho_c - 2\rho\right)\alpha_1 \ > \ \theta\rho_c\alpha_2 Q_{\textit{max},2} \ - \ L_c\rho_c\theta \ - \ 2\rho Q_1 \ + \ 2R_1. \tag{7.23}$$

MGO 2's expected utility function is derived in a similar manner as MGO 1's with indices 1 and 2 reversed.

Proof. Player 1's expected utility under PT, for $\alpha_2 \in \left[\frac{L_c - Q_1}{Q_{2,\max}}, 1\right]$, and $\alpha_1 \in \left[\frac{L_c - \alpha_2 Q_{2,\max}}{Q_1}, 1\right]$, is given by

$$\begin{aligned} E_{\mathrm{PT},1,2b}(\boldsymbol{\alpha}, Q_1) = &\int_0^A \frac{1}{Q_{2,\max}} V\left(\rho\left(Q_1 - \alpha_1 Q_1\right) + \theta\rho_c\alpha_1 Q_1\right) dQ_2 + \\ &\int_A^{Q_{2,\max}} \frac{1}{Q_{2,\max}} V\left(\rho Q_1\left(1 - \alpha_1\right) + \frac{1}{2}\theta\rho_c\left(\alpha_1 Q_1 - \alpha_2 Q_2 + L_c\right)\right) dQ_2. \end{aligned} \tag{7.24}$$

We denote by I_1 the first integral in (7.24), and by I_2 the second. As previously mentioned, PT states that a utility is perceived in terms of gains and losses with respect to the reference point. Next, we analyze the possible values of both integrals I_1 (first integral) and I_2 (second integral) in (7.24) from that perspective. The original utility in I_1, $U_{I,1} = \rho\left(Q_1 - \alpha_1 Q_1\right) + \theta\rho_c\alpha_1 Q_1$, is only a function of α_1 and is independent of Q_2. Equation (7.18) follows from the fact that for $\alpha_1 \leq B$, $U_{I,1}$ is below the reference point R_1 and is thus perceived as a loss. On the other hand, it is considered as a gain for $\alpha_1 > B$.

We then assess the possible values of I_2. The original utility function in I_2, $U_{I,2} = \rho\left(Q_1 - \alpha_1 Q_1\right) + \frac{1}{2}\theta\rho_c\left(\alpha_1 Q_1 - \alpha_2 Q_2 + L_c\right)$ is considered a loss given that

$$\rho\left(Q_1 - \alpha_1 Q_1\right) + \frac{1}{2}\theta\rho_c\left(\alpha_1 Q_1 - \alpha_2 Q_2 + L_c\right) < R_1,$$

which can be rewritten as $Q_{2,r} < Q_2$ with $Q_{2,r}$ given by

$$Q_{2,r} = \frac{2}{\rho_c\theta\alpha_2}\left[\rho\left(Q_1 - \alpha_1 Q_1\right) + \frac{1}{2}\theta\rho_c\left(\alpha_1 Q_1 + L_c\right) - R_1\right]. \tag{7.25}$$

Given that MGO 1's expected utility is taken over MGO 2's type (Q_2), we next analyze I_2 for different values of Q_2. (7.20) follows from the fact that I_2 is a loss integral for $Q_{2,r} < A$. Given that the lower bound of I_2 is larger than A, then the entire range of Q_2 values is as well. The condition $Q_{2,r} < A$ can be rewritten as C_1. On the other hand, I_2 is a gain integral for $Q_{2,r} > Q_{2,\max}$ which can be rewritten as C_2. Finally, for $A < Q_{r,2} < Q_{2,\max}$, I_2 is split into two parts: a gain integral on $[A, Q_{2,r}]$ and a loss integral on $[Q_{\text{ref2}}, Q_{2,\max}]$. $A < Q_{2,r} < Q_{2,\max}$ can be rewritten as C_3. (7.18) and (7.20) are obtained by evaluating the integrals I_1 and I_2 for the described cases. □

Given the complex structure of each MGO's expected utility function with framing, computing the closed-form expression of the best response strategy is difficult for the PT case. In particular, the analysis of $E_{\text{PT},1,2b}$ is quite challenging due to the various forms that the function can take under different conditions as seen in (7.18) and (7.20). Therefore, in order to find the BNE under PT, a best response algorithm is proposed.

This iterative algorithm dictates that, in response to its opponent's current strategy, each MGO sequentially chooses its optimal storage strategy by numerically characterizing, from its action space, the action that maximizes its expected utility. In fact, given the closed-form expressions provided in Propositions 3, 4, and 5, an MGO can easily compute its expected utility for each of its strategies. In this respect, upon convergence, this algorithm is guaranteed to reach an equilibrium [147]. In fact, at the point of convergence, each MGO is playing the strategy that maximizes its expected PT utility facing its opponent's strategy. Hence, the MGOs will reach a BNE from which none has any incentive to deviate since such deviation would not improve their expected payoff. Indeed, as observed in our simulations in Section V, the algorithm always converged to an equilibrium.

7.5 Simulation Results

For our simulations, we consider a smart grid with $N = 2$ MGs capable of supplying power to one of the power grid's critical loads which requires a total of $L_c = 200$ kWh to remain operational until regular power supply is restored. We also assume the regular price per unit of energy to be $\rho = \$0.1$ per kWh. In addition, we take $\theta = 0.01$, and $\rho_c = \$11.6$ per kWh unless stated otherwise. The exponents β^+ and β^- are taken to be both equal to 0.88 and the loss multiplier $\lambda = 2.25$ unless stated otherwise [149]. We simulate the system for two scenarios: CGT, and PT under utility framing.

Fig. 7.1 compares the effects of different MGO reference points on the total energy stored for both CGT and PT analysis. In the classical game theory case $(\beta^+ = \beta^- = \lambda = 1)$, an MGO's reference point is irrelevant given that losses and gains are computed in an identical objective manner. For the PT case, for a reference point below \$8, the BNE action profile is not significantly affected compared to the classical game theory case, since most potential payoffs of the BNE actions are still viewed as gains above the reference point. As the reference point increases from \$8 to $\$11.5$, the total stored energy will decrease from around 200 to 184 kWh, since some of the potential payoffs of the current BNE will start to be perceived as losses, as they cross the reference point.

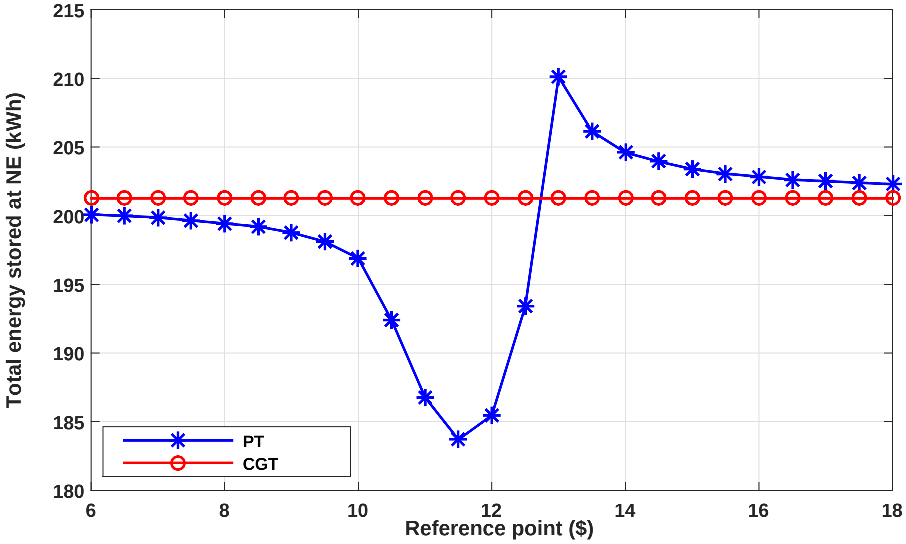

Figure 7.1: Total stored energy under classical game theory and prospect theory.

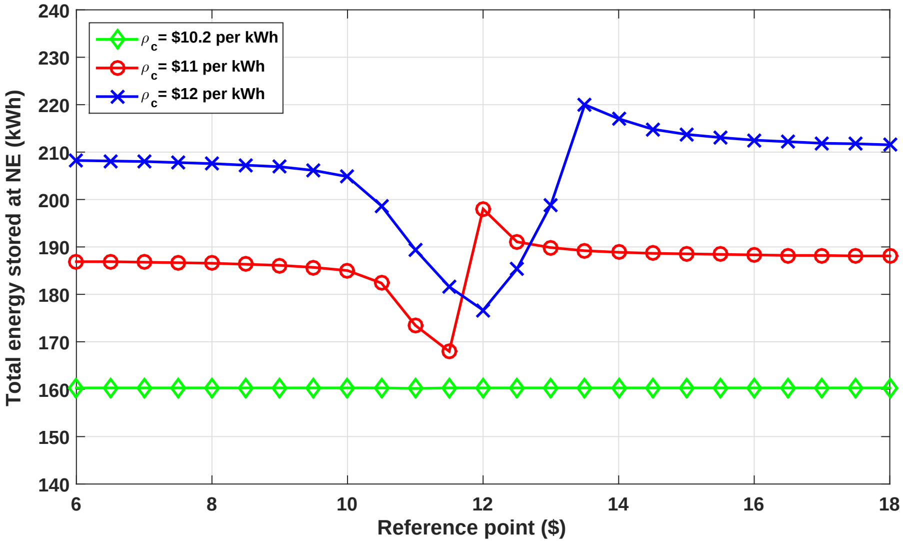

Figure 7.2: Effect of emergency price on PT sensitivity to the reference point.

