Fakultät für Informatik und Mathematik

Universität Passau, Germany

Threat Assessment for Multistage Cyber Attacks in Smart Grid Communication Networks

Xiaobing He

Supervisors: Hermann de Meer

Stefan Rass

A thesis submitted for

Doctoral Degree

July 2017

1. Reviewer: Prof. Hermann de Meer
   Computer Networks and Communications
   University of Passau
   Innstr. 43
   94032 Passau, Germany
   Email: demeer@uni-passau.de
   Web: http://www.net.fim.uni-passau.de

2. Reviewer: Assoc. Prof. Stefan Rass
   System Security Group
   University of Klagenfurt
   Universitätsstr. 65-67
   A9020, Klagenfurt, Austria
   Email: Stefan.Rass@aau.at
   Web: https://www.aau.at

3. Reviewer: Prof. Felix Freiling
   IT Security Infrastructures
   University of Erlangen-Nuremberg
   Martensstr. 3
   91058, Erlangen, Germany
   Email: felix.freiling@cs.fau.de
   Web: https://www1.informatik.uni-erlangen.de

Abstract

In smart grids, managing and controlling power operations are supported by information and communication technology (ICT) and supervisory control and data acquisition (SCADA) systems. The increasing adoption of new ICT assets in smart grids is making smart grids vulnerable to cyber threats, as well as raising numerous concerns about the adequacy of current security approaches.

As a single act of penetration is often not sufficient for an attacker to achieve his/her goal, multistage cyber attacks may occur. Due to the interdependence between the power grid and the communication network, a multistage cyber attack not only affects the cyber system but impacts the physical system. This thesis investigates an application-oriented stochastic game-theoretic cyber threat assessment framework, which is strongly related to the information security risk management process as standardized in ISO/IEC 27005. The proposed cyber threat assessment framework seeks to address the specific challenges (e.g., dynamic changing attack scenarios and understanding cascading effects) when performing threat assessments for multistage cyber attacks in smart grid communication networks.

The thesis looks at the stochastic and dynamic nature of multistage cyber attacks in smart grid use cases and develops a stochastic game-theoretic model to capture the interactions of the attacker and the defender in multistage attack scenarios. To provide a flexible and practical payoff formulation for the designed stochastic game-theoretic model, this thesis presents a mathematical analysis of cascading failure propagation (including both interdependency cascading failure propagation and node overloading cascading failure propagation) in smart grids. In addition, the thesis quantifies the characterizations of disruptive effects of cyber attacks on physical power grids.

Furthermore, this thesis discusses, in detail, the ingredients of the developed stochastic game-theoretic model and presents the implementation steps of the investigated

stochastic game-theoretic cyber threat assessment framework. An application of the proposed cyber threat assessment framework for evaluating a demonstrated multistage cyber attack scenario in smart grids is shown. The cyber threat assessment framework can be integrated into an existing risk management process, such as ISO 27000, or applied as a standalone threat assessment process in smart grid use cases.

Acknowledgements

At the end of this work, I would like to express my sincere thanks to many people who have contributed to the fulfilment of my thesis.

First of all, I would like to express my gratitude to my primary supervisor Professor Hermann de Meer for providing support during my time as a graduate student, investing countless hours into my professional development, and providing me with opportunities to collaborate with a wide range of international partners in interesting and manifold research projects. As a representative example, I would like to mention the European Commission's project HyRiM (Hybrid Risk Management for Utility Networks) here.

Furthermore, I would like to express my extreme appreciation to my secondary supervisor Associate Professor Stefan Rass. His contributions, encouragement and insightful feedback have been invaluable to me during the work. I would never have been able to finish this thesis without his and Prof. de Meer 's support. I also want to cordially thank Professor Felix Freiling for kindly agreeing to serve as a third reviewer.

I would like to acknowledge my parents in deep for their enduring support. I need to address thanks to my husband for invaluable scientific suggestions and continual encouragement. I want to thank my beloved son for bringing so much happiness to my graduate career. I also want to express my gratefulness to the family of Weishäupl for taking care of my son when I was writing this thesis.

I am extremely grateful to the European Union-funded project SPARKS (Smart Grid Protection Against Cyber Attacks) for providing the travel grant to attend the 4th International Symposium for ICS & SCADA Cyber Security Research 2016 in Belfast, UK. I would also like to thank Dr. Paul Smith and Mislav Findrik from AIT Austrian Institute of Technology GmbH for their helpfulness and discussions regarding the formulating of the topic covered in this thesis.

I appreciate the present and former PhD students and postdocs at the chair of computer networks and computer communications for contributing to the open and friendly work atmosphere. I would like to address my special thanks to the administrative and technical staff of the University of Passau.

Last, but not least, I am grateful to the China Scholarship Council (CSC) for the doctoral research funding in Germany. Meanwhile, I would also like to thank EuroNF (Network of excellence) for the support to attend the PhD course of main trends in teletraffic and economic modelling.

Contents

List of Figures

LIST OF FIGURES

List of Tables

Chapter 1

Introduction

"*Security is a process, not a product*"

— Bruce Schneier

The power grid has increasingly relied on information and communication infrastructure for monitoring and controlling grid operations, leading to the gradual evolution of a new concept of power grids, namely, smart grids. From a broad perspective, the smart grid is the term used to refer to an upgraded electricity network, in which information and communication technology (ICT) infrastructure is provided to enable the integration of renewable energy resources/electric vehicles and allow for monitoring and controlling physical power grids. In other words, the smart grid is a cyber-physical system, where the power system, primarily, medium- and low-voltage networks, are supported by ICT and supervisory control and data acquisition (SCADA) systems. Figure 1.1 shows typical smart grid architecture with both physical and cyber systems. In such a complex cyber-physical smart grid, the resources are coordinated by control centres, which can be considered as the brain of the smart grid. These control centres are interconnected by bidirectional cyber system infrastructure comprising software, hardware and communication network [3], as illustrated in Figure 1.1.

1.1 Background

The introduction of new ICT infrastructure in the physical power grid is making the cyber-physical systems more vulnerable to cyber threats that can degrade the performance of physical systems. Moreover, a failure in the cyber-physical architecture of smart grids can result in a cascading effect of failures. As identified by the CEN-CENELEC-ETSI (the three European

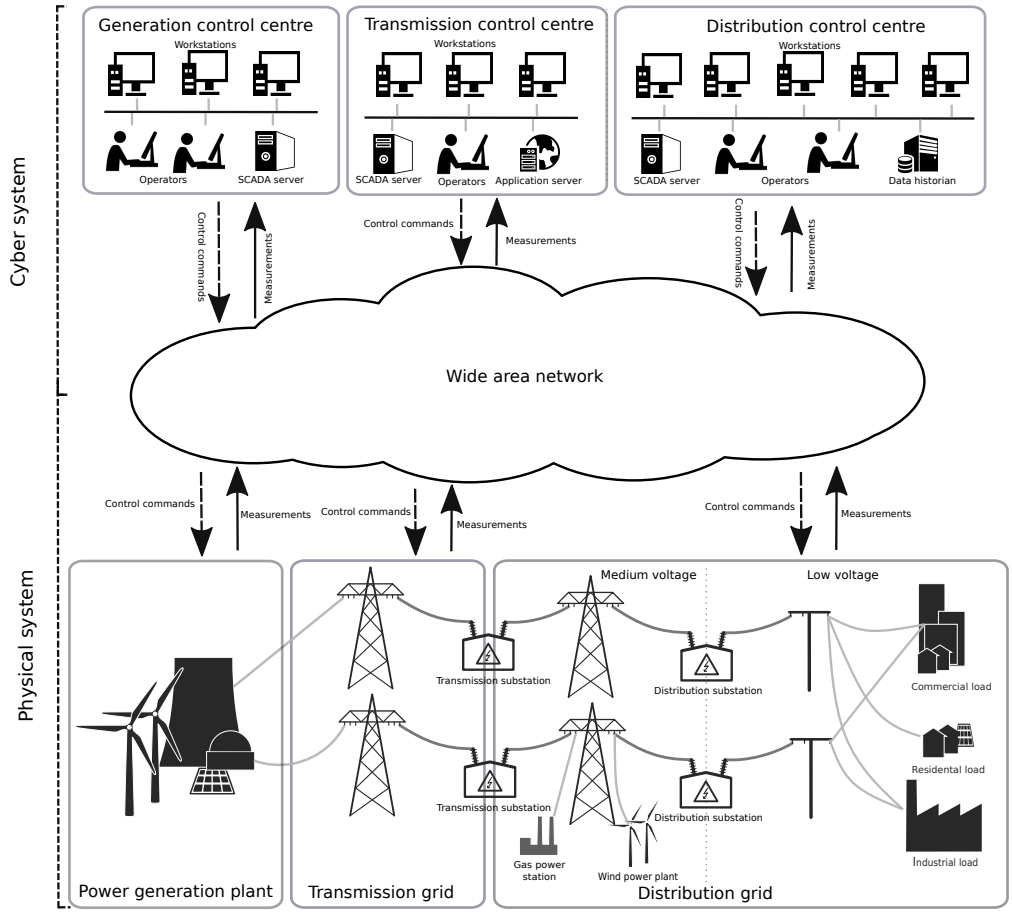


Figure 1.1: A typical cyber-physical structure of the smart grid.

standardization organizations), a cyber attack to the smart grid can lead to serious implications for quality of supply, safety-related incidents, and a catastrophic impact on the economy.

Traditional IT security approaches (e.g., firewalls, cryptographic primitives) are either inapplicable, insufficiently scalable, incompatible or inadequate to secure cyber-physical systems, as safety aspects and functional interdependencies of cyber-physical systems are often often considered. Recent events have shown that cyber attacks on industrial control systems are becoming increasingly sophisticated. Cyber attacks with the ability to compromise physical equipment are considered as the most trivial forms of attacks on any cyber-physical system [4]. Disabling or tampering with physical equipments can easily render them unavailable at critical times of operations, while operational reliability is of the utmost importance in smart grids. Threats are evolving over time, while cybercriminals are becoming smarter and smarter, less so

their victims. Cyber attacks in the past were generally one-dimensional and mainly in the form of denial of service (DoS) attacks, computer viruses or worms, or Trojan horses. However, this has fundamentally changed in recent times. Cyber threats are undergoing a diversification that is resulting in the combination of the "Internet", "teamwork" and "commercial interests", while appearing in multiple forms [5, 6]. BlackEnergy malware is one example of such threats, which has evolved over time from a simple distributed denial of service (DDoS) platform to rather sophisticated plug-in based malware [7]. Moreover, BlackEnergy has been used in numerous targeted attacks [8, 9] since its discovery in 2007.

By exploiting vulnerabilities, an attacker can infect systems with malware, propagate malware within the system (or even between different systems) and use additional attack methods to achieve his/her ultimate goal. In this regard, as a single act of penetration is often not sufficient, this leads to a situation involving multistage attacks, which are composed of a number of dynamically interrelated attack steps, where the occurrence of the next step depends on the successful completion of the previous step. The Stuxnet cyber attack on the Iranian nuclear programme is the best-known example of a multistage attack on physical infrastructure [10]. Stuxnet infected approximately 100,000 hosts across over 155 countries prior to September, 2010, according to the Symantec report [11]. More recent, widely known multistage cyber attack scenarios include the German steel mill breach in December 2014 [12] and the Ukrainian electric power disruption in December 2015, which will be briefly described in the following paragraphs.

1.1.1 German Steel Mill Breach

In December 2014, the German Government's Bundersamt für Sicherheit in der Informationstechnik (BSI) (translated as the Federal Office for Information Security) issued a report about a cyber attack on a steel mill that resulted in significant damage to the facility. The attack has received extensive publicity (from the BBC to YouTube) since then, while the technical details of the attack have been released by SANS [13].

The BSI report stated that adversaries targeted industrial operators with spear phishing emails, which was observed in the HAVEX (targeting OPC communications) [1] and BlackEnergy Version 2 [2] (targeting human-machine interface (HMI) products) malware threats. The attacker, described as an advanced persistent threat (APT) attacker, followed a pattern that is

[1] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A (Retrieved:19/06/2017)

[2] https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf (Retrieved:19/06/2017)

described as a "cyber kill chain" [14] to target the facility. At the first stage, the attacker sent out phishing emails to industrial operators and made use of social engineering techniques to gain access to the network. Those emails, which were attached with malicious documents (such as PDFs), once opened, executed malicious code that targeted an application vulnerability in the facility's corporate network. The attacker worked his/her way to the production network, i.e., industrial control system (ICS)). Owing to the connection between the corporate network and the production network, the exploitation of a vulnerability in the corporate network opened a remote connection point, allowing the attacker access to the production network. The second stage of the attack was the compromise of small sets of workstations. Once workstations were totally in his/her control, the attacker moved into the plant network. Then, the attacker destroyed a blast furnace in the plant network by initiating its security settings in time, causing serious damage to the infrastructure. It took months to replace damaged equipment due to the need to remove and replace large pieces of machinery.

1.1.2 Ukrainian Electric Disruption

On 24, December 2015, TSN (a Ukrainian news outlet) released a report about power outages caused by a cyber attack [1]. Numerous reporting agencies and independent bloggers, including the Washington Post, SANS Institute, New York Times, the BBC, CNN, Fox News, as well as the E-ISAC, had followed up on the initial TSN report and provided further details of that cyber attack, which was targeted at the Ukrainian electric system. The power outage caused by the cyber attack affected roughly 225,000 customers for over six hours during a spell of cold whether [2].

Those outages were due to a combination of BlackEnergy Version 3, unreported backdoors, KillDisk, and malicious firmware uploads within the utility's systems. It was shown that the vulnerabilities in the utility (e.g., a lack of two-factor authentication, no resident capability to continually monitor the ICS network) had provided the adversary with the opportunity to persist within the environment for at least six months in order to conduct extensive reconnaissance and subsequently execute the attack [3]. The attacks was conducted in three sophisticated, well-planned stages, as shown in Figure 1.2. During the cyber attack, spear phishing emails

[1] http://ru.tsn.ua/ukrayina/iz-za-hakerskoy-ataki-obestochilo-polovinu-ivano-frankovskoy-oblasti-550406.html (Retrieved:19/06/2017)

[2] http://money.cnn.com/2016/01/18/technology/ukraine-hack-russia/ (Retrieved:19/06/2017)

[3] http://mobile.reuters.com/article/idUSKCN0VL18E (Retrieved:19/06/2017)

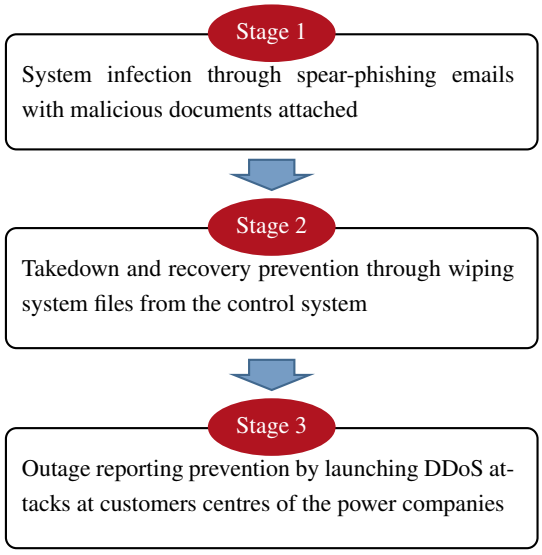


Figure 1.2: Ukraine cyber attacks with three stages.

were sent out to gain access to the business networks of the three regional electric power distribution companies. The remote malicious opening of breakers in a number of substations was conducted by using either existing remote administration tools at the operating system level or remote ICS client software via virtual private network (VPN) connections. Modified KillDisk malware was used to erase selected files on targeted systems and corrupt the master boot record. The adversary also caused serial-to-Ethernet devices (located at substations) to malfunction at a firmware level. Moreover, the attacker also leveraged a remote telephonic denial of service on the energy company's call centre to ensure that the affected customers could not report outages and force the oblenergoes to move to a manual operation system in response to the attacks.