Given that losses have a larger weight under PT compared to classical game theory, the expected utility of the current strategy profile will significantly decrease, thus causing the BNE to drift towards lower storage strategies. The MGOs will exhibit risk averse behavior as they sell more of their energy at the current risk-free retail market price ρ. In fact, as previously mentioned, by decreasing α, the minimum potential payoffs are larger, compared to the larger values of α, and are still above the reference point.

The described behavior is reversed in the $[11.5, 13]$ range where the MGOs start exhibiting more risk seeking behavior, i.e., storing more energy, to reach a total stored energy of 210 kWh. In fact,

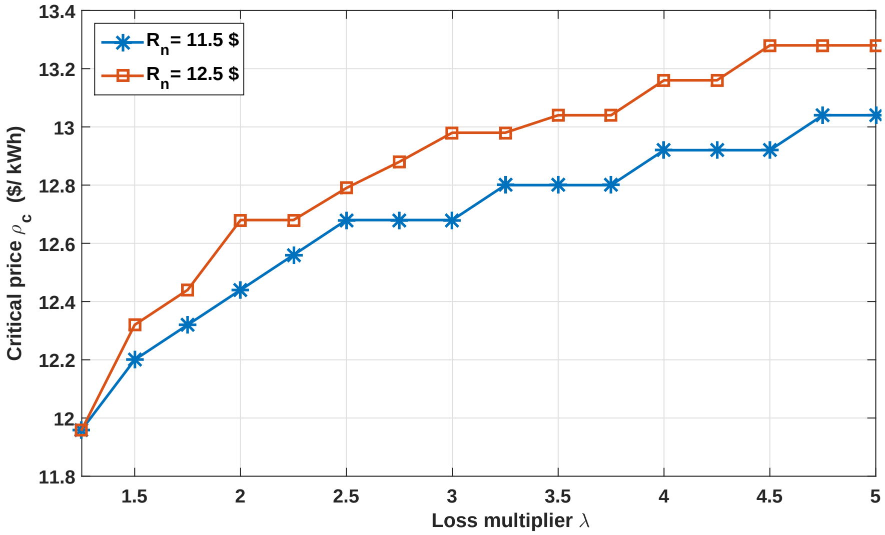

Figure 7.3: Emergency price needed to cover L_c as a function of λ.

the low risk strategies' potential payoffs are now fully perceived as losses causing a significant devaluation of their expected utility values. The BNE will thus go towards higher values of α with larger maximum payoffs, compared to lower values of α, which are partially still considered as gains. Finally, when the reference point is above $\$13.5$, most potential payoffs of most strategies are now perceived as losses and the effect of PT will diminish gradually, and the total energy stored will reach 202 kWh, identically to classical game theory. It is important to note that the critical load energy requirements are 200 kWh, which is met with the stored energy of the MGs under classical game theory but not necessarily under PT analysis. This highlights the need for an accurate behavioral analysis of the studied system.

Fig. 7.2 shows the effect of changing the emergency price ρ_c on the role of the reference point in an MGO's decision, for $\lambda = 4$. For a price of $\rho_c = \$10.2$ per kWh, the total energy stored does not vary with the reference point. In fact, the expected future profits gained from storing energy are close to the profits incurred by selling at the current market price. On the other hand, when the price is increased to $\rho_c = \$11$ per kWh, the total stored energy will vary with the reference point by up to 10% from its original value. In fact, storing energy will now yield significantly higher expected future profits, compared to selling at the current market price. Thus, an MGO's risk-seeking or risk-averse behavior is justified given the increasing uncertainty in profits. Similarly, when $\rho_c = \$12$ per kWh, the total stored energy would vary further with the changing reference point, by up to 17% from its original value.

Fig. 7.3 shows the effect of the loss multiplier λ on the emergency price ρ_c needed to cover the critical load for the reference points of $\$11.5$ and $\$12.5$. The effect of framing is more prominent as the loss multiplier increases. In fact, the MGOs will exhibit more risk averse behavior for the specified reference points as λ increases, thus prompting the power company to increase the critical price in order to cover the critical load. In fact, as λ increases, so will the valuation of the MGOs'

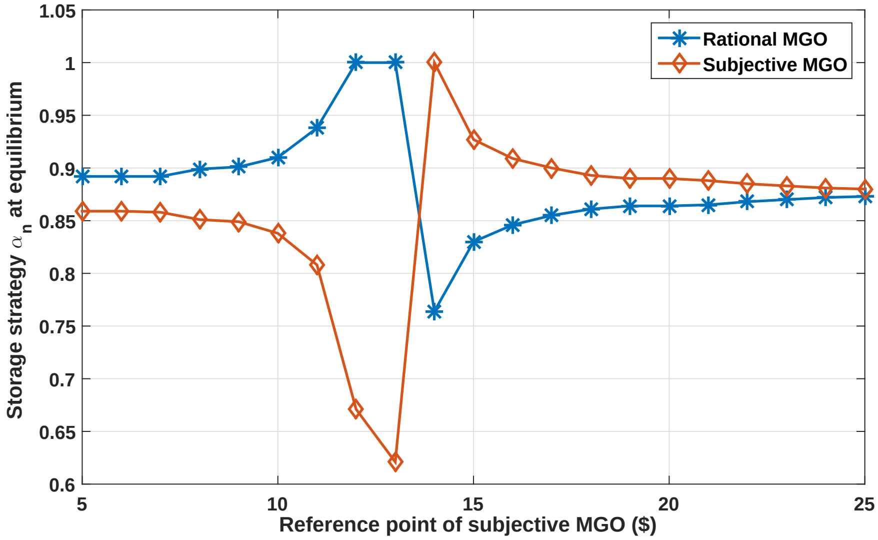

Figure 7.4: Storage strategies at equilibrium for a case with one subjective (PT) MGO and one rational (CGT) MGO.

losses. To avoid the large losses, the MGOs will decrease the energy stored by their MGs and will tend to sell more energy at the current risk free market price. This highlights the importance of behavioral analysis in choosing the proper pricing mechanism in smart grid resilience planning.

Fig. 7.4 illustrates the storage strategies at equilibrium for the case in which one of the MGOs is fully rational, while the second is subjective. The rational MGO will naturally have no reference point. Here, both MGs have the same size of storage $Q_{\max} = 150\,$kWh and energy excess available $Q = 120\,$kWh. As seen in Fig. 7.4, as the reference point of the subjective MGO increases from $\$5$ to $\$13$, it will exhibit risk averse behavior and decrease the portion of energy it stores, to reach a value of 0.625. This is similar to the analysis of Fig. 7.1. To respond, the rational MGO will hence increase the portion of energy stored to reach its maximum of 1, given the lower stored energy of its opponent. As the reference point increases from $\$13$ to $\$14.5$, the subjective MGO will exhibit more risk seeking behavior and increase the portion of energy stored to reach its maximum of 1. The rational MGO, will thus decrease its MG's stored energy, given the storage strategy of its opponent. Finally, as the reference point increases from $\$14.5$ to $\$25$, the effect of utility framing will gradually decrease, and the storage strategy of both MGOs will reach a value of 0.88. Given the negligible effect of PT at the high reference point of $\$25$, both MGOs, rational and subjective, will have equal strategies at equilibrium and thus similar behavioral patterns.

7.6 Summary

In this chapter, we have proposed a novel framework for analyzing the storage strategy of micorgrid operators in an attempt to enhance smart grid resilience. We have formulated the problem as a Bayesian game between multiple MGOs, who must choose the portion of their microgrids' excess to store, in order to maximize their expected profits. The MGOs play a noncooperative game, which is shown to have four Bayesian Nash equilibria for the two MG case, under different conditions. Subsequently, we have used the novel concept of utility framing from prospect theory to model the behavior of MGOs when faced with the uncertainty of their opponents' energy surplus. Simulation results have highlighted the impact of behavioral considerations on the overall process of enhancing the resilience of a smart grid by exploiting distributed, microgrid energy storage.

Chapter 8

Conclusions and Open Problems

In this dissertation, we have identified and addressed a number of challenging security problems in CPSs with human actors. Towards achieving this goal, we have developed a number of mathematical frameworks which capture the operation and security of the studied CPSs; while accounting for the multi-agent interactions within CPSs security settings and explicitly incorporating human decision making processes into the developed frameworks. The performed security analyses have focused on a number of CPS application domains. In this regard, the developed solutions addressed various security problems within the smart electric grid such as: 1) Identifying and defending against observability and data injection attacks which can target the grid, 2) Devising a defense policy to thwart stealthy data injection attacks which can be carried out by multiple adversaries, and 3) Enhancing the resilience of the smart grid by leveraging distributed energy storage. In addition, the developed solutions have also addressed other application areas within the realm of IoT such as the cyber-physical security of time-critical UAV applications, which include drone delivery systems and anti-drone defense systems. In these analyses, we have focused, jointly, on the problem of 1) Finding an optimal path selection strategy for a UAV on a delivery mission to evade attacks, as well as on 2) Devising an optimal interdiction strategy to maximize the likelihood of intercepting a drone on a malicious mission, as part of an anti-drone defense system. In addition to focusing on specific CPSs application domains, this dissertation has also performed a set of analyses addressing general CPSs security problems such as modeling the cyber-physical propagation of threats within CPSs and devising a security strategy to defend the physical components of the CPS against attacks that can penetrate the CPS from its vulnerable cyber entry points.

In this regard, we next present a summary of the research work which have been performed in this dissertation.

8.1 Summary

8.1.1 A Unified Analysis of Observability and Data Injection Attacks in the Smart Grid

In Chapter 3, we have proposed a novel graph-theoretic framework enabling a fundamental unified modeling and analysis of observability and data injection attacks which can target the smart power grid. The proposed framework has introduced a shift in the analysis of observability and data injection attacks from a linear algebra perspective to a graph-theoretic frame of analysis. This graph-theoretic modeling has, as a result, allowed a holistic analysis of observability and data injection attacks requiring only the power system 1-line diagram and the associated locations of the implemented measurement units. Based on this introduced framework, we have characterized the analytical solutions to a number of key observability and data injection attack problems, which have been proposed and studied in literature. The solutions to such problems aim, in particular, at characterizing the possible optimal attack strategies which can target the system as well as deriving optimal defense policies to thwart these attacks. For example, we have shown that our introduced tools allow characterization of the sparsest stealthy attacks (which may or may not include a certain measurement) which can target the power system. In addition, we have shown that the proposed graph-theoretic framework enables an analytical characterization of a minimum set of measurement which when made immune to data injection attacks guarantees thwarting any stealthy attack which can target the system. In addition, we have also shown that our introduced framework allows identifying the minimum set of measurements which, when defended, guarantee that for an attack to potentially be stealthy, it must concurrently compromise a certain number of measurement units which surpasses a defined threshold.

8.1.2 Data Injection Attacks on Smart Grids with Multiple Adversaries

In Chapter 4, we have primarily focused on stealthy data injection attacks which can target the smart grid while addressing, in articular, the potential presence of multiple adversaries. In this regard, a Stackelberg game has been proposed to capture the strategic interactions between the system operator and the adversaries. In the proposed Stackelberg game, the grid operator – aiming at defending the system against potential data injection attacks – acts as the leader and the attackers act as noncooperative followers, aiming at choosing their optimal attack strategies in response to the operator's implemented defense policy. The proposed game model has also allowed the incorporation of the cost of attack and defense in the objective functions of each of the players. For solving the proposed game, we have proven that a generalized Nash equilibrium of the attackers' noncooperative game exists. In addition, we have studied the existence and properties of the equilibrium point of the Stackelberg game (while also considering the potential scarcity of information on the potential adversaries). In this regard, to numerically identify the equilibrium point, we have proposed a learning algorithm which have been shown to successfully converge to the sought equilibrium. Using a numerical analysis, we have shown that the system operator can exploit the competing behavior of potential attackers to successfully defend the system against all potential attacks. In addition, using our derived numerical results, we have characterized the loss level that the defender incurs due to information scarcity about the potential adversaries which may target the system.

8.1.3 Time-critical Network Interdiction Games for Cyber-Physical Security of UAV Systems

In Chapter 5, we have developed a novel mathematical framework which enables analysis of the cyber-physical security of time-critical UAV applications. Time-critical applications include settings such as drone delivery systems and anti-drone systems. The developed framework includes a UAV operator aiming at choosing an optimal path selection policy to reach its target within a minimum expected mission completion time and an interdictor aiming at targeting the UAV with cyber-physical attacks to compromise its mission. In this respect, we have modeled the underlying security problem as a network interdiction game between a UAV operator and an interdictor, where each of the operator and the interdcitor can be benign or malicious. In addition, Chapter 5 have advanced and incorporated principles from cumulative prospect theory in the proposed interdiction game which allows accounting for each player's bounded rationality when making decisions under uncertainty. In this regard, under deterministic strategies, and considering both the fully rational game and the cumulative prospect-theoretic game, we have characterized the necessary conditions for the existence of a Nash equilibrium and derived the equilibrium strategies and game outcome. In addition, when considering a hierarchy in the order of play, we derived the Stackelbeg equilibrium of the game. In addition, considering probabilistic strategies, and considering the fully rational and the cumulative prospect-theoretic games, we have proposed solution algorithms for obtaining the equilibrium strategies of the interdictor and the UAV operator. In addition, we have run a set of simulation results to highlight and analyze the effects of the bounded rationality of the players on their chosen equilibrium strategies and, as a result, the game's outcomes. For example, the obtained numerical results have shown that the players' prospect-theoretic bounded rationality is more likely to be disadvantageous to the UAV operator. In fact, most results have shown that the players' bounded rationality leads to delays in expected mission completion times.

8.1.4 Diffusion of Threats in Cyber-Physical Systems

In Chapter 6, we have introduced a general framework which models the way attacks and threats can propagate from the cyber layer to the physical system in CPSs. In addition, under this threat propagation model, we have considered a potential attacker aiming at targeting a set of cyber nodes with the goal of damaging the physical components of the system by exploiting the cyber-physical propagation of threats. On the other hand, a system defender is considered who aims at selecting a set of cyber nodes to defend to reduce the damage to the physical system which can be caused by cyber attacks. As such, a game-theoretic model is proposed to capture the security interdependence between the attacker and system defender. In addition, using a behavioral model inspired from cognitive hierarchy theory, we have modeled the potential bounded rationality of the attacker by characterizing various levels of skills that the attacker may possess. In addition, the introduced analytical tools have been applied to study the effects of cyber attacks on wide area protection in the smart grid and the implications to the electric energy market which these attacks can entail. In this regard, the generated results have shown the way the attacker's skills affect its chosen attack strategy. In addition, the results have highlighted that by accounting for the potential skill levels of the attacker, the defender can better protect the system against possible attacks.

8.1.5 Enhancing Smart Grid Resilience by Leveraging Distributed Energy Storage

In Chapter 7, we have developed a mathematical framework in which distributed storage capacity in the smart grid could be leveraged for meeting the grids' critical loads in emergency conditions such as during an attack-induced blackout. Indeed, the proliferation of distributed storage has raised the potential of leveraging this distributed storage capacity during blackouts to meet the grid's most critical loads. However, this distributed storage capacity is typically not run by the central electric utility but by local entities or microgrids. Hence, financial incentives must be given to storage capacity owners to save some of their stored capacity for emergency events. Hence, each storage owner is faced with the option of routinely trading its stored energy within the smart grid or to store this energy to potentially sell it in the future, during emergency events, at a higher electricity price. In addition, since the critical load which must be met is limited, each storage owner has no guarantee that all its stored capacity would be used, since this energy can be also fulfilled by other storage owners. As such, we have proposed a novel framework for modeling the decision making processes of storage owners and deriving optimal storage/trading strategies. The problem has been formulated as a Bayesian game between multiple storage owners in which each owner aims to choose its optimal portion of storage capacity to keep stored for emergency events. The game formulation has explicitly accounted for the incomplete information that each storage owner has about its competitors. In addition, we have incorporated notions from prospect theory in the game formulation to model the subjective behavior of each storage owner under uncertainty. In this respect, the equilibrium points of the proposed games have been characterized, which have shown the equilibrium strategies which must be followed by each storage owner. A set of simulation results were also introduced and have shown the impact that the subjective decisions of the storage owners have on the likelihood of storing enough energy to meet the critical load under emergency conditions. This has, hence, highlighted the importance of devising proper financial incentives, which account for the potential subjective behavior of the storage owners, for successfully leveraging the distributed energy storage capacity for enhancing the resilience of the smart grid against emergency events.

8.2 Open Problems

Cyber-physical systems are projected to become central to modern cities and infrastructure and, hence, novel security solutions must be continuously devised to protect these systems against the ever increasing security threats. As such, a number of key open problems which must be investigated are provided next:

8.2.1 General Propagation of Threats in Cyber-Physical Systems

The work presented in Chapter 6 introduced a CPS security framework which can capture the propagation of threats from the cyber layer to the physical system. However, a more general representation of the cyber-physical propagation of threats within CPSs must also account for inter- and intra-layer threats propagation. In this respect, such a generalized model would capture not only the propagation of threats between the cyber and physical systems but also the propagation of threats within each of the cyber and physical realms. Hence, rather than using a bipartite graph to model the propagation of threats, a more general graph-theoretic and probabilistic representation is needed. By developing such generalized threat propagation models, analyses of the effects of a carried out attack can be traced throughout the system and defense strategies can be developed accordingly. In this regard, the intertwined decision making processes of intelligent attackers and defenders can be modeled using game-theoretic tools. In addition, due to the underlying complexities in developing such comprehensive threat propagation models, the involved agents may not always be capable of choosing fully-rational attack and defense strategies. In this respect, capturing such potential bounded rationality in the game-theoretic formulations would allow anticipating the way different types of adversaries might act (based on their skill levels and knowledge), thereby allowing the derivation of effective defense strategies.