1.2 Interdependent Electric Power and Communication Systems

It can be seen that, due to the interdependency in cyber-physical systems, a cyber attack not only affects the cyber network, but also impacts on the physical network. The same also holds for smart grids, where the communication system and the electric power grid are highly coupled. Throughout this thesis, the communication system refers to the telecommunication infrastructures that are responsible for monitoring (e.g., with sensors) and controlling (e.g., with actuators) the electric power system. In this thesis, the term "electric power system" refers to

medium- to low-voltage power grids (i.e., power distribution grids).

Historically, a power distribution grid had less automation than a generation plant or a transmission power grid, while almost all communications within the distribution grid were performed manually [15]. It was unlikely for distribution substations to be connected to a central SCADA system. Hence, load energy consumption and abnormal event data were collected by humans, while manual equipment switching was required at electrical substations. However, with the arrival of smart grids, the distribution grids are shifting to meet distributed systems operators (DSOs)' requirements on automation, monitoring, control and protection of distribution substations and transformer stations/centres. Thus, the dependency of power distribution grids on communication networks are extended by integrating additional communication and control capabilities. The communication infrastructure supporting power distribution operations and distributed energy resources (DERs)/microgrids includes neighbourhood area networks (NANs), field area networks (FANs), advanced metering infrastructures (AMIs), local area networks (LANs) and feeder network, depending on the devices it connects and the applications supported. A distribution substation network, which comprises LANs, provides connectivity to the wide area networks (WANs), either directly or through FANs. The FANs will in turn interconnect several distribution substations before accessing the WANs. Therefore, in smart grids, the communication network provides monitoring and control information to ensure normal operation of the power grid, which supplies electricity to ensure normal operations of the communication network.

1.3 Threat Assessment for Multi-stage Cyber Attacks

There is no universal or standard understanding of the concept of threat. The International Standards Organization (ISO) [16], the National Institute of Standards and Technology (NIST) in the US [17] and European Union Agency for Network and Information Security (ENISA) [18] have their own definitions of a threat. According to American National Standards Institute (ANSI), threats can be defined as "possible actions that can be taken against a system" [19]. These actions may aim to cause harm in the form of death, injury, destruction, disclosure, modification of information and/or denial of services. This thesis uses the ANSI definition, which limits threats to possible actions that can be taken. However, other definitions of a threat are also taken as supplementaries to support ANSI's threat definition.

Cyber attacks typically consist of multiple stages: reconnaissance of the configuration and vulnerabilities in the targeted system, followed by malware injection and some form of intrusion/or privilege escalation, and ending with implanting malicious software or stealing critical information. Characterizing cyber security threats to smart grids is a difficult task, since there are relatively few statistical measures of security breaches. A smart grid is quite a new concept and, as a result, there is little practical experience of cyber attacks affecting this kind of infrastructure (Section 1.1 lists two of them, but still the statistical data are limited). Besides, ICS and industrial cyber security are also fairly new topics, with security experts still learning about these topics, developing hacking tools and finding new vulnerabilities [20]. There are copious amounts of statistical data about physical security and safety (e.g., natural disasters); however, cyber threats depend on underlying system's exploitable vulnerabilities ans security resources, as well as the attackers' motivations and capabilities. As a result, utilities are relatively inexperienced with regard to cyber attacks. Additionally, The cyber threat landscape is fast-growing and continuously evolving. As a large distributed and interconnected system, with an ever-growing number of security assets (e.g., home gateways, smart meters, substations), the smart grid is a potential target for a cyber attack. More seriously, a cyber attack can impact on the physical power grid and lead to a cascade effect resulting in blackouts. Since the smart grid is a combination of power systems and IT communication systems, cybesecurity in this context needs to address vulnerabilities in technologies to mitigate threats [21]. Software and malware vulnerabilities may be exploited to allow the attacker remote access to unprotected security assets. Threats can come not only from running unnecessary and easily exploitable software, but also from failing to enable installed security countermeasures (e.g., intrusion detection systems).

Threat assessment is *a process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, which have or indicate the potential to harm life, information, operations and/or property* [1]. Though formal and succinct, this definition offers little insight into what and how a threat assessment may be performed for cyber attacks. Intuitively, assessing threats means predicting potential actions and estimating the impact of a potential threat, once it has been identified. Thus, by predicting attackers' behaviour, a cyber threat assessment helps the system administrator to better understand the effectiveness of the current network security solution and determine the best approaches to secure the system against a particular threat, or a class of threats. By offering a deep analysis of existing or potential threats, system

[1] http://niccs.us-cert.gov/glossary (Retrieved:19/06/2017)

administrators are given a clear assessment of the risks to their systems, while possessing a clear vision about the kind of security countermeasures that the respective utility should invest in. Traditional practices to defend against cyber attacks are typically reactive yet passive, with log file analysis being one typical example of such practices. Recent research work has been carried out to proactively and preventively predict attackers' behaviours and actions at an early stage of the attack. Threat assessment for multistage cyber attacks is not straightforward, given that, at any stage of a cyber attack, the attacker may decide not to proceed or change his/her attack actions. Since the attacker has motivations (costs versus benefits) and has finite resources to launch a further attack at any stage, the stage in which the multistage attack stops is not necessary predetermined (stochastic). This thesis accounts for this by adding a stopping time to the stochastic model. It is to be noted that an attacker who doesnot have any resource limitations (from an economic point of view) is beyond the scope of this thesis. The stop of the attack or the change of attack actions at any stage makes a threat assessment extremely challenging, as it is difficult to know what the attacker will do or to assess possible cyber or physical impacts resulting from his/her attack actions in the next stage.

1.4 Problem Statements and Research Objectives

Regarding performing threat assessment for multistage cyber attacks in smart grid communication networks, the specific challenges include dynamically changing attack scenarios (even in one attack scenario, the action strategy can change from one step to another), managing security and safety risks, and understanding cascading effects. To address these challenges, there have been significant efforts in terms of smart grid cyber threat and risk assessment standards, cyber threat and risk assessment solutions from diverse European projects, and cyber threat and assessment approaches from worldwide research communities (see Chapter 2). However, some related challenging challenges remain unexplored, including the following:

- It is usually quite difficult for practitioners (such as DSOs and solution providers) to carry out a proper threat assessment in smart grids, as they have not provided enough details about quantitative model-based threat assessments.
- Concerning the development of a cyber threat assessment, the proposed techniques do not adequately address the additional constraints (e.g., a mix of legacy and new systems) required to support a cyber threat assessment in smart grids.

- When implementing a threat assessment in smart grids, the quantification of the physical impact of a cyber attack is not sufficiently explored.
- The majority of the proposed game-theoretic threat and risk assessment models (some of which will be discussed in Chapter 2) have not taken dynamic attack strategy changes and step dependencies of multistage cyber attacks into account.

This thesis proposes a *stochastic game-theoretic cyber threat assessment framework* to address the above-listed challenges. It focuses on the problem of an *application-oriented threat assessment for multistage cyber attacks in smart grid communication networks*. The objectives of this research are:

- To develop an application-oriented cyber threat assessment framework in order to address the risk posed by multistage cyber attacks in smart grids
- To quantify characterizations of disruptive events resulting from cyber attacks
- To contribute towards safety improvements for relevant stakeholders (e.g., policymakers, regulatory agencies, smart grid equipment manufacturers and utility companies) in power distribution grids
- To make recommendations about allocating security resources to reduce cyber security incidents or even safety-related events

The main goal of this work is to check the effectiveness of current network security solutions against a class of threats, as well as making recommendations for appropriate optimal security countermeasures in smart grids. Apart from the main goal, this thesis provides help in carrying out the above-mentioned tasks. Firstly, the threat assessment capabilities for multistage cyber attacks in smart grid communication networks are enhanced. The proposed cyber threat assessment framework is based on a stochastic game-theoretic model, which enables us to capture the fundamental characteristics (e.g., information asymmetry, which has the meaning that decision makers have different kinds of asymmetric information) of adversarial interactions between decision makers in smart grid communication networks. Secondly, a new approach to quantifying the characterizations of the physical impact of cyber attacks on physical power grids is suggested. Finally, the application and implementation of game theory in the threat assessment for multistage cyber attacks in smart grid communication networks are advanced.

1.5 Main Contributions

This work suggests an easy-to-follow threat assessment framework for smart grid practitioners (e.g., DSOs and solution providers). The work proposes new methods relating to the characteristics and physical features of smart grid communication networks. The main contributions of this thesis are summarized as follows:

1. This thesis combines the research fields of threat and risk assessment, game theory and percolation-like cascading failure propagation analysis. State-of-the-art smart grid threat and risk assessment methods and frameworks and cascading failure propagation approaches are investigated. Furthermore, the difficulty of developing easy-to-follow cyber threat assessments for multistage attacks in smart grid use cases and the difficulty for practitioners to set up major existing threat and risk assessment methods and frameworks are also discussed.

2. This thesis proposes an application-oriented stochastic game-theoretic cyber threat assessment framework, which is closely related to the information security risk management process standardized in ISO/IEC 27005 (a summary of the ISO/IEC 27005 information security risk management standard can be found in Appendix D). The cyber threat assessment framework is tailored to address the specific challenges of performing threat assessments for multistage cyber attacks in smart grid communication networks. This thesis presents the implementation steps of the proposed cyber threat assessment framework. The cyber threat assessment framework can be integrated into existing risk management processes, which are already running in a set of smart grid use cases, or can be applied as a standalone threat assessment process in architectural concepts of smart grid use cases.

3. This thesis designs a *stochastic game-theoretic model* as a cyber threat assessment framework. The designed stochastic game-theoretic model can be used to optimize security countermeasures for the defender to defend against multistage cyber attacks. The model captures the key characteristics (e.g., information asymmetry) of the interactions between the attacker and the defender in smart grid communication networks. Information asymmetry means that both the attacker and the defender lack full knowledge of the current system state. Consequently, they both maintain a belief (i.e., a probability distribu-

tion) about the current system state, with such a belief changing along with the ongoing interplay between the attacker and the defender, in a way that needs to be considered.

4. This thesis provides a common belief-updating mechanism for the attacker and the defender in the designed stochastic game-theoretic model so as to refresh their belief about the current system state. The common belief held by the attacker and the defender is dependent on the actions previously taken by them, while the belief value allows them to coordinate their action decisions in each game stage and efficiently control the dynamic networked systems.

5. In order to provide payoffs for the designed stochastic game-theoretic model, a cost and reward analysis is conducted. To quantify the characterizations of the disruptive effects of cyber attacks on physical power grids, this thesis presents a detailed mathematical analysis of the cascading failure propagation in an interdependent power and communication network model. The cascading failures considered in this thesis include both interdependency cascading failures and node overloading cascading failures. The addressed aspects of the proposed theoretical model of interdependent power and communication networks can be briefly summarized as follows:

   - An *interdependence relation allocation* for interdependent power and communication networks. These functional interdependencies between power and communication networks are directional and asymmetric. In addition, physical features (e.g., geographic criteria) of smart grids with heterogeneity are taken into account.
   - A *load redistribution rule* to *non-uniformly* redistribute loads of a failed distribution node among its upstream distribution nodes in the power grid.
   - A *cyber disruption metric* to quantify the characterizations (i.e., scope, magnitude, and time distribution) of the physical impact of cyber attacks on the physical power grid.

6. This thesis captures the spatio-temporal characteristics of cascading failure propagation from the joint effect of interdependency and node overloading cascading failures.

7. Finally, this thesis implements all models, based on suitable software tools. The proposed stochastic game-theoretic cyber threat assessment framework is applied in order to evaluate a demonstration multistage cyber attack scenario in smart grids.

1.6 Thesis Structure

The remainder of this thesis is structured as follows:

- Chapter 2 reviews previous work related to the approach suggested in this thesis. Firstly, an overview of current standardization progress on smart grid cyber threat and risk assessment at international and/or national levels is provided. Then, the most recent European projects that already provided or are trying to provide threat and risk assessment solutions for cyber attacks are discussed, cascading failure propagation approaches related to this thesis are presented, and threat assessment approaches from the worldwide research community are identified. Finally, it discusses the difficulty in performing cyber threat assessment faced by practitioners and the difficulty of developing an easy-to-follow cyber threat assessment for multistage cyber attacks.

- Chapter 3 discusses the possibilities of applying game theory for network cyber security assessments. It presents the preliminaries of game theory, including selective concepts and relevant terms. It also provides an overview of the proposed stochastic game-theoretic cyber threat assessment framework, which draws inspiration from the ISO/IEC 27005 information security risk management standard and is tailored to address the specific challenges of performing threat assessments for multistage cyber attacks. Furthermore, it presents the implementation steps of the proposed stochastic game-theoretic cyber threat assessment framework.

- Chapter 4 investigates the design of a stochastic game-theoretic model, which is the core part of the proposed stochastic game-theoretic cyber threat assessment framework presented in Chapter 3. It first describes the general stages involved in a multistage cyber attack on smart grids, then discusses the design of a stochastic game-theoretic model according to the characteristics of the interactions of the attacker and the defender in smart grid communication networks. The elements of the designed stochastic game-stochastic model are elaborated in detail. Due to the information asymmetry between the two decision makers in the stochastic game model, either decision maker knows the exact current system state. Therefore, a belief-updating mechanism is proposed for both decision makers to form a common belief about the current system state. It further discusses the computation of Nash equilibria for the designed stochastic game-theoretic model.

- Chapter 5 analyses the cost and reward of players' actions in the smart grid in order to provide a payoff formulation for the designed stochastic game-theoretic model. The reward of an action from the attacker includes disruption events caused by a cyber attack on the physical power grid. Therefore, the cascading effect of a cyber attack is investigated. The interdependent power and communication networks are modelled as fully directed networks, where the directions represent the directions of information flow in the communication network or the directions of power flow in the power network. The interdependence for power and communication networks are directional and asymmetric, while the physical features of smart grids are considered in allocating interdependence relations. It presents a mathematical analysis of the cascading failure propagation, where cascading effects are joint effects of interdependency and node overloading failures. A load redistribution rule is proposed in order to non-uniformly redistribute loads of a failed distribution node among its upstream functional distribution nodes in the power grid. In order to provide quantitative reward analysis of players' actions, a cyber disruption metric is defined to quantify the characterizations (i.e., scope, magnitude, and time) of the physical impact of cyber attacks on physical power grids. Meanwhile, an information impact metric is defined to measure the impact of the attacker's action on the network information security impairment of the communication nodes. The entire interdependency cascading failure propagation and load redistribution process are implemented and the simulation results are analysed.