8.2.2 General Mechanisms to Leverage Energy Storage for Enhancing Smart Grid Resilience

In Chapter 7, we have investigated leveraging distributed storage for meeting critical loads during emergency situations. With CPS attacks and emergency events potentially causing blackouts that cut power supplies to hospitals, police stations, and rescue services, there is an obvious need to have ready-to-use emergency power which would provide the needed power supplies to such critical loads until normal power operation has been restored. Distributed storage can provide such ready-to-use power for meeting local critical loads. In the analysis in Chapter 7, we have looked at regular and emergency electricity prices being specified by the electric power company without modeling the strategic decision making of this power company. In this regard, as shown in Chapter 7, the choice of the regular and emergency power prices have a direct effect on the energy trading and storing strategies of the storage owners. Hence, when optimally choosing these prices, the utility power company can maximize the likelihood of meeting critical loads during emergency situations.

As such, a potential extension of this work consists of modeling the strategic interaction between the electric power company and the distributed storage units. Based on this modeling, an optimal and effective choice of electricity prices can be devised, by the power company, to offer effective incentives to distributed storage owners – which explicitly account for their potential subjectivity – to participate in such storage management systems for enahncing the resilience of smart grids against emergency events.

8.2.3 Artificial Intelligence Techniques for Securing CPSs

As has been thoroughly addressed in this dissertation, securing CPSs must account for the various multi-agent interactions which take place within a CPS. However, with an increased complexity of the system, and accounting for nonlinearities incorporated by bounded rationality models, analytically analyzing these multi-agent interactions and interdependencies and mathematically solving the resulting games becomes an increasingly arduous task. Hence, developing multi-agent learning algorithms which can learn optimal security-related strategies from successive observations and interactions with the environment, as well as by leveraging historical data, can provide tremendous help in better understanding the multi-agent interactions and interdependencies within the complex settings of CPSs and in devising security solutions which can be effective in defending CPSs against the emerging threats.

Bibliography

[1] R. Alur, *Principles of Cyber-Physical Systems*. MIT Press, 2015, pp. 1–11.

[2] P. Derler, E. Lee, and A. Vincentelli, “Modeling cyber physical systems,” *Proceedings of the IEEE*, vol. 100, no. 1, pp. 13–28, Jan 2012.

[3] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, “Cyber-physical systems: The next computing revolution,” in *47th ACM/IEEE Design Automation Conference (DAC)*, June 2010, pp. 731–736.

[4] “Cyber-physical systems,” http://cyberphysicalsystems.org/, accessed: 2015-11-14.

[5] S. K. Sowe, E. Simmon, K. Zettsu, F. de Vaulx, and I. Bojanova, “Cyber-physical-human systems: Putting people in the loop,” *IT Professional*, vol. 18, no. 1, pp. 10–13, Jan 2016.

[6] F. Wang, “The emergence of intelligent enterprises: From cps to cpss,” *IEEE Intelligent Systems*, vol. 25, no. 4, pp. 85–88, July 2010.

[7] V. Terzija, G. Valverde, D. Cai, P. Regulski, V. Madani, J. Fitch, S. Skok, M. Begovic, and A. Phadke, “Wide-area monitoring, protection, and control of future electric power networks,” *Proceedings of the IEEE*, vol. 99, no. 1, pp. 80–93, Jan 2011.

[8] ETP, “Smartgrids sra 2035 strategic research agenda update of the smartgrids sra 2007 for the needs by the year 2035,” 2012. [Online]. Available: http://www.smartgrids.eu/documents/sra2035.pdf

[9] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications,” *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–1, 2017.

[10] S. Hayat, E. Yanmaz, and R. Muzaffar, “Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint,” *IEEE Communications Surveys Tutorials*, vol. 18, no. 4, pp. 2624–2661, Fourth quarter 2016.

[11] L. Gupta, R. Jain, and G. Vaszkun, “Survey of important issues in uav communication networks,” *IEEE Communications Surveys Tutorials*, vol. 18, no. 2, pp. 1123–1152, Second quarter 2016.

[12] K. P. Valavanis and G. J. Vachtsevanos, *Handbook of Unmanned Aerial Vehicles*. Springer, Dordrecht, 2015.

[13] R. Austin, *Unmanned aircraft systems: UAVS design, development and deployment*. John Wiley & Sons, 2011, vol. 54.

[14] D. S. Gallo, C. Cardonha, P. Avegliano, and T. C. Carvalho, "Taxonomy of citizen sensing for intelligent urban infrastructures," *IEEE Sensors Journal*, vol. 14, no. 12, pp. 4154–4164, Dec 2014.

[15] Z. Xiao, H. B. Lim, and L. Ponnambalam, "Participatory sensing for smart cities: A case study on transport trip quality measurement," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 759–770, April 2017.

[16] J. Zhang, F. Y. Wang, K. Wang, W. H. Lin, X. Xu, and C. Chen, "Data-driven intelligent transportation systems: A survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 4, pp. 1624–1639, Dec 2011.

[17] J. Engelbrecht, M. J. Booysen, G. J. van Rooyen, and F. J. Bruwer, "Survey of smartphone-based sensing in vehicles for intelligent transportation system applications," *IET Intelligent Transport Systems*, vol. 9, no. 10, pp. 924–935, 2015.

[18] S. G. Kashid and S. A. Pardeshi, "A survey of water distribution system and new approach to intelligent water distribution system," in *First International Conference on Networks Soft Computing (ICNSC2014)*, Aug 2014, pp. 339–344.

[19] J. P. Sutton, "Smart medical systems," in *Proceedings of the Second Joint 24th Annual Conference and the Annual Fall Meeting of the Biomedical Engineering Society*, vol. 3, Oct 2002, pp. 2166 – 2167.

[20] T. C. Robert M. Lee, Michael J. Assante, "Analysis of the cyber attack on the Ukranian power grid. defense use case." *SANS ICS*, March 2016. [Online]. Available: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[21] E. Perez, "U.S. investigators find proof of cyberattack on ukraine power grid," *CNN*, February 2016. [Online]. Available: http://www.cnn.com/2016/02/03/politics/cyberattack-ukraine-power-grid/

[22] J. A. Jerkins, "Motivating a market or regulatory solution to iot insecurity with the mirai botnet code," in *7th IEEE Annual Computing and Communication Workshop and Conference (CCWC)*, Jan 2017, pp. 1–5.

[23] S. Burke, "Massive cyber attack turned ordinary devices into weapons," *Reuters*, October 2016. [Online]. Available: http://money.cnn.com/2016/10/22/technology/cyberattack-dyn-ddos/index.html?iid=EL

[24] E. Auchard, “Deutsche telekom says was targeted in global internet attack,” *Reuters*, November 2016. [Online]. Available: http://www.reuters.com/article/deutsche-telekom-outages-idUSL8N1DU4L

[25] D. Kushner, “The real story of stuxnet,” *Spectrum, IEEE*, vol. 50, no. 3, pp. 48–53, March 2013.

[26] J. Slay and M. Miller, *Critical Infrastructure Protection*. Springer, 2008, pp. 73–82.

[27] M. Abrams and J. Weiss, “Malicious control system cyber security attack case study-maroochy water services, australia. national institute of standards and technology,” *Computer Security Division*, 2008.

[28] G. Loukas, *Cyber-physical attacks: a growing invisible threat*. Butterworth-Heinemann, 2015, pp. 21–58.

[29] T. Kim and H. V. Poor, “Strategic protection against data injection attacks on power grids,” *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326–333, June 2011.

[30] O. Kosut, L. Jia, R. Thomas, and L. Tong, “Malicious data attacks on the smart grid,” *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec 2011.

[31] S. Amin, G. A. Schwartz, and S. S. Sastry, “Security of interdependent and identical networked control systems,” *Automatica*, vol. 49, no. 1, pp. 186–192, 2013.

[32] A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson, “Quantifying cyber-security for networked control systems,” in *Control of Cyber-Physical Systems*. Springer, 2013, pp. 123–142.

[33] S. Gorman, “Electricity grid in US penetrated by spies,” *The Wall Street Journal*, vol. 8, 2009.

[34] E. Bumiller and T. Shanker, “Panetta warns of dire threat of cyberattack on U.S,” *New York Times*, vol. 11, p. A1, 2012.

[35] J. Finkle, “US probes cyber attack on water system,” *Reuters*, November 2011. [Online]. Available: http://www.reuters.com/article/2011/11/21/us-cybersecurity-attack-idUSTRE7AH2C320111121

[36] J. G. Kassakian, R. Schmalensee, G. Desgroseilliers, T. D. Heidel, K. Afridi, A. Farid, J. Grochow, W. Hogan, H. Jacoby, J. Kirtley *et al.*, “The future of the electric grid,” *Massachusetts Institute of Technology, Tech. Rep*, pp. 197–234, 2011.

[37] J. Meserve, “Sources: Staged cyber attack reveals vulnerability in power grid,” *CNN. com*, vol. 26, 2007.

[38] P. McDaniel and S. McLaughlin, “Security and privacy challenges in the smart grid,” *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, May 2009.

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

[40] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, “Smart-grid security issues,” *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, Jan 2010.

[41] D. E. Nordell, “Terms of protection: The many faces of smart grid security,” *IEEE Power and Energy Magazine*, vol. 10, no. 1, pp. 18–23, Jan 2012.

[42] A. J. McBride and A. R. McGee, “Assessing smart grid security,” *Bell Labs Technical Journal*, vol. 17, no. 3, pp. 87–103, Dec 2012.

[43] S. J. Pavel Polityuk, Oleg Vukmanovic, “Ukraine’s power outage was a cyber attack: Ukrenergo,” *Reuters*, January 2017. [Online]. Available: http://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA

[44] J. Pagliery, “Sniper attack on california power grid may have been an insider, dhs says,” *CNN. com*, October 2015.

[45] P. W. Parfomak, “Physical security of the U.S. power grid: High-voltage transformer substations,” *Congressional Research Service*, June 2014.

[46] M. Faisal and M. Ibrahim, “Stuxnet, duqu and beyond,” *International Journal of Science and Engineering Investigations*, vol. 1, no. 2, pp. 75–78, 2012.

[47] B. Bencsáth, G. Pék, L. Buttyán, and M. Félegyházi, “Duqu: A stuxnet-like malware found in the wild,” *CrySyS Lab Technical Report*, vol. 14, 2011.

[48] T. Emergency Response, “Duqu: son of stuxnet?” *Computer Fraud & Security*, vol. 2011, no. 11, p. 3, 2011.

[49] K. Boatman, “Can your car be hacked?” *Norton*. [Online]. Available: https://us.norton.com/yoursecurityresource/detail.jsp?aid=car_computer

[50] J. Pagliery, “Cars can be hacked. what about a plane?” *CNN*, July 2015. [Online]. Available: http://money.cnn.com/2015/07/22/technology/car-hack-plane/

[51] C. Rieger, D. Gertman, and M. McQueen, “Resilient control systems: Next generation design research,” in *2nd Conference on Human System Interactions, 2009.*, May 2009, pp. 632–636.

[52] A. Metke and R. Ekl, “Security technology for smart grid networks,” *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99–107, June 2010.

[53] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: A survey of existing protocols and open research issues," *IEEE Communications Surveys Tutorials*, vol. 17, no. 3, pp. 1294–1312, Third quarter 2015.

[54] S. N. Premnath and Z. J. Haas, "Security and privacy in the internet-of-things under time-and-budget-limited adversary model," *IEEE Wireless Communications Letters*, vol. 4, no. 3, pp. 277–280, June 2015.

[55] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ads-b implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 78 – 87, 2011.

[56] C. Finke, J. Butts, R. Mills, and M. Grimaila, "Enhancing the security of aircraft surveillance in the next generation air traffic control system," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 1, pp. 3 – 11, 2013.

[57] K. Hartmann and C. Steup, "The vulnerability of uavs to cyber attacks - an approach to the risk assessment," in *5th International Conference on Cyber Conflict (CYCON 2013)*, June 2013, pp. 1–23.

[58] F. Silva Ferraz and C. Guimaraes Ferraz, "Smart city security issues: Depicting information security issues in the role of an urban environment," in *IEEE/ACM 7th International Conference on Utility and Cloud Computing (UCC)*, Dec 2014, pp. 842–847.

[59] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart community: an internet of things application," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 68–75, November 2011.

[60] F. Silva Ferraz and C. Guimaraes Ferraz, "More than meets the eye in smart city information security: Exploring security issues far beyond privacy concerns," in *11th IEEE Intl Conf on Autonomic and Trusted Computing*, Dec 2014, pp. 677–685.

[61] M. St.John-Green and T. Watson, "Safety and security of the smart city - when our infrastructure goes online," in *9th IET International Conference on System Safety and Cyber Security*, Oct 2014, pp. 1–6.

[62] P. Wang, A. Ali, and W. Kelly, "Data security and threat modeling for smart city infrastructure," in *International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, Aug 2015, pp. 1–6.

[63] Z. Khan, Z. Pervez, and A. Ghafoor, "Towards cloud based smart cities data security and privacy management," in *IEEE/ACM 7th International Conference on Utility and Cloud Computing (UCC)*, Dec 2014, pp. 806–811.

[64] C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol, "Scada cyber security testbed development," in *38th North American Power Symposium*, Sept 2006, pp. 483–488.

[65] R. Berthier, J. G. Jetcheva, D. Mashima, J. H. Huh, D. Grochocki, R. B. Bobba, A. A. Cardenas, and W. H. Sanders, "Reconciling security protection and monitoring requirements in advanced metering infrastructures," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct 2013, pp. 450–455.

[66] F. Cleveland, "Iec tc57 security standards for the power system's information infrastructure - beyond simple encryption," in *IEEE/PES Transmission and Distribution Conference and Exhibition*, May 2006, pp. 1079–1087.

[67] C. Ten, C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for scada systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836–1846, Nov 2008.

[68] G. Hug and J. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sept 2012.

[69] F. Pasqualetti, F. Dorfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC)*, Dec 2011, pp. 2195–2201.

[70] W. Niemira, R. Bobba, P. Sauer, and W. Sanders, "Malicious data detection in state estimation leveraging system losses and estimation of perturbed parameters," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct 2013, pp. 402–407.

[71] R. Mitchell and I. Chen, "Effect of intrusion detection and response on reliability of cyber physical systems," *IEEE Transactions on Reliability*, vol. 62, no. 1, pp. 199–210, March 2013.

[72] S. Zonouz, K. Rogers, R. Berthier, R. Bobba, W. Sanders, and T. Overbye, "Scpse: Security-oriented cyber-physical state estimation for power grid critical infrastructures," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1790–1799, Dec 2012.

[73] L. Mili, "Taxonomy of the characteristics of power system operating states," in *2nd NSF-VT Resilient and Sustainable Critical Infrastructures (RESIN) Workshop*, Jan. 2011, pp. 13–15.

[74] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec 2011.

[75] Y. Liu, P. Ning, and M. K. Reiter, "Data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*. New York, NY, USA: ACM, 2009, pp. 21–32.

[76] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, May 2011.

[77] C. Ten, C. Liu, and M. Govindarasu, “Vulnerability assessment of cybersecurity for scada systems using attack trees,” in *IEEE Power Engineering Society General Meeting*, June 2007, pp. 1–8.

[78] S. Cui, Z. Han, S. Kar, T. Kim, H. Poor, and A. Tajer, “Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions,” *IEEE Signal Processing Magazine*, vol. 29, no. 5, pp. 106–115, Sept 2012.

[79] S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber-physical system security for the electric power grid,” *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, Jan 2012.

[80] E. Bertino and N. Islam, “Botnets and internet of things security,” *Computer*, vol. 50, no. 2, pp. 76–79, Feb 2017.

[81] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, “Non-invasive spoofing attacks for anti-lock braking systems,” in *Cryptographic Hardware and Embedded Systems-CHES 2013*. Springer, 2013, pp. 55–72.

[82] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. Pappas, “Robustness of attack-resilient state estimators,” in *ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, April 2014, pp. 163–174.

[83] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, “Cyber security threat analysis and modeling of an unmanned aerial vehicle system,” in *IEEE Conference on Technologies for Homeland Security (HST)*, Nov 2012, pp. 585–590.

[84] D. He, S. Chan, and M. Guizani, “Communication security of unmanned aerial vehicles,” *IEEE Wireless Communications*, vol. PP, no. 99, pp. 2–7, 2017.

[85] N. M. Rodday, R. d. O. Schmidt, and A. Pras, “Exploring security vulnerabilities of unmanned aerial vehicles,” in *IEEE/IFIP Network Operations and Management Symposium (NOMS)*, April 2016, pp. 993–994.

[86] L. Petnga and H. Xu, “Security of unmanned aerial vehicles: Dynamic state estimation under cyber-physical attacks,” in *International Conference on Unmanned Aircraft Systems (ICUAS)*, June 2016, pp. 811–819.

[87] A. Y. Javaid, W. Sun, and M. Alam, “Uavsim: A simulation testbed for unmanned aerial vehicle network cyber security analysis,” in *IEEE Globecom Workshops (GC Wkshps)*, Dec 2013, pp. 1432–1436.

[88] K. Manandhar, X. Cao, and F. Hu, “Attack detection in water supply systems using kalman filter estimator,” in *35th IEEE Sarnoff Symposium (SARNOFF)*, May 2012, pp. 1–6.

[89] D. Eliades and M. Polycarpou, “A fault diagnosis and security framework for water systems,” *IEEE Transactions on Control Systems Technology*, vol. 18, no. 6, pp. 1254–1265, Nov 2010.

[90] F. Miao, M. Pajic, and G. Pappas, "Stochastic game approach for replay attack detection," in *52nd IEEE Annual Conference on Decision and Control (CDC)*, Dec 2013, pp. 1854–1859.

[91] Q. Zhu and T. Başar, "Robust and resilient control design for cyber-physical systems with an application to power systems," in *Proc. 50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC)*, Dec 2011, pp. 4066–4071.

[92] ——, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Systems*, vol. 35, no. 1, pp. 46–65, Feb 2015.

[93] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 160–169, March 2013.

[94] H. Niu and S. Jagannathan, "Optimal defense and control for cyber-physical systems," in *IEEE Symposium Series on Computational Intelligence*, Dec 2015, pp. 634–639.