- Chapter 6 applies the proposed stochastic game-theoretic cyber threat assessment framework in order to evaluate a demonstration multistage cyber attack scenario in a smart grid use case. It elaborates a game set-up (including game stages and states) in relation to the demonstrated attack scenario, instantiates the defined cyber disruption metric and the information impact metric, and implements the game between the attacker and the defender for the demonstration multistage cyber attack. It explains the practical meanings of the game equilibrium for each type of assets in the smart grid. Furthermore, it discusses the difficulties in evaluating/comparing cyber threat assessment processes and presents challenging and possible approaches to validate the proposed cyber threat assessment framework. The main features of the developed cyber threat assessment framework is presented. Finally, further modelling issues that may rise when extending the proposed cyber threat assessment framework are investigated.

- Chapter 7 concludes the thesis, by summarizing up the main contributions and results of the work. Besides, it addresses future research directions, which could extend the proposed stochastic game-theoretic cyber threat assessment framework.

Chapter 2

Literature Review

2.1 Introduction

This thesis focuses on threat assessment, which is a main point in any risk assessment methodology. Figure 2.1 sets out the position of threat assessment within a general risk assessment process. As shown in Figure 2.1, threat assessment includes risk identification, impact assessment and likelihood assessment within a general risk assessment process. In the literature, most of the time, threat assessment and risk assessment are discussed together. Therefore, this chapter will provide a non-exhaustive literature review of various cyber threat and risk assessment methods and frameworks, with an emphasis on threat assessment approaches involved in. Firstly, Section 2.2 provides an overview of current standardization progresses on smart grid cyber threat and risk assessment at national and/or international levels. Then, Section 2.3 introduces the very recent European projects that have already offered or are trying to offer threat and risk assessment solutions for cyber attacks. Understanding cascading failures facilitates a better appraisal of the risk from the physical consequences of cyber attacks. Therefore, Section 2.4 presents cascading failure propagation approaches related to this thesis, while Section 2.5 identifies various catalogue-based and model-based threat assessment approaches, which can be used to inform system operators about attack and threat scenarios and appropriate security countermeasure options. Finally, Section 2.6 discusses and presents the difficulty of cyber threat assessment for multistage attacks on smart grids.

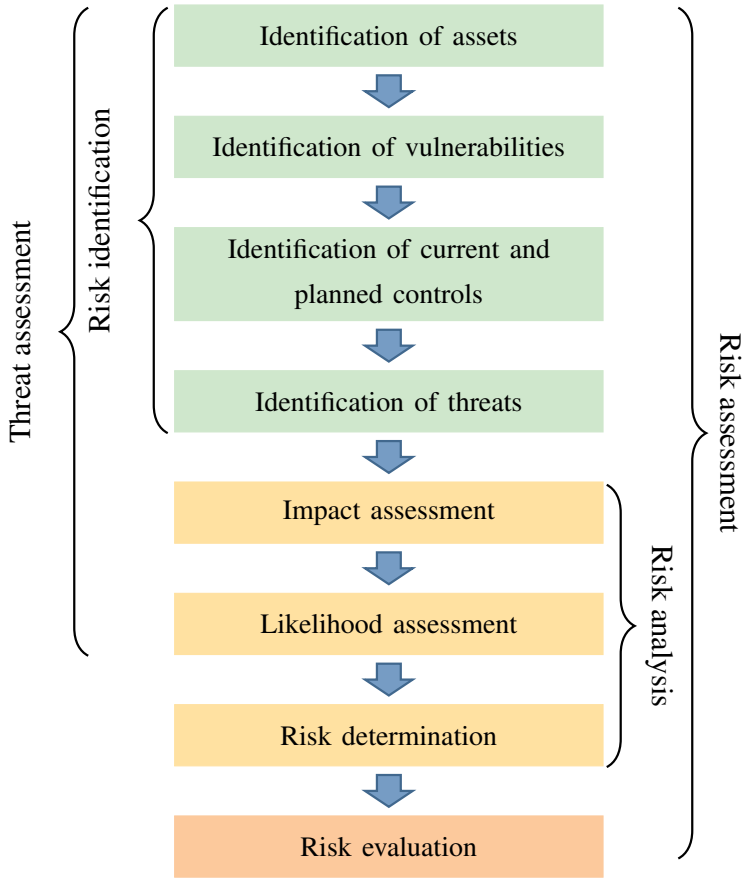


Figure 2.1: The position of threat assessment within a general risk assessment process. Adapted and refined from [1] according to Figure D.1 in Appendix D.

2.2 Smart Grid Cyber Threat and Risk Assessment

The interconnectivity of smart grid technologies allows for more accurate monitoring and reduced electricity consumption on behalf of the consumer, but it also introduces many larger opportunities for cyber attacks than ever before. Existing threat and risk assessment methods are divided into qualitative and quantitative approaches. Given the difficulties in presenting accurate numerical risk estimates, a qualitative risk assessment (e.g., low-medium-high), based on expert judgement and limited ranges of risk attributes, is recommended (e.g., by BSI). However, model-based quantitative approaches are more effective in determining risk indices, as they take into account the potential damage of assets, service interruptions, the likelihood of successful attacks, etc. Current risk assessment methods and frameworks mostly focus on conventional ICT systems or traditional power grids. Meanwhile, only a small number of smart

grid cybersecurity and risk management standards, guidelines, and recommendations has been published or is currently under development.

The UK Government has conducted a risk assessment on the smart metering implementation programme. The results of this risk assessment methodology are classified as restricted information and cannot be published. The Netherlands has conducted a privacy and security risk analysis of its advanced metering infrastructure. However, it encompasses only the smart metering segment of the smart grid. The German BSI has developed the *Common Criteria Protection Profile for the Gateway of a Smart Metering System and its Security Module* [22, 23]. Based on a threat analysis, both profiles define a set of minimum security requirements. Nevertheless, protection profiles are focused on smart metering gateways, which represent only one type among the many components found in smart grids. The CEN-CENELEC-ETSI Smart Grid Information Security (SGIS) working group has developed the so-called SGIS toolbox, which is a risk based approach, to identify security requirements for smart grid use cases [24]. As part of the M/490 framework [25], the SGIS report provides a framework for assessing the criticality of smart grid components by estimating the power loss caused by potential ICT system failures. The SGIS toolbox uses the HMG IS1 standard [26] for the purpose of vulnerability and threat analysis. The HMG IS1 standard has been designed to complement the frameworks provided by the ISO/IEC 27001:2005, ISO/IEC27002:2005, ISO/IEC27005 and ISO31000 standards. The SGIS toolbox has defined five security levels to categorize the inherent risks associated with smart grid information assets. The risk assessment proposed by SGIS takes a clean-slate approach, by assuming that an asset in smart grids has no security controls in place. Consequently, it is not suitable for a more practical scenario that focuses on actual, currently deployed or foreseeable security countermeasures.

The Reference Security Management Plan for Energy Infrastructure (RSMP) developed for the European Commission (EC) is intended to provide guidance to operators of energy grids or components. The RSMP contains recommendations on performing a risk assessment based on the *Performance and Risk-based Integrated Security Methodology (PRISM)*. The *Guidelines for Smart Grid Cyber Security (NIST-IR 7628)* [21], meanwhile, provides a set of high-level recommendations applicable to the smart grid architecture in the US. The importance and desirable goals of risk assessment are highlighted in this report. Similarly, the North American Electric Reliability Corporation (NERC) guidelines have elaborated further detailed aspects that a smart grid security assessment needs to cover [27]. However, both the NIST-IR 7628 and the NERC guidelines have provided a general approach for assessing cybersecurity risks. The

ENISA has maintained an inventory of risk assessment/risk management methods and tools [28], while the European Institute for the Protection and Security of Citizen (EC Joint Research Centre [29]) has reviewed 21 European and worldwide risk assessment methodologies and identified their gaps. However, most of the listed/compared risk assessment methodologies in [28] and [29] involve qualitative risk analysis (e.g., based on failure mode effects and criticality analysis), while the majority of them are targeted at terrorist attacks or physical attacks, rather than cyber attacks on smart grids. A report on smart grid security from ENISA [30] has provided a set of specific security measures for smart grid service providers, aimed at establishing a minimum level of cybersecurity. This report also points out the importance of performing a comprehensive risk assessment before selecting appropriate measures. Nevertheless, it does not recommend any specific risk assessment methodology. While smart grid-specific threat and risk assessment standards and recommendations do exist, they often insufficiently or fail to understand the mix of legacy and novel systems, functional dependency of information assets and the potential cascading effects in smart grids. Additionally, it is indicated in [31] that standards such as NIST-IR 7628 or the protection profiles published by BSI are only of limited practical use to utilities.

2.3 Threat and Risk Assessment Solutions for Cyber Attacks

A number of ongoing research activities has provided or is attempting to provide threat and risk assessment solutions for cyber attacks on smart grids. The Austrian research project Smart Grid Security Guidance ($(SG)^2$) has developed a cybersecurity risk assessment method using a cumulative smart grid model to represent both current and future European smart grids. The goal of $(SG)^2$ is to come up with a comprehensive catalogue of ICT-related risks for smart grids in Europe from a distribution system operator's perspective. A threat catelogue has been compiled from existing collections of ICT-related security threats, as developed by BSI. Subsequently, the identified threats has been applied to the components of the $(SG)^2$ architecture model, while a semi-quantitative approach has been taken in $(SG)^2$ to assess the probability and impact of threats.

Risk assessment methodologies have also been conducted by the FP7 project European Risk Assessment and Contingency Planning Methodologies for interconnected networks (EURACOM) [1], which has addressed the issue of protection and resilience of the energy supply

[1] http://www.eos-eu.com/Middle.aspx?Page=euracom (Retrieved: 28/06/2017)

within European interconnected energy networks. Working together with critical energy infrastructures operators in Europe, the goal of EURACOM is to identify a common and holistic approach (end-to-end energy supply chain) for risk assessment and risk management solutions. The first step in the holistic risk assessment methodology is to constitute a holistic risk assessment team, which consists of a team leader (responsible for the completeness, consistency and homogeneity of the risk evaluation) and several team members (with holistic security physical, ICT, organizational and human areas of expertise). Subsequently, the scope of the risk assessment is defined (with details dependent on the resources applied and the stakeholders involved), while the assessment of the risk is reached by directly evaluating the probability of occurrence and severity.

The EU-funded Security for Smart Electricity GRIDs (SEGRID) project [1] is investigating risk assessment methodologies and their possible enhancement to protect smart grids against cyber attacks. Based on the HMG IS1 standard, the SEGRID threat and risk assessment approach comprises four steps: 1) establishing the scope of the threat and the risk assessment process, wherein stakeholders are identified and stakeholders' information assets are documented; 2) involving an assessment of the risk in terms of the impact of a security incident that compromises a particular asset involved in a stakeholder process; 3) identifying threat actors, potential attacks and threat scenarios, based on the system components diagram for the SEGRID use case; 4) determining the risk for each of the stakeholders based on an estimated likelihood and impact for each stakeholder. Additionally, the overall risk for each threat scenario is estimated. Specifically, SEGRID uses CORAS threat scenario diagrams (CORAS provides a customized language for threat and risk modelling) in the third step, while including the threat actor motivation and capability in the fourth step for the likelihood and impact assessment.

The EU-funded Smart Grid Protection Against Cyber Attacks (SPARKS) project [2] has investigated a cybersecurity risk management process based on the information security risk management process, which is standardized in ISO/IEC 27005. The SPARKS risk management process aims to reflect both cyber and physical aspects of smart grids. There are four main topics defined in the overall risk management process: 1) context establishment; 2) impact assessment; 3) likelihood assessment; and 4) security requirements and recommendations. The context establishment step constructs the scope of the risk management process by making

[1] https://segrid.eu/ (Retrieved:20/06/2017)

[2] https://project-sparks.eu/ (Retrieved:20/06/2017)

use of the smart grid architecture model (SGAM) framework. Meanwhile, the SGIS toolbox is utilized to describe a voltage control and power flow optimization smart grid use case. The impact assessment step involves identifying the violation of confidentiality, integrity, and availability (CIA) for the information assets, which are defined in the use case. The impact assessment is also undertaken with regard to operational, regulatory, economic and reputational factors. SPARKS has taken advantage of the HMG IS1 risk assessment standard to develop a threat model and semantic attack graphs to support likelihood assessment. The threat assessment method in the HMG IS1 risk assessment standard focuses significantly on possible threats by looking at the capabilities and motivation of attackers, thus ignoring vulnerabilities and countermeasures. In SPARKS, risk treatment is followed after completing the risk assessment process. For the specific voltage control use case, SPARKS has derived specific smart grid security requirements and made recommendations based on the NIST-IR 7628 [32] and ENISA guidelines [15].

The Hybrid Risk Management for Utility Providers (HyRiM) project [1] is not specifically tailored to threat and risk assessments of smart grids, but it is developing novel risk analysis techniques that can be applied to interdependent complex systems, for example, smart grids. One aspect of HyRiM is the investigation of repeated game-based hybrid risk metrics for managing security risks in interconnected utility infrastructure networks. HyRiM has approached the interactions between the attacker and the system administrator as a repeated game. The project has argued that the outcome of an action from either the attacker or the system administrator is almost never fully certain. As a consequence, the game, within the context of HyRiM, has been designed to enable all uncertainties of the game play in terms of action outcomes. In order to estimate the cascading effects of a specific attack scenario (e.g., ransomware attack) for a given defense situation, as well provide the payoffs for the investigated repeated game, connections within an infrastructure and/or with other infrastructures are divided into different types, while percolation theory-based models [33] are adapted in HyRiM.

2.4 Cascading Failures in Smart Grids

Understanding cascading effects is one key challenge that should be addressed in the risk assessment of smart grids. One important step in the SGIS toolbox is assessing the potential cascading effects, which are associated with information assets. As discussed in [34], cascading

[1] https://hyrim.net/ (Retrieved:20/06/2017)

effect analysis facilitates a better understanding of the risk of possible physical consequences from cyber attacks and/or the risk of possible cyber consequences from physical attacks. In the last decade, numeric models have been proposed for analysing cascading failure propagations in interdependent power grids and communication networks. This work briefly summarizes the major related studies on cascading failure propagations in smart grids, while presenting a summary and comparison of these approaches in Table 2.1.

Ruj and Pal [35] investigated cascading failure propagations in smart grids subject to random and targeted attacks initiated in the communication network. The random attack randomly chose nodes to compromise, while the targeted attack selectively compromised high-link degree nodes with higher probabilities. The communication node supported one power station and was powered by one power node, while a power node was controlled by multiple communication nodes and supplied power to multiple communication nodes. Both the power network and the communication network were modelled as undirected interdependent scale-free networks. the authors of [35] mathematically analysed the size of the giant components of the network experiencing targeted attacks and derived a steady analysis for cascading failure propagations.

In order to characterize the performance effects of the communication network on smart grid operations, Lu et al. [36] considered a fault occurrence scenario in a power distribution network to analyse possible cascading failure behaviours implied in coupled and interdependent power and communication networks. Intelligent electrical devices (IEDs) are nodes in the communication network. Different from those models developed in [42, 43, 44] (these are based on the assumption that the communication nodes malfunction immediately after losing power supply from power substations), communication nodes in [36] were installed with backup power supplies. A python-based co-simulation framework was designed and implemented to replay interdependent iterations of the cyber-physical system, in order to verify the domino effect of communication transmission failures.

Huang et al. [37] considered both the power grid and the communication network as undirected scale-free networks with a power-law degree distribution. The authors of [37] observed that the inter links between the power grid and the communication network were of the "one-to-multiple" type: each communication node received energy from one power station and each power station provided energy to many communication nodes. The effect of cascading failure was studied with percolation theory, along with a detailed mathematical analysis of the failure

Scheme	Network Model	Original of failures	Power grid		Cascading effects	
			Trans.	Dist.	Interdependency	Node/Line overloading
Ruj and Pal [35]	undirected, scale-free	commun. network	✓	✓	✓	
Lu et al. [36]	co-simulation	commun. network		✓	✓	
Huang et al. [37]	undirected, scale-free	commun. network	✓		✓	
Huang et al. [38]	undirected, scale-free	power grid		✓	✓	✓
Parandehgheibi et al. [39]	undirected	power grid	✓		✓	✓
Rahnamay-Naeini and Hayat [40]	co-simulation	power grid	✓		✓	✓
Rahnamay-Naeini [41]	directed and weighted, Erdős-Rényi	commun. network or power grid	✓		✓	

Table 2.1: Summary of cascading failure propagation schemes in smart girds.

propagation in [37]. The robustness of the interdependent complex network model was analysed in terms of random attacks or failures by estimating the fraction of functional nodes after the stop of the cascading failures in both networks.

Huang et al. [38] also studied cascading failures that were jointly caused by load propagation and interdependence in smart grids. The authors of [38] argued that interdependency cascading failure had been mainly performed using pure topological methods, resulted in the lack of considerations of electricity characteristics. Additionally, studies conducted on load propagation cascading failure have been limited to power grids without interdependent ICTs. The interdependence relationship between the power grid and the communication was as follows: each power station was monitored and operated by several distinct control nodes in the communication network; the number of communication nodes that one power node could support was dependent on and limited to the power node's capacity. Similar to the work in [37], both the power grid and the communication network were undirected scale-free networks. A power node's capacity is defined as a function of its link degree, with the load of a failed node uniformly distributed to its neighbours. A percolation-based mathematical method was devised to simulate the propagation of cascading failures and to calculate the fraction of survival in both the power grid and communication network, when initial failures occurred in the power grid.

Parandehgheibi et al. [39] considered the power flow equation for analysing the behaviour of interdependent power grid and communication networks. Both the power grid and the communication network are modelled as graphs. The interdependency between the power grid and the communication network is assigned as follows: each communication node receives power from one power node, with each power node able to support multiple communication nodes. Additionally, the interdependency model is slightly modified by the power flow equation, meaning that, when the required power is not sufficient to support a communication node, the communication node will fail. If a power substation loses its control and there are failures in the power grid, the transmission line would be tripped and such a failure would propagate to the communication network, resulting in additional failures in both interdependent power grids and communication networks. Additionally, a load control mitigation policy was developed in [39] to mitigate cascading failures in the interdependent power grids and communication networks.

Rahnamay-Naeini and Hayat [40] investigated the effect of overestimation of transmission line capacity in functional interdependent communication networks and power grids. If failures (e.g., line overloading) occurred in the power transmission system, power would be

redistributed in the power grid by solving a direct current (DC) power flow optimization problem. If lines were overloaded after power redistribution, more failures would occur in the power grid. On the other hand, a communication node probabilistically fails if the power node in its geographical proximity fails. Failures in the communication system affect the power flow redistribution decision, while the failure of power nodes leads to further failures in the communication network. This cycle goes on until no more failures exist in the interdependent power grids and communication networks.

Rahnamay-Naeini [41] adopted a networked Markov chain framework and presented an interdependent network model to investigate the effects of interdependencies on cascading failures and to characterize the optimum allocation of interdependencies. Nodes in both the power grid and the communication network were clustered and receives services from each other according to geographical constraints. The intranetwork and the internetwork were modelled as directed and weighted graphs. The cascading failure could be initiated from any one of those interdependent networks. The internetwork was modelled as follows: a communication node received electricity from several power nodes, while a power node received monitoring and controlling services from several communication nodes. Based on a networked Markov chain framework, the optimum interdependencies for minimizing cascading effects was obtained by solving a nonlinear optimization problem. The author observed that multiple internetwork allocation leads to more reliable interdependent networks compared to the allocation of single interpower law degree distributionnetwork links.

2.5 Threat Assessment Approaches for Cyber Attacks

Representing the first few steps of a general risk assessment process, threat assessment is essential to inform the security operator about the potential attack/threat scenarios and the appropriate security countermeasure selections. Withstanding cyber threats of unpredictable patterns is a massive challenge and has received much attention from the research community. Generally, the used methods can be categorized into *catalogue-based* and *model-based* approaches. Catalogue-based approaches are typically defined in standards and use deterministic elements to evaluate the system, while model-based analyses are more context-specific. This thesis provides a subjective, non-exhaustive survey of threat assessment approaches identified from the literature.

2.5.1 Catalogue-based Analysis

Catalogue-based analysis methods typically provide checklists, constraints and scoring spreadsheets to deterministically evaluate a system. Those catalogues include BSI IT-Grundschutz Catalogues [45], ISO/IEC 27002 [46] and NIST 800-53 [47]. Regaring BSI IT-Grundschutz Catalogues, for example, they provide lists of typical relevant threats and the respective standard security measures for standard asset types. Technical, organizational, personnel and infrastructural issues are encountered in BSI IT-Grundschutz Catalogues. Catalogue-based analysis methods are attractive for norms and standards (e.g., EC, ETSI, ISO, MITRE, NIST), as they support deterministic security evaluations. The threat assessment & remediation analysis (TARA) methodology [48], as reported by MITRE, aims to identify and assess cyber threats and select countermeasures that are effective at mitigating the APT. In TARA, the cyber asset's architecture, technology, and security capabilities were evaluated against tactics, techniques, and procedures (TTPs) in the mission assurance engineering catalogue, which includes common attack pattern enumeration and classification (CAPEC), common weakness enumeration (CWE), and common vulnerability enumeration (CVE). Scoring spreadsheets were applied to quantitatively rank attack TTPs. In turn, a threat matrix was produced to list plausible attack TTPs, which were ranked by decreasing risk score, while attacks were mapped onto cyber assets as a function of adversary types. Based on the BSI IT-Grundschutz Catalogues, the $(SG)^2$ project compiled a threat catalogue to conduct cyber threat and risk assessment in smart grids. The downside of most catalogue-based threat and risk assessment methods is their incomplete analysis, as assets or interdependencies among assets, which are not covered by the catalogue, are not evaluated properly. Another challenging issue for catalogue-based threat assessment methods is the selection of criteria for risk scoring and threat likelihood assignment.

2.5.2 Model-based Analysis

The cybersecurity research community has been working to develop various model-based tools to support threat assessment. Model-based analysis approaches use a sequential and explorative process to gradually identify and assess the system under evaluation. The model-based tools available today include (but are not limited to) attack tree-based approaches, attack graph-based approaches, game-theoretic-based approaches and Bayesian network-based approaches. Regardless of the modelling formalism, such tools share many common objectives and features.

For example, many of the model-based analysis approaches provide a quantitative evaluation of cyber attacks using various metrics to support decision-making.

Attack tree and attack graph approaches

Adapted from fault analysis trees, attack trees (ATs) are prominent tools for threat analysis [49, 50, 51]. The underlying philosophy of attack trees is to identify and evaluate the whole system in the same way as an attacker in order to identify the most attractive path (with minimal effort or least resistance) for the attacker. An attack tree uses a root node to represent the attacker's top-level goal. This root node is recursively defined into the attacker's subgoal, while leaf nodes are defined to enumerate possible attacks that contribute to reaching the (sub)goal through logical gates. To succeed in propagating attacks through the system in this step, AND-gates model conditions that the attack must succeed in all his/her child nodes; and OR-gates model conditions that the attacker must succeed in at least one of his/her child nodes. Attack trees are high-level representations of threats and provide a structured way of performing security analysis. Figure 2.2 shows a measurement interruption attack tree in the context of an advanced metering infrastructure. The leaf nodes are attack actions, while the attack tree uses AND and OR gates to define combinations of attack actions (or combinations of attack action and subgoal), which are needed to achieve the ultimate goal of the attacker. The likelihood for measurement interruption occurring is computed by simple logic rules after the likelihood of each attack has been determined by expert judgement.

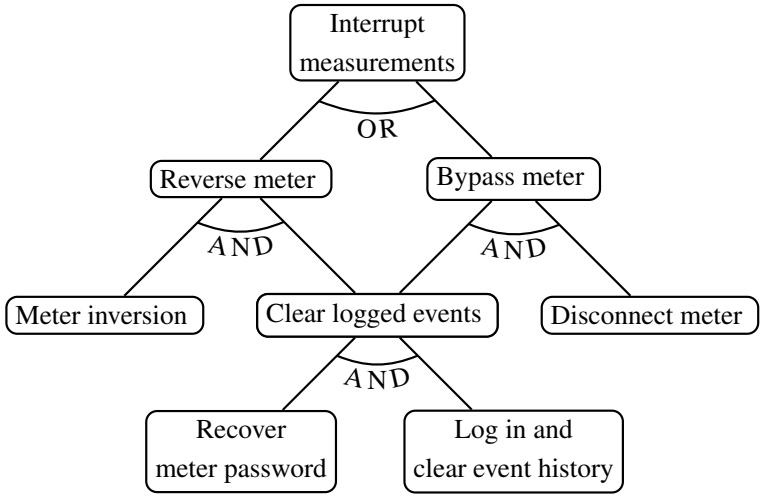


Figure 2.2: A sample attack tree.

A significant limitation of typical attack tree approaches is scalability: for more attack goals, more trees need to be constructed. Since attack trees are not used to capture low-level or concrete security configuration details, it is difficult to construct attack trees that contain enough details (e.g., vulnerabilities in smart grids) for meaningful analysis [52]. Kordy et al. [53] proposed attack-defense trees (ADTs) to extend attack trees with defensive measures to model the interaction between attacks and defences using game theory for arbitrary alternation between these two types of actions. That work also provided semantical approaches regarding how to quantitatively analyse attack and defence scenarios using attributes. However, in ADTs, the defence metrics were absent in the probabilistic analysis of real cyber-attack cases. Roy et al. [54] presented attack countermeasure trees (ACTs) to enable defence mechanisms at all nodes of the tree and to avoid state explosion. Several studies have transformed attack trees into models that allow for the analysis of attack steps as a sequence. Qin and Lee [55] proposed a conversion of attack trees into causal networks representing an order of the execution of steps contained in the tree to evaluate the likelihood of attack goals and predict future attacks. Dalton et al. [56] proposed a transformation of attack trees into Petri nets. The purpose of the transformation to Petri nets is to use simulation to perform probabilistic analysis, i.e., the likelihood that the attacker will obtain his/her (sub)goal along paths in the attack tree.

Different from attack trees, attack graphs (AGs) provide a low-level description of a system, which focuses on the vulnerability exploitation of attacks, privileges that the attacker may have on network components, and transitions between network components. In AGs, nodes can be used to represent system and network states (e.g., user privilege levels) and edges (to enables transition from one node to another) can be used to present vulnerability exploitations. Attack graphs allow us to consider potential attacks and their consequences in a particular context. Such a context makes it possible to compose individual measures of vulnerabilities, resources, and configurations into a global measure of network security. Attack graphs offer great potential in detecting hidden multiple staged attack paths, as well as facilitating deeper understanding of security risks. Over the last decade, researchers have started to focus their interests on attack graphs in network security. Numerous papers, including [57, 58, 59, 60, 61] have been published in recent years, which measure and analyse network security using attack graphs. This work examines and reviews those approaches with the application of attack graphs in smart grid and other critical infrastructures.

Zhu et al. [62] argued that the assumption of the synchronous removal of substation/transmission lines has apparent limitations when seeking to comprehensively exploit the character-

istics of cascading failures, as well as discovered a sequential attack scenario. Consequently, a sequential attack graph (SAG) was proposed to capture the combination of vulnerable nodes and to indicate their removal order. Based on this graph, a practical sequential attack strategy was designed with good attack performance and low complexity. The authors of [62] foresaw that the results from the SAG could be explored to design defence solutions against attacks.

Hawrylak et al. [63] modelled the attack on smart grids using a hybrid attack graph (HAG). Compared with traditional attack graphs, a HAG includes both cyber and physical parameters in smart grids. The authors assumed that an attacker's goal was to overheat and destroy a transformer. The generator built the HAG from a cyber physical system description file (which included network connections and component parameters) and an exploit file (which contained a set of preconditions that an exploit must satisfy and a set of post-conditions that may change the system state). In this graph, the physical dynamics of the system under attack were simplified without discussing the implications of the simplifications.

Beckers et al. [64] combined the attack tree and the attack graph to determine the probability of smart grid attacks. Lever et al. [60], meanwhile, presented a distributed attack graph generation solution in order to evaluate interdependencies and cascading failures in critical infrastructures. Attack graphs can be automatically generated by various tools, for example MulVAL [65]. Finding the optimal attack path in an attack graph is an NP-hard problem [66]. Some researchers have translated an attack graph into a Markov decision process (MDP) in order to find the optimal attack path [67, 68, 69]. However, the characterization of changing topologies and the dynamic nature of the attacks are important challenges that need to be addressed in order to make attack graphs effective in network security analysis. As with ATs, AGs also model a system with a predetermined end goal for an attacker. While AGs work for a small system, they cannot be scale to a system that has different targets depending on an attacker's goal.

Game theory approaches

A game consists of players (in this thesis, the attacker and the defender), strategies (i.e., actions of players) available to each player, and utilities depending on the joint decisions of all players. Game theory depicts dynamic interactions between players, involving a complementary methodology of attack trees and/or attack graphs in face of changing attack patterns.

Ismail et al. [70] modelled the problem of optimizing the distribution of defence resources on communication equipment as a one-shot game [71] between the attacker and the defender.