[95] S. Amin, G. A. Schwartz, and A. Hussain, "In quest of benchmarking security risks to cyber-physical systems," *IEEE Network*, vol. 27, no. 1, pp. 19–24, January 2013.

[96] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for risk minimization in automatic generation control," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 223–232, Jan 2015.

[97] P. Y. Chen, S. M. Cheng, and K. C. Chen, "Information fusion to defend intentional attack in internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 337–348, Aug 2014.

[98] S. Rass, A. Alshawish, M. A. Abid, S. Schauer, Q. Zhu, and H. de Meer, "Physical intrusion games - optimizing surveillance by simulation and game theory," *IEEE Access*, vol. PP, no. 99, pp. 1–1, 2017.

[99] P. Y. Chen, S. M. Cheng, and K. C. Chen, "Smart attacks in smart grid communication networks," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 24–29, August 2012.

[100] T. Alpcan and S. Buchegger, "Security games for vehicular networks," *IEEE Transactions on Mobile Computing*, vol. 10, no. 2, pp. 280–290, Feb 2011.

[101] C. A. Kamhoua, H. Zhao, M. Rodriguez, and K. A. Kwiat, "A game-theoretic approach for testing for hardware trojans," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 2, no. 3, pp. 199–210, July 2016.

[102] Q. Zhu, C. Rieger, and T. Başar, "A hierarchical security architecture for cyber-physical systems," in *4th International Symposium on Resilient Control Systems (ISRCS)*, Aug 2011, pp. 15–20.

[103] A. Clark, Q. Zhu, R. Poovendran, and T. Basar, “An impact-aware defense against stuxnet,” in *American Control Conference (ACC), 2013*, June 2013, pp. 4140–4147.

[104] Y. Li, L. Shi, P. Cheng, J. Chen, and D. Quevedo, “Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach,” *IEEE Transactions on Automatic Control*, vol. 60, no. 10, pp. 2831–2836, Oct 2015.

[105] Q. Zhu, L. Bushnell, and T. Başar, “Resilient distributed control of multi-agent cyber-physical systems,” in *Control of Cyber-Physical Systems*. Springer, 2013, pp. 301–316.

[106] X. Feng, Z. Zheng, D. Cansever, A. Swami, and P. Mohapatra, “Stealthy attacks with insider information: A game theoretic model with asymmetric feedback,” in *IEEE Military Communications Conference MILCOM*, Nov 2016, pp. 277–282.

[107] A. Gupta, C. Langbort, and T. Başar, “Dynamic games with asymmetric information and resource constrained players with applications to security of cyberphysical systems,” *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 71–81, March 2017.

[108] N. S. V. Rao, C. Y. T. Ma, U. Shah, J. Zhuang, F. He, and D. K. Y. Yau, “On resilience of cyber-physical infrastructures using discrete product-form games,” in *18th International Conference on Information Fusion (Fusion)*, July 2015, pp. 1451–1458.

[109] D. Bauso and H. Tembine, “Crowd-averse cyber-physical systems: The paradigm of robust mean-field games,” *IEEE Transactions on Automatic Control*, vol. 61, no. 8, pp. 2312–2317, Aug 2016.

[110] M. Zhu and S. Martinez, “Stackelberg-game analysis of correlated attacks in cyber-physical systems,” in *American Control Conference (ACC)*, June 2011, pp. 4063–4068.

[111] S. Amin, “Security games on infrastructure networks,” in *Science of Security for Cyber-Physical Systems Workshop (SOSCYPS)*, April 2016, pp. 1–4.

[112] Z. Xu and Q. Zhu, “A cyber-physical game framework for secure and resilient multi-agent autonomous systems,” in *54th IEEE Conference on Decision and Control (CDC)*, Dec 2015, pp. 5156–5161.

[113] ——, “Cross-layer secure cyber-physical control system design for networked 3d printers,” in *2016 American Control Conference (ACC)*, July 2016, pp. 1191–1196.

[114] Z. Zhang, M. Trinkle, A. Dimitrovski, and H. Li, “Combating time synchronization attack: A cross layer defense mechanism,” in *ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, April 2013, pp. 141–149.

[115] Z. Zhang, S. Gong, A. Dimitrovski, and H. Li, “Time synchronization attack in smart grid: Impact and analysis,” *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 87–98, March 2013.

[116] S. H. Horowitz, A. G. Phadke, and J. K. Niemira, *Power system relaying*, 4th ed. Chichester, West Sussex, UK: John Wiley & Sons Inc, 2013.

[117] A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *28th International Conference on Distributed Computing Systems Workshops ICDCS*, June 2008, pp. 495–500.

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

[119] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *47th Annual Allerton Conference on Communication, Control, and Computing*, Sept 2009, pp. 911–918.

[120] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, Nov 2013.

[121] R. Czechowski and A. M. Kosek, "The most frequent energy theft techniques and hazards in present power energy consumption," in *Joint Workshop on Cyber- Physical Security and Resilience in Smart Grids (CPSR-SG)*, April 2016, pp. 1–7.

[122] A. J. Wood and B. F. Wollenberg, *Power generation, operation, and control.* John Wiley & Sons, 2012.

[123] R. Billinton, R. N. Allan, and S. O. service), *Reliability Evaluation of Power Systems*, 2nd ed. Boston, MA: Springer US, 1996.

[124] A. K. Sood and R. J. Enbody, "Targeted cyberattacks: A superset of advanced persistent threats," *IEEE Security Privacy*, vol. 11, no. 1, pp. 54–61, Jan 2013.

[125] E. Baize, "Developing secure products in the age of advanced persistent threats," *IEEE Security Privacy*, vol. 10, no. 3, pp. 88–92, May 2012.

[126] E. L. Quinn, "Privacy and the new energy infrastructure," *Social Science Research Network*, 2009.

[127] Y. Yuan, Q. Zhu, F. Sun, Q. Wang, and T. Başar, "Resilient control of cyber-physical systems against denial-of-service attacks," in *6th International Symposium on Resilient Control Systems (ISRCS)*, Aug 2013, pp. 54–59.

[128] M. Rahman, E. Al-Shaer, and R. Kavasseri, "A formal model for verifying the impact of stealthy attacks on optimal power flow in power grids," in *ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, April 2014, pp. 175–186.

[129] C. Phillips and L. P. Swiler, "A graph-based system for network-vulnerability analysis," in *Workshop on New Security Paradigms.* New York, NY, USA: ACM, 1998, pp. 71–79.

[130] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, “Automated generation and analysis of attack graphs,” in *IEEE Symposium on Security and Privacy*, May 2002, pp. 273–284.

[131] H. M. J. Almohri, L. T. Watson, D. Yao, and X. Ou, “Security optimization of dynamic networks with probabilistic graph modeling and linear programming,” *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 4, pp. 474–487, July 2016.

[132] S. M. Mitchell and M. S. Mannan, “Designing resilient engineered systems,” *Chemical Engineering Progress*, vol. 102, no. 4, pp. 39–45, 04 2006.

[133] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi, and J. Chen, “Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges,” *IEEE Communications Magazine*, vol. 56, no. 4, pp. 68–74, APRIL 2018.

[134] I. Guvenc, F. Koohifar, S. Singh, M. L. Sichitiu, and D. Matolak, “Detection, tracking, and interdiction for amateur drones,” *IEEE Communications Magazine*, vol. 56, no. 4, pp. 75–81, APRIL 2018.

[135] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, “Stealthy deception attacks on water scada systems,” in *Proceedings of the 13th ACM International Conference on Hybrid Systems: Computation and Control*, ser. HSCC ’10. New York, NY, USA: ACM, 2010, pp. 161–170.

[136] T. Alpcan and T. Başar, *Network security: a decision and game-theoretic approach*. New York: Cambridge University Press, 2011, pp. 98–129.

[137] Z. Liu, D. Yang, D. Wen, W. Zhang, and W. Mao, “Cyber-physical-social systems for command and control,” *IEEE Intelligent Systems*, vol. 26, no. 4, pp. 92–96, July 2011.

[138] C. Bergenhem, S. Shladover, E. Coelingh, C. Englund, and S. Tsugawa, “Overview of platooning systems,” in *Proceedings of the 19th ITS World Congress*, Oct 2012.

[139] H. Hu, R. Lu, Z. Zhang, and J. Shao, “Replace: A reliable trust-based platoon service recommendation scheme in vanet,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1786–1797, Feb 2017.

[140] B. Pal and B. Chaudhuri, *Robust control in power systems*, 1st ed. New York: Springer, 2005.

[141] A. R. Hota and S. Sundaram, “Interdependent security games on networks under behavioral probability weighting,” *IEEE Transactions on Control of Network Systems*, vol. 5, no. 1, pp. 262–273, March 2018.

[142] L. Xiao, C. Xie, M. Min, and W. Zhuang, “User-centric view of unmanned aerial vehicle transmission against smart attacks,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 4, pp. 3420–3430, April 2018.

[143] D. Xu, L. Xiao, N. B. Mandayam, and H. V. Poor, "Cumulative prospect theoretic study of a cloud storage defense game against advanced persistent threats," in *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, May 2017, pp. 541–546.