That game took into account the interdependency between the cyber and physical components in the power grid. It was assumed that the initial risk, the immediate risk on a node before any incidents or failure propagations is a positive real number and evaluated using other risk assessment methods. The immediate risk and the future cascading risk from interdependent electrical and communication infrastructures were balanced in [70]. The interdependency between the electrical and communication infrastructures were modelled as a weighted directed interdependency graph. Each communication equipment was associated with a load. The worst-case scenario, where both the attacker and the defender have complete knowledge of the architecture of the system, was considered in [70]. The utility functions of both players are composed of three parts: the reward for an attack, the cost of attacking/defending, and the impact of redundant communication equipment. The impact of attacks in the electric and communication infrastructures was evaluated by solving power flow equations and using attack graphs, in conjunction with other risk assessment methods. The dataset of the Polish electric transmission system, provided in the MATPOWER computational packages, was taken as a case study to validate the proposed game-theoretic model, while Nash equilibria for the attacker and the defender for each type of communication equipment in the case study were presented.

Jiang et al. [72] proposed a two-player non-cooperative, zero-sum, and finite stochastic game for the attacker and the defender in computer networks. A Markov chain for a privilege model and a privilege-escalating attack taxonomy were presented. By making use of the developed stochastic game model, a Markov chain for the privilege model, and a cost-sensitive model, the attacker's behaviour and the optimal defence strategy for the defender were predicted. He et al. [73] studied a network security risk assessment-oriented game-theoretic attack-defence model to quantify the probability of threats. The payoff matrix was formulated from a cost-benefit analysis, where the cost to the defender when taking actions was made up of the operational cost, the response cost, and the response negative cost. Combined with the vulnerability associated with the nodes, risks of the system were computed as the sum of the threat value of all nodes.

Guillarme et al. [74] presented an attack stochastic game model for adversarial intention recognition (and, by extension, threat assessment) for situations featuring strategic interactions between an attacker and a defender. The attack stochastic game model is a coupling of discounted stochastic games and probabilistic attack graphs, although it suffers from zero-sum constraints. In the attack stochastic game model, it was assumed that both the attacker's action and the defender's action, as well as the states experienced by players, were fully observable to

both players. This model was inverted to infer the intention of an attacker from observations of his/her (sub-)optimal actions. However, this model does not have the ability to detect intention changes, while the scalability is the principal limitation of this attack stochastic game model.

Nguyen et al. [75] studied a two-player zero-sum stochastic game-theoretic approach to provide the defender with guidelines to allocate his/her resources to secure his/her communication and computer networks. Linear influence networks [76] were used to present the interdependency of nodes in terms of security assets and vulnerabilities. He et al. [1]° investigated game-theoretic risk assessment in smart grid communication networks and noticed that the data acquisition and data interpretation for risk assessment and prediction had not been intensively explored. Therefore, [1]° established a surveillance architecture to monitor message transactions in communication networks, while surveillance observations were further interpreted as Dirichlet-distributed security events with certain probabilities. By taking the interactions between possible suspicious nodes and the security operators as a repeated zero-sum transmitting-monitoring game, a game-theoretic risk assessment framework was established to compute and forecast the risk of network security impairment. Rass and Zhu [77] presented a sequence of nested finite two-player zero-sum games for developing effective protective layers and designing defence-in-depth strategies against APTs. In the game-theoretical model, nodes in an infrastructure were equidistantly separated into different levels according to their layers in the infrastructure. Within each level, the game structure was determined by the nodes' vulnerabilities and their distances from the target node. The authors of [77] discussed some closed form solutions for their APTs games and analytically formulated infrastructure design problems to optimize the quality of security across several layers. Under the framework of the HyRiM project, Rass et al. [78] investigated an extensive form game as a risk mitigation tool for defending against APTs. An APT was modelled as a zero-sum one-shot game with complete information, but uncertainty was observed in the game payoffs. Based on a topological vulnerability analysis and an established attack graph, all the attack vectors covered in enumerated attack paths (from the root node to the target node in the attack graph) made up the attacker's action space. By defining players' payoffs as probability-distributed values, instead of real numbers, [78] provided a relative new approach to tackling ambiguous and inconsistent expert opinions in risk management.

Miscellaneous approaches

Ma and Smith [52] proposed a vulnerability-centric risk analysis approach to determine security risks associated with multistep cyber attacks in critical information infrastructures. The hosts' vulnerabilities were mapped into preconditions and effects, while rule-based reasoning was used for vulnerability chaining. Finally, attack paths in the system were identified with a vulnerability chain augmented graph. However, this study did not calculate risk levels nor identify which attack path was the most likely to compromise the whole system. A Bayesian network may be created to depict stochastic dependencies between the actions involved in an attack-defense tree (ADTree) in order to perform a probabilistic evaluation of attack-defence scenarios [79]. Bayesian networks were also applied in AgenaRisk [1]to provide decision support solutions to industry sectors. The conditional probability tables (CPTs) in Bayesian networks are difficult to define and expand linearly with the number of loops in which they are involved. Therefore, Bayesian network-based threat assessment approaches are impractical for analysing large complex systems, such as smart grids. Fielder et al. [80] proposed a simulation of resource-limited attackers and defenders of an ICS. The objective here [80] was to identify the appropriate deployment of specific defensive strategies to reduce the risk of destructive cyber-physical effects initiated from cyber attacks. The optimal defensive strategies were obtained by solving a co-evolutionary particle swarm optimization problem. Continuous-time hidden Markov models (HMMs) for real-time risk assessment were introduced in [81]. The risk to assets in a network was evaluated as the probability and consequence of unwanted incidents. However, the parameters of the mathematical models to calculate the probability and consequence values are highly uncertain. Based on fuzzy theory and Petri nets, Liao et al. [82] assessed and forecast network security risks based on detection alerts and network attack information. Since extensive attack information is difficult to obtain, or is not totally known to the public, this approach suffers from the problem of attack information incompleteness.

2.6 Cyber Threat Assessment Difficulty in Smart Grids

The concerns from standardization bodies and research communities are mainly centred around assessing vulnerabilities and cyber threats, providing generic guidelines for effective threat and risk assessment, and detecting and mitigating attack scenarios. The challenges relating to threat

[1]http://www.agenarisk.com (Retrieved: 28/06/2017)

and risk assessments in smart grids have increased rapidly with the introduction of ICT components. This situation will become even worse when the roll-out of smart grids results in a large complex combination of legacy and new technologies. Threat and risk assessments for emerging multistage attacks, such as APTs, are extremely challenging and have not yet been comprehensively investigated. Assessing threats for multistage cyber attacks is not an easy task, since numerous unknown variables (e.g., vulnerability dependencies, attack stages, and possible physical impacts) need to be taken into account. For the time being, from practitioners' perspective, performing threat and risk assessments requires skills, time and strong management support. Most importantly, it is rather difficult for practitioners to set up major existing threat and risk assessment frameworks within their respective infrastructure. However, preventive estimation and minimization of the risk of multistage cyber attacks on smart grid communication networks are essential to prevent smart grids from industrial espionage and damage to physical plants. Therefore, the difficulty and challenges relating to cyber threat assessments lies in the development of easy-to-follow methods and frameworks.

2.7 Summary

This chapter presented a literature review of smart grid cyber threat and risk assessment methods and frameworks and their deficiencies. It also surveyed cyber threat and risk assessment efforts from standardization bodies at national and/or international levels, introduced recent threat and risk assessment solutions from diverse European projects, presented cascading failure propagation approaches, which facilitate the process of threat and risk assessments, and identified threat assessment approaches from worldwide research communities. Finally, it discussed the difficulty faced by system operators in performing cyber threat assessments and the obstacles in developing easy-to-follow cyber threat assessments for multi-stage attacks. The following chapter will present details on a stochastic game-theoretic cyber threat assessment framework, which can be used to assess threats and provide defence recommendations to mitigate such threats in smart grid communication networks.

Chapter 3

Stochastic Game-Theoretic Cyber Threat Assessment Framework

3.1 Introduction

As discussed in Chapter 2, the majority of existing threat and risk assessment methods and frameworks are generic and not easy for practitioners, especially those working in smart grids, to follow. This is because these methods usually evaluate the system from the defender's perspective, and ignore the fact that the attacker also has a perspective on the entire defence mechanisms of the system that he/she wants to attack. As a consequence, recommended defence techniques are not always feasible or appropriate to protect a system. While some threat and risk assessment methods and frameworks consider the interactions between attackers and defenders, they always assume that the defender and the attacker can fully observe the system state, which is not true in many realistic cases. The biggest drawback regarding contemporary threat and risk assessment methods and frameworks is that some of them have not taken the multistage nature of attacks (i.e., the occurrence of the next step being dependent on the success of the previous step) into account, with some exceptions [77, 78, 83]. None of these precursor works has looked at the stochastic and dynamic nature of attacks in smart grid use cases (modelled as stochastic games). Additionally, the impact of cyber attacks on physical power grids is not fully explored in current existing threat and risk assessment methods and frameworks.

This chapter presents a threat assessment framework for multistage cyber attacks, taking into account the dual perspectives of both the attacker and the defender. The rationale behind

the approach is to consider the key aspects of cyber attacks, namely, the resulting physical impacts from cyber attacks and the cost of the attacker to launch an attack. The physical impact of cyber attacks on smart grids is occasionally oversimplified by researchers (e.g., they do not consider functional dependencies in interdependent power grids and communication networks), which can lead to incomplete and ineffective threat assessment models. This thesis attempts to provide a cyber threat assessment framework for multistage attacks by considering some of the real-world issues that are necessary for accurate threat assessments in smart grid communication networks. The objective of the developed cyber threat assessment framework is to facilitate easy-to-follow cyber threat assessments for practitioners. These practitioners may include (but are not limited to) DSOs and solution providers, who are concerned with security in smart grids and interested in learning about applicable state-of-the-art solutions. Section 3.2 of this chapter will first identify the benefits of applying game theory in analysing network cyber security assessments, while Section 3.3 presents the preliminaries of game theory, including some selected concepts and terms used in game theory. Finally, before summarizing this chapter, the developed stochastic game-theoretic cyber threat assessment framework is introduced in detail in Section 3.4.

3.2 Game Theory and Network Cyber Security Assessment

Cyber security can be seen as an adversarial game comprising multiple decision makers: that is, attackers and defenders, who have different objectives and choose their course of action based on certain rationales (e.g., cost-benefit analysis). The growing complexity and interconnected nature of cyber infrastructure in smart grids make network cyber security a challenging issue. Game theory models conflicting situations and provides a scientific basis for high-level security-related decision-makings [84]. Game theory has attracted more and more attention in the network security community recently, because of its role in decision-making and control theory [73], [85], [86], [87].

There are indeed several kinds of situations in the network security domain where decision makers have conflicting interests and must deploy complex strategies in order to reach the most profitable outcome. Examples of such situations are security assessment, network attack prediction, optimal active defence deployment, and intrusion response. Game theory is particularly well suited in all those cases to characterize the nature and complexity of the

interactions among decision makers. Furthermore, game theory lays the foundation for our developed stochastic game-theoretic cyber threat assessment framework, which will be reviewed in Section 3.4.

Game theory provides mathematical approaches for analysing and predicting how decision makers behave in strategic situations. Although it has seen widespread applications in economics, its application to cyber security is quite recent. The potential benefits of applying game theory to cyber security problems are fourfold [88, 89, 90]:

1. Game theory captures the interactions between attackers and defenders and provides a set of quantitative and analytical tools. These games for cyber security interactions suggest optimal defence strategies with accompanying predicted outcomes to defend against attackers.
2. Game theory provides the capability of examining a large number of possible attack scenarios, so that human experts can leave the burden of decision-making in large action spaces to optimization algorithms provided by game theory.
3. Game theory has been proven to be rather effective at analysing certain what-if scenarios, i.e., give minimax decisions, which are the best defence against any possible behaviour on the part of the opponent (provided that the set of possible actions is exhaustively known). Such strategies are called *security strategies*.
4. Game theory can model situations where only partial knowledge about the game is accessible to certain decision makers, as well as analyse scenarios where attackers and defenders have asymmetric information about the underlying game.

There are also criticisms of game theory or its rationality assumptions. Rationality assumptions imply that every player is motivated by maximizing his/her own payoff, thus he/she is able to perfectly calculate the probabilistic result of every action. This thesis assumes both players have perfect rationality.

3.3 Preliminaries of Game Theory

Game theory [71, 91] is a mathematical model of decision-making which allows modelling conflict and cooperation between two or more separate decision makers, the *players*. The basic assumptions that underlie the theory are that players are *rational*, i.e., they are triggered by the

selfish incentive of maximising their individual benefit, which is usually expressed in terms of a *utility function*. Utility functions are mathematical formulae (involving variables and constants) which describe the method to assign *payoffs* to players depending on the action taken in the game. Payoffs may represent *reward*, *quantity*, or other such measures. If payoffs represent *rewards* in a certain game, then negative values for payoffs can be presumed to be a *loss* and a *zero* to be *no reward* or *no loss*. During the game, in order to maximise the payoff they are receiving as an outcome of the game, players can choose and implement an *action* from a set of different behavioural options, the so-called *action space*. Figure 3.1 shows the game-theoretic formalisation of interactions between two players.

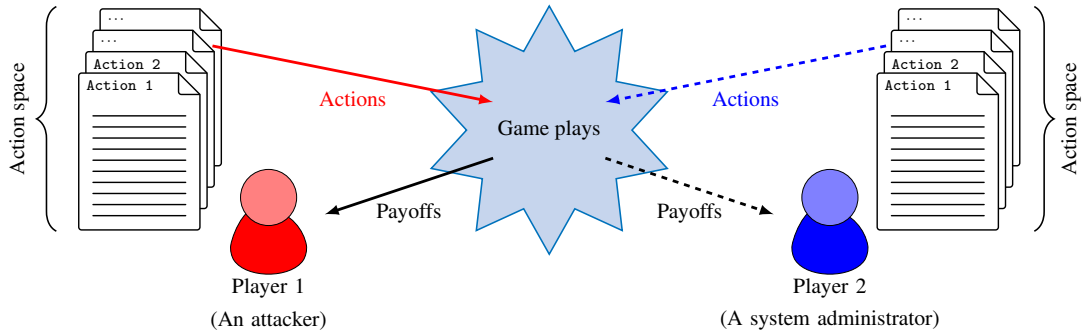


Figure 3.1: Game theoretic formalisation of interactions between two players.

Hence, formally a game can be defined as a triple $\Gamma = \{ I , \mathbf{G}, AS\}$, where I is a finite set of players and $I = \{1, 2, \cdots, i, \cdots\}$, $AS = \{AS_1, AS_2, \cdots, AS_i, \cdots\}$ is a finite family of action spaces for all players and $m_i = |AS_i|$, and $\mathbf{G} = (\mathbf{G}_1, \mathbf{G}_2, \cdots, \mathbf{G}_i, \cdots)$ where $\mathbf{G}_i = \{g_i : AS_i \times AS_{-i} \rightarrow \mathbb{R} | i, -i \in I\}$ is a family of utility functions to characterise the payoff received by player i when the action from player i and the joint action by other players $-i$ are taken. Here, $-i$ is a shorthand to mean the other players except player $i \in I$. And correspondingly, AS_{-i} denotes the collective action space of other players except player i (i.e., $AS_{-i} = (AS_1, AS_2, \cdots, AS_{i-1}, AS_{i+1}, \cdots)$). Note that an individual element a_i (i.e., action a_i) of the action space AS_i is called a *pure strategy*, whereas a *mixed strategy* can be described as a linear combination of two or more pure strategies, with weights summing up to 1. A pure strategy can also be considered as a mixed strategy at its extreme, with binary assignment (setting one action to 1 and all other actions to 0). However, in this thesis, pure strategies are not mixed strategies. A mixed strategy can be interpreted as the probability distribution $\mathbf{x}_i$ for player i

choosing randomly among the pure strategies involved, hence

$$\mathbf{x}_i = \left\{ (x_{i,1}, x_{i,2} \cdots, x_{i,a_i}, \cdots, x_{i,m_i}) \in \mathbb{R}_+^{m_i} | \sum_{a_i=1}^{m_i} x_{i,a_i} = 1, 0 \leq x_{i,a_i} \leq 1 \right\}. \tag{3.1}$$

The goal is to determine for each player i the probability distribution maximising the *expected payoff* with function

$$\mathcal{F}_i(\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_i, \cdots) = \mathbf{x}_i \cdot \mathbf{G}_i \cdot \mathbf{x}_{-i}^T, \tag{3.2}$$

where $\mathbf{x}_{-i}^T$ denotes the transposition of the mixed strategy $\mathbf{x}_{-i}$. For a non-trivial game, the objective function (see Equation (3.2)) of a player depends on the choices (actions, or equivalently decision rules) of at least one player, and generally of all the players. Hence, a player cannot simply optimise his/her own objective function independently of the choices of other players. This results in a coupling between the actions of the players in decision making even in a non-cooperative environment. If players were able to enter into a cooperative agreement, then we would be in the realm of *cooperative game theory*, with issues of bargaining, coalition formation, excess utility distribution and so on. More reference examples of cooperative games can be found in [92, 93, 94]. Otherwise, if no cooperation is allowed or possible among players, we are in the realm of *non-cooperative game theory*. A non-cooperative game is *zero-sum* if payoffs of players all summing up to the constant zero, which corresponds to "my reward is your loss", or equivalently, a total budget being distributed among the players according to the game's outcome. If players' payoffs added up to a constant (without scaling or translation), then the game is called *constant sum*. And the *non-zeor-sum* game is the mere else-case. A game is *finite* if each player has a finite number of moves and a finite number of actions; otherwise the game is *infinite*. A game is a *complete information game* if the description of the game (i.e., the players, the objective functions, the action of each player) is common information to all players; otherwise we have an *incomplete information game*, where there are some uncertainties about the actions of players, the moving sequence of the game, or the payoffs. A *static game* rewards the players in the same way in each repetition. In contrast, in a *dynamic game*, players observe the payoffs in the previous repetition before playing later round. A game is said to have *symmetric information*, when players have symmetric information. Where players' information may include the sequence of the game, actions have been taken in the last round, and player's payoffs. In contrary, in a game of *asymmetric information*, players have different information, for example, the attacker is better informed about the compromised nodes than the defender. This work covers only non-cooperative games with asymmetric information.

3.3.1 Nash Equilibrium

Game-theoretic analysis attempts to understand the probable behaviour of the players, regarding their strategy choice, and thus to determine the presumable outcome of the game. In some cases, this works relatively straightforward, for instance, if any player can identify a "dominant strategy", i.e., a strategy that outperforms all alternatives. A much broader equilibrium concept, the so-called *Nash equilibrium* is achieved if an operational point is reached where each player is giving his/her best response facing his/her opponents' strategies; that is to say, none of the players is willing to unilaterally change his/her strategy, given that the strategies chosen by all other players are fixed. Formally, if a set of pure strategies (a_i, a_{-i}) $(i \in I)$ is the strategy profile with $a_i \in AS_i$ stands for a pure strategy of player i and $a_{-i} \in AS_{-i}$ stands for joint pure strategy of other players except player i, a *pure Nash equilibrium* is a profile (a_i^*, a_{-i}^*) such that $\forall i \in I$,

$$g_i(a_i^*, a_{-i}^*) \geq g_i(a_i, a_{-i}^*), \forall a_i \in AS_i,$$
$$g_i(a_i^*, a_{-i}^*) \geq g_i(a_i^*, a_{-i}), \forall a_{-i} \in AS_{-i}.$$

In other words, the action a_i^* of player i is a best response to other players' strategies. The well-known prisoner's dilemma game has a pure Nash equilibrium. In this game, there are two players, two action spaces $AS_1 = AS_2 = \{\text{Cooperate}, \text{Defect}\}$ for player 1 and player 2, and the payoff matrices for both two prisoners are represented by a combined payoff matrix, as shown in Table 3.1.

	Cooperate	Defect
Cooperate	2,2	0,3
Defect	3,2	1,1

Table 3.1: A combined 2×2 payoff matrix of the prisoner's dilemma game.

it is to be noted that player 1 is the row player and player 2 is the column player. From Table 3.1, it can be seen that the likely outcome of the game is (Defect, Cooperate) (where player 1 plays "Defect" and player 2 plays "Cooperate"), with a payoff of "3" to player 1 and "2" to player 2, as verified by the Gambit software tool [95]. Therefore, the prisoner's dilemma game has a pure Nash Equilibrium, which is the action profile (Defect,Cooperate). However, there are also cases that there are many pure Nash equilibria exist or no Nash equilibrium exists. The

matching pennies game with a combined payoff matrix shown in Table 3.2 is an example of a game that does not have any pure Nash equilibrium.

	H	T
H	1,-1	-1,1
T	-1,1	1,-1

Table 3.2: A combined 2×2 payoff matrix of the matching pennies game.

A more generalized concept of equilibrium in strategic games is a *mixed Nash Equilibrium* [96]. The mixed strategy $\mathbf{x}_i^*$ for player i is a mixed Nash equilibrium strategy if for every player i

$$\mathcal{F}_i(\mathbf{x}_i^*, \mathbf{x}_{-i}^*) \geq \mathcal{F}_i(\mathbf{x}_i, \mathbf{x}_{-i}^*), \tag{3.3}$$

where $\mathcal{F}_i(\mathbf{x}_i, \mathbf{x}_{-i}^*)$ is a function for calculating player i's expected payoff when all players randomize according to the mixed strategy profile pair $(\mathbf{x}_i, \mathbf{x}_{-i}^*)$ (where $\mathbf{x}_i$ and $\mathbf{x}_{-i}^*$ are defined in Equation (3.1)). In the above mentioned matching pennies example (see Table 3.2), the mixed Nash Equilibrium is obtained when player 1 (the row player) chooses his/her actions (H,T) with a probability distribution of $\left(\frac{1}{2}, \frac{1}{2}\right)$ and player 2 (the column player) chooses his/her actions (H,T) with a probability distribution of $\left(\frac{1}{2}, \frac{1}{2}\right)$ (Nash equilibria are verified by the Gambit software tool [95]).

There are also some other equilibrium concepts, such as *correlated equilibrium* [92] and *trembling-hand pefect equilibrium* [71, 93]. A correlated equilibrium is randomised assignment of potentially *correlated* action recommendations to players, such that nobody will deviate. A trembling-hand perfect equilibrium is an equilibrium that takes into consideration the possibility of off-the-equilibrium play be assuming that the players's trembling hands may choose unintended strategies, although with a negligible probability. However, those equilibrium concepts are not suitable for the game covered in this thesis and are hence not considered.

3.3.2 Non-zero-sum Games

In non-zero-sum games, every player has his/her own individual payoff matrix and the sum of payoffs from their individual payoff matrix is not constant (and hence not zero) over the elements of matrices. Every player is aiming at maximizing his/her own expected payoff. In a

two-player non-zero-sum game, each player (either player 1 or player 2) has his/her own payoff matrix. Suppose these payoff matrices for player 1 and player 2 are

$$\mathbf{G}_1 = \begin{bmatrix} g_1(1,1) & g_1(1,2) & \cdots & g_1(1,m_2) \\ \vdots & \vdots & \ddots & \vdots \\ g_1(m_1,1) & g_1(m_1,2) & \cdots & g_1(m_1,m_2) \end{bmatrix}, \tag{3.4}$$

and

$$\mathbf{G}_2 = \begin{bmatrix} g_2(1,1) & g_2(1,2) & \cdots & g_2(1,m_2) \\ \vdots & \vdots & \ddots & \vdots \\ g_2(m_1,1) & g_2(m_1,2) & \cdots & g_2(m_1,m_2) \end{bmatrix}, \tag{3.5}$$

respectively (where m_1 and m_2 are the total number of actions for player 1 and player 2, respectively). And the payoff matrices $\mathbf{G}_1$ and $\mathbf{G}_2$ for player 1 and player 2 do not sum up to zero,

$$\mathbf{G}_1 + \mathbf{G}_2 \neq 0.$$

These payoff matrices in Equations (3.4) and (3.5) can also be written as one bimatrix. The payoff matrix in the prisoner's dilemma game shown in Table 3.1 is an example of such bimatrix, where the individual matrices for the two prisoners are

$\mathbf{G}_1 =$

	Cooperate	Defect
Cooperate	2	0
Defect	3	1

,

and

$\mathbf{G}_2 =$

	Cooperate	Defect
Cooperate	2	3
Defect	2	1

.

In a non-zero-sum game, there may be many Nash equilibria and the payoff of the game to each player is no longer unique as that in zero-sum games. For example, in the game called "Chicken", where two players drive very fast cars towards each other from opposite ends of a long straight road. The one, who swerves first, will be called "chicken". The bimatrix of the game is (suppose the first player is the row player and the second player is the column player)

	Swerve	Drive straight
Swerve	2,2	1,3
Drive straight	3,1	0,0

.

There are three different Nash equilibria for this chicken game (as shown in Table 3.3): the first player swerves and the second player drives straight; both players swerve or drive straight with a probability of 0.5; the first player drives straight and the second player swerves. As illustrated in Table 3.3, each Nash equilibrium corresponds to one game value for each player and those values are not unique: the first Nash equilibrium outputs "3" for the first player and "1" for the second player; the second Nash equilibrium outputs "1.5" for each player, and the third Nash equilibrium outputs "3" for the first player and "1" for the second player (game values are verified by the Gambit software tool [95]).

# of Nash equilibrium	Player 1		Player 2		Game value	
	Swerve	Drive straight	Swerve	Drive straight	Player 1	Player 2
1	1	0	0	1	1	3
2	$1/2$	$1/2$	$1/2$	$1/2$	$3/2$	$3/2$
3	0	1	1	0	3	1

Table 3.3: Nash equilibria and their corresponding game values in the chicken game.

3.3.3 Stochastic Games

A *stochastic game* [97] is a multi-stage non-cooperative game played in discrete time where, at each stage, the game is in one of many *states*, $s \in S := \{s_1, s_2, \cdots\}$. The game begins with a start state; the players choose actions and receive payoffs that depend on the current state of the game. The game moves into a new state with a probability that controlled by players' actions and the current game state. Stochastic games can be viewed as a generalization of MDP [98] to a multiplayer setting and an extension of repeated games to multiple states. An illustration of a stochastic game with four states (s_1, s_2, s_3, s_4) is depicted in Figure 3.2, where the (current) state

of the game determines the (current) payoff for each player (game dynamics). The text above (or below) the solid line in Figure 3.2 denotes the state transition probability. For example, when the game is in state s_1, the game has a probability of "0.6" to move to state s_2 and has a probability of "0.3" to stay at state s_1.

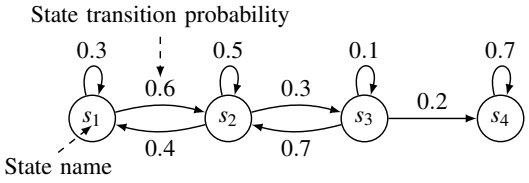


Figure 3.2: A stochastic game with four states.

The state transition probabilities and the immediate payoffs depend jointly on all players' actions. It is to be mentioned that the state transitions can be controlled by a single player or none of those players, but this thesis considers only the situations where the transitions are controlled jointly by all players. In a two-player non-zero-sum stochastic game, for each player (either player 1 or player 2) and each state $s \in S$, there are two $m_1 \times m_2$ matrices $\mathbf{G}_{\{1,s\}}$ and $\mathbf{G}_{\{2,s\}}$ associated, whose entries are given by $g_{\{1,s\}}(a,b) \in \mathbb{R}$ and $g_{\{2,s\}}(a,b) \in \mathbb{R}$, respectively. The payoff entry $g_{\{1,s\}}(a,b)$ (or $g_{\{2,s\}}(a,b)$) is received by player 1 (or player 2) when player 1 chooses his/her action $a \in AS_1$ and player 2 chooses his/her action $b \in AS_2$. Since there are many different states in the stochastic game, naturally there should be a transition matrix Q : $S \times AS_1 \times AS_2 \times S \to [0,1]$, which describes the probability $q(s'|s,a,b)$ that the game moves from a state $s \in S$ to another state $s' \in S$ when action a from player 1 and action b from player 2 are chosen. The transition matrix is defined as

$$Q := \{q(s'|s,a,b) \in \mathbb{R}_+ | s', s \in S, a \in AS_1, b \in AS_2\}.$$

A two-player stochastic game is played as follows. Suppose the game play is currently in state $s \in S$ and player 1 and player 2 play action a and action b, respectively. The players receive immediate payoffs $g_{\{1,s\}}(a,b)$ and $g_{\{2,s\}}(a,b)$ and the game play goes to next state s' according to the transition probabilities $q(s'|s,a,b)$. The expected payoffs of players are accumulated (typically with a discounting factor) through all stages of the game until the game stops. To make sure the game eventually ends (thus the game is finite), an assumption that the game in each state $s \in S$ has a positive probability to stop is made. This assumption guarantees

that the probability of infinite play is zero and the expected payoffs of players (with or without discounting factor) is finite [93].