[144] B. Ford, T. Nguyen, M. Tambe, N. Sintov, and F. Delle Fave, "Beware the soothsayer: From attack prediction accuracy to predictive reliability in security games," in *International Conference on Decision and Game Theory for Security*. Springer, 2015, pp. 35–56.

[145] D. B. West, *Introduction to graph theory*, 2nd ed. Upper Saddle River, N.J: Prentice Hall, 2001.

[146] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*. Philadelphia, PA, USA: SIAM Series in Classics in Applied Mathematics, Jan. 1999.

[147] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjorungnes, *Game theory in wireless and communication networks: theory, models, and applications*. Cambridge University Press, 2012.

[148] D. Kahneman and A. Tversky, "Prospect theory: An analysis of decision under risk," *Econometrica*, vol. 47, no. 2, pp. 263–291, March 1979.

[149] A. Tversky and D. Kahneman, "Advances in prospect theory: Cumulative representation of uncertainty," *Journal of Risk and uncertainty*, vol. 5, no. 4, pp. 297–323, 1992.

[150] C. F. Camerer, T.-H. Ho, and J.-K. Chong, "A cognitive hierarchy model of games," *The Quarterly Journal of Economics*, vol. 119, no. 3, pp. 861–898, 2004.

[151] S. Ross and B. Chaib-draa, "Learning to play a satisfaction equilibrium." in *Workshop on Evolutionary Models of Collaboration*, 2007.

[152] ——, *Satisfaction Equilibrium: Achieving Cooperation in Incomplete Information Games*. Berlin, Heidelberg: Springer, 2006, vol. 4013, pp. 61–72.

[153] A. Rege, F. Ferrese, S. Biswas, and L. Bai, "Adversary dynamics and smart grid security: A multiagent system approach," in *7th International Symposium on Resilient Control Systems (ISRCS)*, Aug 2014, pp. 1–7.

[154] A. Mas-Colell, M. D. Whinston, and J. R. Green, *Microeconomic theory*. New York: Oxford University Press, 1995.

[155] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surv.*, vol. 45, no. 3, pp. 25:1–25:39, Jul. 2013.

[156] C. Ma, N. Rao, and D. Yau, "A game theoretic study of attack and defense in cyber-physical systems," in *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, April 2011, pp. 708–713.

[157] Z. Ismail, J. Leneutre, D. Bateman, and L. Chen, “A game-theoretical model for security risk management of interdependent ict and electrical infrastructures,” in *16th IEEE International Symposium on High Assurance Systems Engineering (HASE)*, Jan 2015, pp. 101–109.

[158] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Başar, “Dependable demand response management in the smart grid: A stackelberg game approach,” *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 120–132, March 2013.

[159] M. Jain, J. Pita, M. Tambe, F. Ordóñez, P. Paruchuri, and S. Kraus, “Bayesian stackelberg games and their application for security at los angeles international airport,” *SIGecom Exch.*, vol. 7, no. 2, pp. 10:1–10:3, Jun. 2008.

[160] S. Farhang, M. H. Manshaei, M. N. Esfahani, and Q. Zhu, “A dynamic bayesian security game framework for strategic defense mechanism design,” in *Decision and Game Theory for Security*. Springer, 2014, pp. 319–328.

[161] D. Kahneman, *Thinking, fast and slow*, 1st ed. New York: Farrar, Straus and Giroux, 2011.

[162] D. Prelec, “The probability weighting function,” *Econometrica*, vol. 66, no. 3, pp. 497–527, 1998.

[163] R. Gonzalez and G. Wu, “On the shape of the probability weighting function,” *Cognitive Psychology*, vol. 38, no. 1, pp. 129 – 166, 1999.

[164] W. Saad, A. L. Glass, N. B. Mandayam, and H. V. Poor, “Toward a consumer-centric grid: A behavioral perspective,” *Proceedings of the IEEE*, vol. 104, no. 4, pp. 865–882, April 2016.

[165] Y. Wang, W. Saad, N. B. Mandayam, and H. V. Poor, “Load shifting in the smart grid: To participate or not?” *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2604–2614, Nov 2016.

[166] T. Li and N. B. Mandayam, “When users interfere with protocols: Prospect theory in wireless networks using random access and data pricing as an example,” *IEEE Transactions on Wireless Communications*, vol. 13, no. 4, pp. 1888–1907, April 2014.

[167] J. Yu, M. H. Cheung, and J. Huang, “Spectrum investment under uncertainty: A behavioral economics perspective,” *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 10, pp. 2667–2677, Oct 2016.

[168] D. Xu, Y. Li, L. Xiao, N. B. Mandayam, and H. V. Poor, “Prospect theoretic study of cloud storage defense against advanced persistent threats,” in *IEEE Global Communications Conference (GLOBECOM)*, Dec 2016, pp. 1–6.

[169] L. Xiao, D. Xu, C. Xie, N. B. Mandayam, and H. V. Poor, “Cloud storage defense against advanced persistent threats: A prospect theoretic study,” *IEEE Journal on Selected Areas in Communications*, vol. PP, no. 99, pp. 1–1, 2017.

[170] L. Xiao, J. Liu, Q. Li, N. B. Mandayam, and H. V. Poor, "User-centric view of jamming games in cognitive radio networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2578–2590, Dec 2015.

[171] S. M. Perlaza, H. Tembine, S. Lasaulce, and M. Debbah, "Satisfaction equilibrium: A general framework for qos provisioning in self-configuring networks," in *IEEE Global Telecommunications Conference GLOBECOM*, Dec 2010, pp. 1–5.

[172] S. Perlaza, H. Tembine, S. Lasaulce, and M. Debbah, "Quality-of-service provisioning in decentralized networks: A satisfaction equilibrium approach," *IEEE Journal of Selected Topics in Signal Processing*, vol. 6, no. 2, pp. 104–116, April 2012.

[173] L. Rose, S. M. Perlaza, M. Debbah, and C. J. L. Martret, "Distributed power allocation with sinr constraints using trial and error learning," in *IEEE Wireless Communications and Networking Conference (WCNC)*, April 2012, pp. 1835–1840.

[174] A. Sanjab and W. Saad, "Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 2038–2049, July 2016.

[175] ——, "Smart grid data injection attacks: To defend or not?" in *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Nov 2015, pp. 380–385.

[176] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. New York: Marcel Dekker, 2004.

[177] J. B. A. London, L. F. C. Alberto, and N. G. Bretas, "Network observability: identification of the measurements redundancy level," in *Proc. International Conference on Power System Technology (PowerCon)*, vol. 2, 2000, pp. 577–582.

[178] K. C. Sou, H. Sandberg, and K. H. Johansson, "Computing critical k-tuples in power networks," *IEEE Transactions on Power Systems*, vol. 27, no. 3, pp. 1511–1520, Aug 2012.

[179] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *First Workshop on Secure Control Systems (SCS)*, 2010.

[180] K. C. Sou, H. Sandberg, and K. H. Johansson, "Electric power network security analysis via minimum cut relaxation," in *Proc. 50th IEEE Conference on Decision and Control and European Control Conference*, Dec 2011, pp. 4054–4059.

[181] J. M. Hendrickx, K. H. Johansson, R. M. Jungers, H. Sandberg, and K. C. Sou, "Efficient computations of a security index for false data attacks in power networks," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3194–3208, Dec 2014.

[182] J. London, A. Bretas, and N. Bretas, "Algorithms to solve qualitative problems in power system state estimation," *International Journal of Electrical Power and Energy Systems*, vol. 26, no. 8, pp. 583 – 592, 2004.

[183] E. Castillo, A. J. Conejo, R. E. Pruneda, C. Solares, and J. M. Menendez, "$m - k$ robust observability in state estimation," *IEEE Transactions on Power Systems*, vol. 23, no. 2, pp. 296–305, May 2008.

[184] K. C. Sou, H. Sandberg, and K. H. Johansson, "On the exact solution to a smart grid cyber-security analysis problem," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 856–865, June 2013.

[185] Y. Zhao, A. Goldsmith, and H. V. Poor, "Minimum sparsity of unobservable power network attacks," *IEEE Transactions on Automatic Control*, vol. 62, no. 7, pp. 3354–3368, July 2017.

[186] ——, "A polynomial-time method to find the sparsest unobservable attacks in power networks," in *Proc. American Control Conference (ACC)*, July 2016, pp. 276–282.

[187] G. R. Krumpholz, K. A. Clements, and P. W. Davis, "Power system observability: A practical algorithm using network topology," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-99, no. 4, pp. 1534–1542, July 1980.

[188] V. H. Quintana, A. Simoes-Costa, and A. Mandel, "Power system topological observability using a direct graph-theoretic approach," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-101, no. 3, pp. 617–626, March 1982.

[189] A. Bargiela, M. R. Irving, and M. J. H. Sterling, "Observability determination in power system state estimation using a network flow technique," *IEEE Transactions on Power Systems*, vol. 1, no. 2, pp. 108–112, May 1986.

[190] R. Zimmerman, C. Murillo-Sanchez, and R. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, Feb 2011.

[191] A. L. Ott, "Experience with pjm market operation, system design, and implementation," *IEEE Transactions on Power Systems*, vol. 18, no. 2, pp. 528–534, May 2003.