In a two-player zero-sum game, one player wishes to maximise his/her own expected payoffs and the other player tries to minimise such payoffs. Suppose there are totally k ($k = |S|$) game states and these game states are independent on each other in the two-player stochastic game, we can define the vector of expected payoff $\mathbf{v} = (v_{s_1}, v_{s_2}, \cdots, v_{s_k})$, where v_s is the expected payoff (to player 1) in the state s ($s \in S$). With the above setting, each state can be specified as the starting point and the corresponding game element can be replaced by the value of state s ($s \in S$)

$$v_s = val(\mathbf{U}_s),$$

where the shorthand notation *val* denotes the value (in mixed strategy) of the zero-sum matrix game $\mathbf{U}_s$. The value of a game can be defined in terms of the *min-max* theorem. $\mathbf{U}_s$ is a $m_1 \times m_2$ matrix with entries given by

$$u_s(a,b) = g_s(a,b) + \sum_{\ell=1}^{n_s} q(s_\ell|s,a,b)v_{s_\ell}. \tag{3.6}$$

Equation (3.6) has two parts: the first one $g_s(a,b)$ is called as a short-term payoff and the second one $\sum_{\ell=1}^{n_s} q(s_\ell|s,a,b)v_{s_\ell}$ is called as a long-term payoff. In Equation (3.6), s_ℓ is the state that can be obtained from state s, v_{s_ℓ} is the game value at state s_ℓ, and n_s is the number of states that can be obtained from state s. The notion of Nash equilibrium extends naturally to stochastic games. In a two-player non-zero-sum game, let $\mathcal{H}_1(\mathbf{x}_1,\mathbf{x}_2) = \sum_{\ell=1}^{k_C} \mathbf{x}_{1,s_\ell} \cdot \mathbf{G}_{\{1,s_\ell\}} \cdot \mathbf{x}_{2,s_\ell}^T$ and $\mathcal{H}_2(\mathbf{x}_1,\mathbf{x}_2) = \sum_{\ell=1}^{k_C} \mathbf{x}_{1,s_\ell} \cdot \mathbf{G}_{2,s_\ell} \cdot \mathbf{x}_{2,s_\ell}^T$ denote functions representing the *total expected payoff* of player 1 and player 2, respectively, where the vector $\mathbf{x}_1 = \left(\mathbf{x}_{1,s_1}, \mathbf{x}_{1,s_2}, \cdots, \mathbf{x}_{1,s_\ell}, \cdots, \mathbf{x}_{1,s_{k_C}}\right)$ is a vector of mixed strategies for player 1 and the vector $\mathbf{x}_2 = \left(\mathbf{x}_{2,s_1}, \mathbf{x}_{2,s_2}, \cdots, \mathbf{x}_{2,s_\ell}, \cdots, \mathbf{x}_{2,s_{k_C}}\right)$ is a vector of mixed strategies for player 2. A pair of strategy $(\mathbf{x}_{1,s_\ell}^*, \mathbf{x}_{2,s_\ell}^*)$ constitutes a Nash equilibrium point for state s_ℓ ($s_\ell \in S$ and $\ell \in \{1,2,\cdots,k_C\}$) if and only if

$$\mathcal{H}_1(\mathbf{x}_1^*,\mathbf{x}_2^*) \geq \mathcal{H}_1(\mathbf{x}_1,\mathbf{x}_2^*),$$
$$\mathcal{H}_2(\mathbf{x}_1^*,\mathbf{x}_2^*) \geq \mathcal{H}_2(\mathbf{x}_1^*,\mathbf{x}_2),$$

where the vector $\mathbf{x}_1^*$ for player 1 is composed of all mixed strategies from Nash equilibrium and it is defined as $\mathbf{x}_1^* = \left(\mathbf{x}_{1,s_1}^*, \mathbf{x}_{1,s_2}^*, \cdots, \mathbf{x}_{1,s_\ell}^*, \cdots, \mathbf{x}_{1,s_{k_C}}^*\right)$. Similarly, the vector $\mathbf{x}_2^*$ for player 2 is $\mathbf{x}_2^* = \left(\mathbf{x}_{2,s_1}^*, \mathbf{x}_{2,s_2}^*, \cdots, \mathbf{x}_{2,s_\ell}^*, \cdots, \mathbf{x}_{2,s_{k_C}}^*\right)$.

3.3.4 Bayesian Games

Bayesian games (also known as games with incomplete information) are a branch of game theory that consider scenarios where decision makers have some uncertainty about the underlying game state, their types or preferences, etc [99]. In a Bayesian game, it is necessary to specify the strategy spaces, state spaces, payoff functions, and beliefs about the state for every player. The probabilistic analysis of Bayes' inference rule is used to update players' beliefs during the game process, and hence, such developed games are called Bayesian games. Bayesian games relax the assumption that all information of the game is common knowledge among all players and each player knows complete information of the game.

The idea of Bayesian games is tremendously important in capturing the overwhelming majority of real-life scenarios where players may have private information about payoffs, their opponents, and strategies, etc. A player has some beliefs, namely prior distributions, about parameters (e.g., payoffs, player's type, current state of the game, etc) which he/she is uncertain. Those beliefs are mutually relevant, since they affect each other. For example, a player has beliefs about the beliefs of other players.

A *Bayesian Nash Equilibrium (BNE)* is a Nash equilibrium of a Bayesian game. For illustrative purposes, consider two persons of different types (in terms of strong or weak) are fighting with each other. Suppose that the column player has uncertainty about the type (i.e, strong, weak) of the opponent he/she faces and both players know the game payoffs. Example payoff matrices for both players with two types of the row player are described as

	Fight	Not
Fight	1, -2	2,-1
Not	-1,2	0, 0

, and

	Fight	Not
Fight	-2,1	2,-1
Not	-1,2	0,0

.

Type=**Strong** Type=**Weak**

The row player knows whether he/she is strong (compared to his/her opponent) or not with a belief ρ. A belief is a probability distribution. For example, the belief ρ can be $\rho = (p, 1-p)$, where the probability p means that the row player believes he/she is strong (compared to his/her opponent) and the probability $1-p$ means that the row player believes he/she is weak (compared to his/her opponent). While the column player does not know such a belief. Therefore, this sample game plays with asymmetric information among both players. The BNE

can be found based on the belief value p. Here this thesis gives out one example on finding one such equilibrium when the row player is always fighting. The probability that the row player is strong is denoted as p. Such that no matter whether the row player is strong or not, if the column player chooses to fight, he/she will receive a payoff $g_2(\text{Fight}, \text{Fight}) = (-2) \cdot p + 1 \cdot (1-p)$; if he gives up fighting, his/her payoff will be $g_2(\text{Fight}, \text{Not}) = (-1) \cdot (p) + (-1) \cdot (1-p)$. If he chooses not to fight whatever the row player is, to maximise his/her own payoff, the payoff received from action "Not" should be greater than that received from action "Fight". Therefore, $g_2(\text{Fight}, \text{Not}) > g_2(\text{Fight}, \text{Fight})$ should be satisfied. In summary, in this case, if the column player guesses the probability that his/her opponent is strong is greater than $\frac{2}{3}$, the Bayesian Nash equilibrium is (Fight, Not) for any type of the row player.

3.4 Quantitative Cyber Threat Assessment Framework

This thesis proposes a stochastic game-theoretic cyber threat assessment framework to capture the fundamental characteristics of adversarial interactions between the attacker and the defender in smart grid communication networks. In these networks, the attacker knows the type and location of compromised communication nodes, although it may be impossible for the defender to have full knowledge about compromised nodes and the action spaces of the attacker. However, the defender knows about the resource characteristics (e.g., current and planned controls) of the system. In this case, the type of the game changes to an asymmetric information game. For a multistage attack, the success of the previous step usually provides occurrence conditions for the next step; and such situations are covered by a stochastic game. Therefore, a stochastic game-theoretic model with asymmetric information is designed in this thesis for the quantitative cyber threat assessment framework.

The stochastic game-theoretic model presented in this thesis is intended to be a general and intuitive framework, which models representative stakeholders, their objectives, and their typical interactions in smart grid communication networks. The objective of this quantitative cyber threat assessment framework is to assess attack scenarios at an early stage of multistage attacks and to capture cascading effects of multistage attacks at every stage. As a consequence, optimal proactive defence countermeasures can be suggested to defeat or mitigate future attacks, while security incidents, which have the potential to cause safety-related events (e.g., a loss of human life), can be avoided. This section provides a dictionary of terminologies and characteristics in the proposed stochastic game-theoretic cyber threat assessment framework, elaborates

assumptions that are made in relation to realistic scenarios, and reviews the implementation steps of the proposed stochastic game-theoretic cyber threat assessment framework.

3.4.1 Terminologies and Characteristics

- **Attacker:** A person whose intention is to disrupt the normal functionality of the smart grid (including both power grids and communication networks). This can be an inside or an outside attacker. Malware and other tools used to perform attacks are considered as attack vectors, but not as the attacker him/herself.

- **Defender:** A system administrator who is responsible for deploying defence countermeasures (e.g., intrusion prevention/detection systems) to protect hosts in a system.

- **Two player:** This refers to two decision makers in a game. In this stochastic game-theoretic threat assessment framework, the two players in the games are the attacker and the defender. The physical appearance of either player can be diverse, that is, the defender can be an entire team of people, just as the attacker can be a team of cooperating physical entities. The "players" are, however, considered as the respective team (irrespective of their physical form).

- **Positive stop probability:** This refers to the probability that a game will go to end in any state of a stochastic game is positive.

- **Non-zero-sum:** If a game has not ended, in each state of the game, the payoffs of the attacker and the defender do not sum up to zero because of the presumably different goals of the two players.

- **States and stages:** In stochastic games the play proceeds by steps from state (or position, in Shapley's language [97]) to state. At each stage of a game, the game play is in a given state.

- **Simultaneous game:** At each game stage, one player makes his/her decision on which action to take without any prior knowledge of the other's decision on actions. In this context, "simultaneous" does not mean that both players will choose their actions at the same time; rather, it means that one player does not know what action the other player will choose when he/she is making his/her action decision. The time point for the attacker

to take an action can be a certain point or a certain interval in time. This thesis assumes that both players simultaneously take action only at discrete time instants.

- **Asymmetric information:** Each player has *different* information about the system under threat and the *current* state of the game. For example, the attacker knows his/her attack vectors and whether a host in the system is compromised, while the defender does not have such information.

- **Perfect recall:** Both the attacker and the defender will never forget anything once acquired. This thesis deals with the case that, at any stage of a stochastic game, both players remember all past actions chosen by them at all previous game stages.

- **Interdependency cascading failures:** These kinds of failures result from the interdependent nature of the coupled power grids and communication networks. They are also called vertical failures in this thesis.

- **Node overloading cascading failures:** These kinds of failures result from the overloading of distribution substations, where the initial node overloading can be caused by interdependency cascading failures. The load of the overloaded distribution substations is redistributed to their neighbouring operational distribution substations, which will also fail, in turn, a failure cascades among the power grid. These failures are also called horizontal failures in this thesis.

3.4.2 Assumptions

The assumptions made by a model have a direct effect on the analysis of threats and can possibly lead to unreliable assessments if those assumptions are unrealistic. The effect caused by an unreliable threat assessment includes a false sense of security, inefficient defence countermeasure deployment or, even worse, cyber security incidents and safety-related events. Hence, for the sake of accurate threat assessments, objective and fair assumptions need to be made to keep them as close to a real-world scenario as possible.

In order to facilitate the proposition of a stochastic game-theoretic cyber threat assessment framework, this thesis first makes the following assumptions about the smart grid. It assumes there are two types of communication nodes in the smart grid communication network: information relay nodes and control centres. Information relay nodes are IEDs that send the monitored data to control centres and transmit commands from control centres to distribution

substations in power grids. Control centres are powerful computers, besides monitoring power nodes, which collect information from adjacent IEDs and make electricity controlling decisions. Since this work focuses on medium- to low-voltage power grids, it is assumed that there are generators (most of them are renewable energy resources) and distribution substations in the power grid, while only distribution substations can directly provide electricity to communication nodes (information relay nodes and control centres).

Although there may be scenarios with multiple attackers versus multiple defenders, the stochastic game described in this thesis is modelled as a two-player game, in which all of the attackers are treated as one player, as are all of the defenders. In this thesis, without loss of generality, it is assumed that the action spaces for both players are the same in every game state. One player (either the attacker or the defender) can observe the actions that have been taken by the other, which further means that both players have perfect recall. However, as discussed at the beginning of this section, both players have asymmetric information about the current state of the system under attack/defence. No player has full knowledge of the current game state; nevertheless, each player keeps a local private game state about the game play. Although one player has uncertainty about the local private game state of the other player, he/she has a probability distribution of the local private state of the other player and can use his/her observations of the other player's actions during game play to eventually learn about the local private state of the other player. The game to capture interactions between the defender and the attacker is assumed to be finite, since the game will end with a probability of one, where either the attacker arrived at his/her target or the defender detected the attacker and broke the attack chain. The finite game assumption holds for realistic scenarios, since every multistage attack has a few finite steps. It is also assumed that, at each stage, the probability that the game will end is positive. This is a valid assumption, as will be discussed in Section 4.1. Though the attacker launches an attack by exploiting vulnerabilities, the game-theoretic model does not account for the time interval of vulnerability exploitations. More significantly, the cyber threat assessment for insider attacks is not considered as it is beyond the scope of this thesis.

3.4.3 Quantitative Cyber Threat Assessment Framework Overview

The stochastic game-theoretic cyber threat assessment framework proposed in this thesis models interactions between the attacker and the defender from a technological point of view. It also elaborates detailed ingredients needed to model such interactions. Threat assessment (which is depicted in Figure 2.1) covers the first few steps of the risk assessment process, which is

ISO/IEC 27005 threat assessment		Stochastic game-theoretic cyber threat assessment	
Process step	Terminology	Process step	Description
Risk Identification	Identification of assets	1. Attack scenario investigation	A network knowledge library collects all the possible states of the communication network in smart grids
	Identification of vulnerabilities		
	Identification of threats		
	Identification of current and planned controls	2. Player identification	Tow players: the attacker and the defender
		3. Action space determination	The action space and cost of each actions are determined for each player
		4. Game state space identification	All the possible states of involved communication nodes in the investigating attack scenario constitute the game state space
		5. State transition probability determination	The probability from one state to another depends on the joint actions of both players and on whether the attack action will succeed
Impact assessment	Assessment of consequences	6. Players' payoff formulation	The payoff of each player is formulated from the disruptive effects of cyber attacks in the physical power grid, impact of the attacker's action on information security, and the cost of taking actions
Likelihood assessment	Assessment of incident likelihood	7. Control recommendation	Probability for actions of each player is computed for each game state

Table 3.4: Mapping between threat assessment in ISO/IEC 27005 standard and the stochastic game-theoretic cyber threat assessment process.

the first process in risk management methodology. The quantitative cyber threat assessment process, which is included in the stochastic game-theoretic cyber threat assessment framework, is strongly related to the information security risk management process as standardized in ISO/IEC 27005. The reason for relating the threat assessment process to the ISO/IEC 27005 is to avoid redefining an overall novel set of process steps; instead, this thesis are tailoring an existing approach to the smart grid communication network. Additionally, the risk assessment process in the ISO/IEC 27005 standard is familiar to the information security community. The cyber threat assessment framework proposed in this thesis is based on a stochastic game-theoretic model. Game theory can help with the implementation of the cyber threat assessment framework, since the latter framework requires the selection and planning of controls and an effectiveness check on those controls. All of these implementation steps can be supported by game theory. It has been shown that all the steps of the ISO/IEC 27005 standard can be mapped to the steps in the game-theoretic model [100]. This thesis focuses on threat assessments for multistage cyber attacks in smart grid communication networks. Therefore, it has made some changes to the overall threat assessment process covered in ISO/IEC 27005 standard in order to reflect the specific challenges of cyber threat assessment for multistage cyber attacks in smart grid communication networks. Adapted from the work in [100], Table 3.4 presents a mapping sketch between threat assessment in ISO/IEC 27005 standard and the stochastic game-theoretic cyber threat assessment process in smart grid communication networks. It should be noted that this work is not going to elaborate "what" is defined in the overall threat assessment process, rather, it focuses on describing "how" those main topics in the overall threat assessment process are implemented. In the following, this thesis will review the implementation steps of the stochastic game-theoretic cyber threat assessment framework:

Step 1: Attack scenario investigation

This step involves a network knowledge library to collect all the possible states of the communication network in smart grids. This information includes the topology and assets (also called nodes in this thesis) of the targeted smart grid (including the power grid and the communication network), vulnerabilities of nodes (already publicly known, as well as zero-day vulnerabilities, which are scanned by Nessus, Snort etc) in the smart grid communication network, network connectivities, current and planned controls, and vulnerability dependencies, as shown in Figure 3.3.