[192] F. Li, Y. Wei, and S. Adhikari, "Improving an unjustified common practice in ex post lmp calculation," *IEEE Transactions on Power Systems*, vol. 25, no. 2, pp. 1195–1197, May 2010.

[193] F. Miao, Q. Zhu, M. Pajic, and G. Pappas, "Coding sensor outputs for injection attacks detection," in *53rd IEEE Annual Conference on Decision and Control (CDC)*, 2014, pp. 5776–5781.

[194] A. Von Heusinger and C. Kanzow, "Relaxation methods for generalized nash equilibrium problems with inexact line search," *Journal of Optimization Theory and Applications*, vol. 143, no. 1, pp. 159–183, 2009.

[195] G. Debreu, "A social equilibrium existence theorem," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 38, no. 10, p. 886, 1952.

[196] F. Facchinei and C. Kanzow, "Generalized nash equilibrium problems," *4OR*, vol. 5, no. 3, pp. 173–210, 2007.

[197] A. von Heusinger and C. Kanzow, "Optimization reformulations of the generalized nash equilibrium problem using nikaido-isoda-type functions," *Computational Optimization and Applications*, vol. 43, no. 3, pp. 353–377, 2009.

[198] K. S. Narendra and M. A. L. Thathachar, *Learning automata: an introduction*. Englewood Cliffs, N.J: Prentice Hall, 1989.

[199] P. Sastry, V. Phansalkar, and M. Thathachar, "Decentralized learning of nash equilibria in multi-person stochastic games with incomplete information," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 24, no. 5, pp. 769–777, May 1994.

[200] O. Alsac and B. Stott, "Optimal load flow with steady-state security," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-93, no. 3, pp. 745–751, May 1974.

[201] R. Ferrero, S. Shahidehpour, and V. Ramesh, "Transaction analysis in deregulated power systems using game theory," *IEEE Transactions on Power Systems*, vol. 12, no. 3, pp. 1340–1347, Aug 1997.

[202] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Unmanned aerial vehicle with underlaid device-to-device communications: Performance and tradeoffs," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 3949–3963, June 2016.

[203] M. Asadpour, B. V. den Bergh, D. Giustiniano, K. A. Hummel, S. Pollin, and B. Plattner, "Micro aerial vehicle networks: an experimental analysis of challenges and opportunities," *IEEE Communications Magazine*, vol. 52, no. 7, pp. 141–149, July 2014.

[204] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Mobile unmanned aerial vehicles (uavs) for energy-efficient internet of things communications," *IEEE Transactions on Wireless Communications*, vol. 16, no. 11, pp. 7574–7589, Nov 2017.

[205] S. Choi, N. Sung, J. Park, I. Ahn, and J. Kim, "Enabling drone as a service: One m2m-based uav/drone management system," in *International Conference on Ubiquitous and Future Networks (ICUFN)*, July 2017, pp. 18–20.

[206] M. McFarland, "Google drones will deliver chipotle burritos at Virginia Tech," *CNN Money*, September 2016.

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

[208] I. Bucaille, S. HÃ©thuin, A. Munari, R. Hermenier, T. Rasheed, and S. Allsopp, "Rapidly deployable network for tactical applications: Aerial base station with opportunistic links for unattended and temporary events absolute example," in *IEEE Military Communications Conference (MILCOM)*, Nov 2013, pp. 1116–1120.

[209] R. Pahonie, R. Mihai, and C. Barbu, "Biomechanics of flexible wing drones usable for emergency medical transport operations," in *E-Health and Bioengineering Conference (EHB)*, Nov 2015, pp. 1–4.

[210] G. Xiang, A. Hardy, M. Rajeh, and L. Venuthurupalli, "Design of the life-ring drone delivery system for rip current rescue," in *IEEE Systems and Information Engineering Design Symposium (SIEDS)*, April 2016, pp. 181–186.

[211] V. Gatteschi, F. Lamberti, G. Paravati, A. Sanna, C. Demartini, A. Lisanti, and G. Venezia, "New frontiers of delivery services using drones: A prototype system exploiting a quadcopter for autonomous drug shipments," in *39th IEEE Annual Computer Software and Applications Conference (COMPSAC)*, vol. 2, July 2015, pp. 920–927.

[212] Amazon, "Amazon prime air," 2016. [Online]. Available: https://www.amazon.com/b?node=8037720011

[213] P. M. Kornatowski, A. Bhaskaran, G. M. Heitz, S. Mintchev, and D. Floreano, "Last-centimeter personal drone delivery: Field deployment and user interaction," *IEEE Robotics and Automation Letters*, vol. 3, no. 4, pp. 3813–3820, Oct 2018.

[214] N. Peinecke and A. Kuenz, "Deconflicting the urban drone airspace," in *IEEE/AIAA Digital Avionics Systems Conference (DASC)*, Sept 2017, pp. 1–6.

[215] J. Lee, "Optimization of a modular drone delivery system," in *Annual IEEE International Systems Conference (SysCon)*, April 2017, pp. 1–8.

[216] T. Asma, S. Addouche, S. Dellagi, and A. E. Mhamedi, "Post-production analysis approach for drone delivery fleet," in *IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, Sept 2017, pp. 150–155.

[217] K. Dorling, J. Heinrichs, G. G. Messier, and S. Magierowski, "Vehicle routing problems for drone delivery," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 47, no. 1, pp. 70–85, Jan 2017.

[218] K. Mansfield, T. Eveleigh, T. H. Holzer, and S. Sarkani, "Unmanned aerial vehicle smart device ground control station cyber security threat model," in *IEEE International Conference on Technologies for Homeland Security (HST)*, Nov 2013, pp. 722–728.

[219] J. Su, J. He, P. Cheng, and J. Chen, "A stealthy gps spoofing strategy for manipulating the trajectory of an unmanned aerial vehicle," *IFAC-PapersOnLine*, vol. 49, no. 22, pp. 291 – 296, 2016.

[220] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via gps spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[221] M. L. Puterman, *Markov decision processes: discrete stochastic dynamic programming*. John Wiley & Sons, 2008.

[222] C. Audet and J. E. Dennis Jr., "Analysis of generalized pattern searches." *SIAM Journal on Optimization*, vol. 13, no. 3, p. 889, 2002.

[223] O. Yagan, D. Qian, J. Zhang, and D. Cochran, "Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1708–1720, Sept 2012.

[224] C. F. Camerer, T.-H. Ho, and J.-K. Chong, "A cognitive hierarchy model of games," *The Quarterly Journal of Economics*, pp. 861–898, 2004.

[225] F. Li and R. Bo, "Small test systems for power system economic studies," in *IEEE Power and Energy Society General Meeting*, July 2010, pp. 1–4.

[226] S. H. Horowitz and A. G. Phadke, *Power system relaying*, 4th ed. Chichester, West Sussex: John Wiley Sons Inc, 2014.

[227] P. F. Schewe, *The grid: a journey through the heart of our electrified world*. Washington, D.C: J. Henry Press, 2007.

[228] H. Dommel and W. Tinney, "Optimal power flow solutions," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-87, no. 10, pp. 1866–1876, Oct 1968.

[229] B. Stott and O. Alsaç, "Optimal power flow–basic requirements for real-life problems and their solutions," in *SEPOPE XII Symposium, Rio de Janeiro, Brazil*, 2012.

[230] H. Farhangi, "The path of the smart grid," *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, January-February 2010.

[231] I. Atzeni, L. G. Ordonez, G. Scutari, D. P. Palomar, and J. R. Fonollosa, "Demand-side management via distributed energy generation and storage optimization," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 866–876, June 2013.

[232] ——, "Noncooperative and cooperative optimization of distributed energy generation and storage in the demand-side of the smart grid," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2454–2472, February 2013.

[233] C. Wu, H. Mohsenian-Rad, and J. Huang, "Wind power integration via aggregator-consumer coordination: A game theoretic approach," in *Proc. IEEE PES Innovative Smart Grid Technologies (ISGT)*, Washington, DC, USA, January 2012, pp. 1–6.

[234] R. Arghandeh, M. Brown, A. Del Rosso, G. Ghatikar, E. Stewart, A. Vojdani, and A. von Meier, "The local team: leveraging distributed resources to improve resilience," *IEEE Power and Energy Magazine*, vol. 12, no. 5, pp. 76–83, September-October 2014.

[235] M. McGranaghan, M. Olearczyk, and C. Gellings, "Enhancing distribution resiliency-opportunities for applying innovative technologies," *white paper - Electric Power Research Institute*, January 2013.

[236] U.S. Department of Energy, "The potential benefits of distributed generation and rate-related issues that may impede their expansion: A study pursuant to section 1817 of the energy policy act of 2005," *USDOE, (Ed.)*, February 2007.

[237] G. Venkataramanan and M. Illindala, "Microgrids and sensitive loads," in *Proc. IEEE Power Engineering Society Winter Meeting*, vol. 1, New York, NY, USA, January 2002, pp. 315–322.

[238] E. Aeloiza, P. Enjeti, L. Moran, and I. Pitel, "Next generation distribution transformer: to address power quality for critical loads," in *Proc. IEEE 34th Annual Power Electronics Specialist Conference*, vol. 3, Acapulco, Mexico, June 2003, pp. 1266–1271.