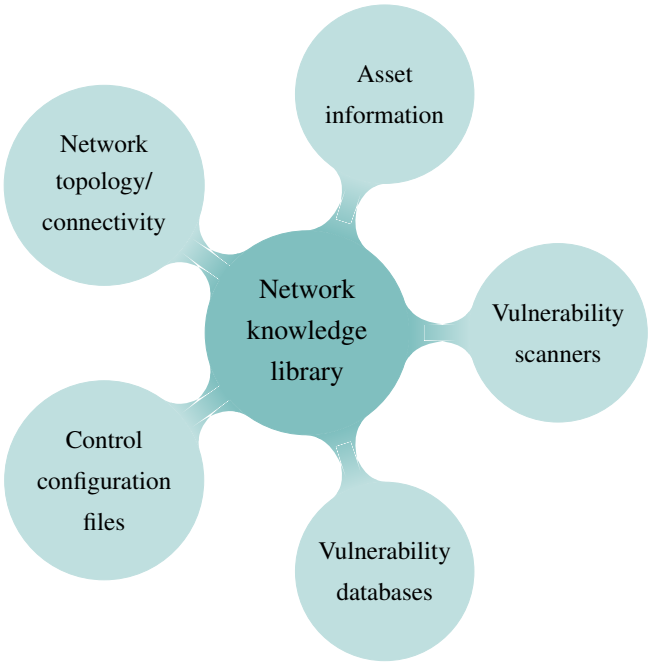


Figure 3.3: Network knowledge library for attack scenario investigation.

Step 2: Player identification

This thesis collects all physical existing opponents into a single adversary, who is called the attacker and acts as player 2 in the game. Correspondingly, all system administrators and security operators represent the defender, who acts as player 1.

Step 3: Action space determination

To keep matters of presentation simple, the (non-exhaustive) action space AS_1 for the defender is $AS_1 = \{\text{Email-filter configuration, Intrusion detection system (IDS) deployment, Patch}\}$. Email filters can be configured on the corresponding communication nodes. Email filtering refers mostly to the automatic processing of incoming emails, but it can also be applied to outgoing emails as well as that have been received. An IDS can be deployed in a network-based or node-based manner to help the defender to see whether there has been any activity that could result in the compromise of the monitored communication nodes. "Patch" denotes the action of applying a patch to a vulnerability in order to remove the option for the attacker to use an exploit for that vulnerability. Correspondingly, the (non-exhaustive) action space AS_2 for the attacker is $AS_2 = \{\text{Exploit, Do nothing}\}$. "Exploit" means that the attacker launches an attack

by exploiting an vulnerability, while “Do nothing” refers to the action whereby the attacker does not launch a further attack, but conceals him/herself in order to guarantee enough time to test and validate attack capabilities for his/her next exploits. Besides, the cost of taking any action is also estimated by the corresponding player.

Step 4: Game state space identification

After actions are taking from both players, the game is played from one state to another. All the possible states of involved communication nodes in the investigating attack scenario constitute the game state space S. The state of a node ℓ in the communication networks contains two parts: a working state $\phi_N(\ell)$ and a defence state $\theta_N(\ell)$ at any stage N of the system. Throughout this work, N takes values from $\mathbb{N}$, which is the set of natural numbers. The working state $\phi_N(\ell)$ for a communication node ℓ at stage N can be either “normal" or “malfunctioning", meaning that node ℓ either has a normal operational state or is malfunctioning at stage N. Meanwhile, the defence state $\theta_N(\ell)$ of node ℓ refers to the defence countermeasures assigned to the node at stage N. For example, if a communication node is deployed with an IDS at stage N, then $\theta_N(\ell)$ is “IDS".

Step 5: State transition probability determination

The probability that the game state will transition from one to another depends not only on the joint actions of both players, but also on whether the attack action will be successful, meaning that the attacker has the motivation to launch attacks. Whether an action from the attacker will succeed relies on his/her capabilities and the available exploitable vulnerabilities of an asset. Depending on exploitable vulnerabilities, there are cases where there is no transition between certain states. In the cyber threat assessment framework, both players take their actions simultaneously, while state transition probabilities are common information shared between them.

Step 6: Players’ payoff formulation

Every player has a payoff matrix in each state of game play. For a game state $s \in S$, this work assigns a payoff value $g_{\{1,s\}}(a,b) \in \mathbb{R}$ to each action profile $(a,b) \in AS_1 \times AS_2$ for the defender, and assign a payoff value $g_{\{2,s\}}(a,b) \in \mathbb{R}$ to each action profile $(a,b) \in AS_1 \times AS_2$ for the attacker. Multistage cyber attacks in smart grid communication networks can cause not only cyber damage to the communication network, but also cause disruptive events in the

power grid. Due to their interdependency, a disruptive event in the power grid can lead to further failures in the communication network, resulting in a cascading failure. Besides, each player (either the defender or the attacker) incurs a certain cost to perform an action. Therefore, players' payoffs are composed of three parts:

1. The cyber disruption metric $M_c = t_d \cdot \underbrace{\left(w_P^{\{i_1\}} \cdot m_P^{\{i_1\}} + w_P^{\{i_2\}} \cdot m_P^{\{i_2\}} + \cdots + w_P^{\{i_{n_{P,\infty}}\}} \cdot m_P^{\{i_{n_{P,\infty}}\}} \right)}_{u_{P,\infty} \text{ failed power nodes}}$ $\in \mathbb{R}_+$, which quantifies the three primary characterizations (identified by ENISA [101]) of the impact of cyber attacks (i.e., disruptive events) on physical power grids. The three characterizations of scope, magnitude, and time are quantified as $u_{P,\infty}$ (the total number of failed power nodes from the beginning until the steady state of the cascading failure propagation process), while $m_P^{\{i_\ell\}} \in [0,10]$ ($\ell \in \{1,2,\cdots,n_{P,\infty}\}$ and $m_P^{\{i_\ell\}}$ denote the disruption magnitude of the node $v_P^{\{i_\ell\}}$) and the time duration the disruptive events t_d, respectively. The power node weight $w_P^{\{i_\ell\}}$ of node $v_P^{\{i_\ell\}}$ and all other parameters of the cyber disruption metric M_c are defined in Chapter 5. The units for the quantified time characterization should be chosen carefully, depending on the application. They are suitable and compatible with other units.

2. The information metric impact $I_b = \text{Con}_b \cdot \alpha + \text{Int}_b \cdot \beta + \text{Ava}_b \cdot \delta \in \mathbb{R}_+$ measures the impact of action $b \in AS_2$ from the attacker on the information security of communication nodes. α, β, and δ are communication nodes' assets in terms of confidentiality (C), integrity (I), and availability (A), respectively. Con_b, Int_b, and Ava_b are the relative impairment degrees that the action b has made in the confidentiality, integrity, and availability of communication nodes.

3. The cost of taking actions. The cost is not necessarily monetary and its units are suitable for the application. The cost for the attacker or the defender of performing an action is captured as the lot of implementation costs and /or the management costs of the action.

The type and the number of failed nodes (both failed power nodes and failed communication nodes) needed in both the cyber disruptive metric M_c and the information impact metric I_b are captured through a detailed mathematical analysis of the cascading failure propagation in an interdependent power and communication network. Both interdependency failure and node overloading failure propagation are taken into account in order to understand the cascading effects of multistage attacks in smart grids.

Step 7: Control recommendation

The game model is solved in this step, resulting in a mixed Nash equilibrium point for each game state. Nonlinear programming (NLP) is studied to formulate the stochastic game of the attacker and the defender in the smart grid communication network in one-stage and two-stages games, then extending to M-stage games ($M \in \mathbb{N}$). By finding probabilities for each of the strategies regarding both the attacker and the defender in each state, the optimal strategies for risk mitigation at each state will be recommended to the defender so as to better manage the network defence resources.

3.5 Summary

This chapter discussed the possibilities of applying game theory for network cyber security assessment, presented preliminaries of game theory, and reviewed the stochastic game-theoretic cyber threat assessment framework, as proposed in this thesis. The presented threat assessment process is strongly related to the information security risk management process given in the ISO/IEC 27005 standard, which is a well-defined approach that is familiar to the information security community. Nevertheless, cyber threat assessment is tailored to address the specific challenges (presented in Section 1.4 of Chapter 1) of performing threat assessments for multistage cyber attacks in smart grid communication networks. This chapter presented implementation steps of the stochastic game-based cyber threat assessment, which can serve as guidance for practitioners to follow when performing risk assessments in their organizations. This stochastic game-theoretic cyber threat assessment framework can also be integrated into existing risk management processes that are already running in smart grids, or more specifically, a set of smart grid use cases. The following chapter will investigate the designing of the stochastic game-theoretic model, which is the core part of the proposed stochastic game-theoretic cyber threat assessment framework.

Chapter 4

Designing a Stochastic Game-Theoretic Model for Smart Grid Communication Networks

4.1 Introduction

Network security is a critical concern with regard to cyber-physical systems. For a long time, security operators have been interested in knowing what an attacker can do to a cyber-physical system and what can be done to prevent or counteract cyber attacks [86, 102]. It is suggested that risk assessment must be integral to the overall life cycle of the smart grid systems. A major aspect of risk assessment is identifying threats and assessing attack scenarios. Attack scenarios are dynamically changing in smart grid communication networks, for example, because of existing of legacy and new systems in smart grid communication networks. Many current threat assessment methods are catalogue-based approaches, which provide checklists, constraints and scoring spreadsheets to deterministically evaluate a system. Unfortunately, catalogue-based approaches provide nothing more than general guidelines, best practice or advice on how to be more secure. If the system administrator alters the system to mitigate risks of multistage cyber attacks in smart grid communication networks, without the availability of a catalogue, catalogue-based approaches provide no suggestions as to which changes would be more secure. Other methods, such as the threat assessment process defined in the HMG IS1 risk assessment standard [26], completely ignores (from a technical point of view) the equipment in place, referring only to the motivation and capabilities of an attacker to derive a threat

level. Besides, logic- and graph-based approaches are proposed for finding attack paths and attack scenarios. However, the majority of existing logic- and graph-based approaches (most of which are reviewed in Chapter 2) do not take into account known and new attacks based on zero-day vulnerabilities. An extension of anticipation games, which are the most attack graphs that have evolved available to date, can mitigate zero-day exploits; however, their rules can be arbitrarily complex.

Multistage cyber attacks, as important threats in smart grid communication networks, make use of a variety of different exploits, propagation methods, and payloads, resulting in the emergence of many more sophisticated cyber attacks. Current protection mechanisms, which rely on isolation techniques, such as firewalls, data diodes, and zoning concepts, are not sufficiently applicable in cyber-physical systems. For more than a decade, game-theoretic approaches have been recognized as useful tools to handle network attacks [84, 103, 104, 105]. Significant results from game theory concerning cyber situation awareness and network security risk assessment in conventional ICT systems have been reported [72, 86]. But the application of game theory for the assessment of threats from multistage cyber attacks and the prediction of an attacker's actions in smart grid communication networks are still in their infancy nowadays. Cyber attacks on smart grid communication networks can cause physical damage to the power grid; however, the physical impact of cyber attacks on power grid has not been fully analysed. Many existing stochastic game-theoretic threat assessment methods assume symmetric information among the players, which implies that all the players share the same information, i.e., the same signal observed and the same knowledge about states/payoffs in a game. However, in many situations, this assumption is unrealistic. There are many games arising out of communication networks, electronic commerce systems, and society's critical infrastructures involving players with different kinds of information about the game state and action processes over time [106, 107, 108]. For instance, in cyber-security systems, the attacker knows his/her own skill set, while the defender knows the current and planned resource characteristics of the system. In short, the attacker and the defender do not share their available information with each other.

This thesis attempts to design a stochastic game-theoretic model with asymmetric information and positive stop probabilities in order to assess the threat of multistage cyber attacks in smart grid communication networks. The positive stop probability means that the probability of the game to end at any state is positive. Unlike random failures, attackers have motivations and capabilities to launch further attacks. Both the attacker and the defender will act in consideration of the consequences of their corresponding actions, with such consequences including

satisfactions, risk versus effort, and effectiveness. In each state of the game, if launching a further attack would have limited benefits, and take months of time and huge amount of computers and memory, the attacker will most probably stop his/her attack. Once the defender observed these phenomena regarding the attacker, he/she will not deploy any corresponding countermeasures. Therefore, this situation will be accounted for by adding a stop probability to the stochastic model; and such a stop probability is positive. This model permits us to take into account the common knowledge about the system that is available to both the attacker and the defender in terms of security assets (i.e., nodes in the communication network) and vulnerabilities (including both publicly known and zero-day vulnerabilities, see Section 4.3.1 for a detailed description of vulnerabilities covered in this work). The designed stochastic game-theoretic model extends an existing stochastic game-theoretic model with specific characteristics of attacker-defender interactions in smart grid communication networks. The objectives of this attacker-defender stochastic game-theoretic model is to assess attack scenarios at an early stage of the attack, where the defender makes correct optimal proactive defence decisions. Therefore, a defense system can be prewarned, security resources can be better allocated to defeat or mitigate future attacks, and security incidents can be avoided. This thesis considers the worst-case scenario where the attacker has complete knowledge of the architecture/infrastructure of the system and hosts' vulnerabilities in the system, and the attacker has full knowledge of the target smart grid defense configurations. In Section 4.2, the game framework is established, with a description of multi-stage attacks. While Section 4.3 presents an attacker-defender stochastic game-theoretic model to represent the attacker-defender interactions. Section 4.4 analyses the belief-updating mechanisms and the feasible computation of Nash equilibria. Finally, Section 4.5 summarizes the chapter.

4.2 Description of Multistage Cyber Attacks

As a single act of cyber attacks is often not sufficient for an attacker to reach his/her ultimate goal, multiple stages from attack preparation and network penetration to the final attacks often occur (see the attack scenarios described in Chapter 1). ICS-CERT received a total of 245 reported incidents across all sectors in 2014, with multistage APT account representing roughly 55% amongst other cyber attacks against ICS [109]. Different assets in the smart grid can be targets at various stages of the attack. Nevertheless, communication is always seen as an enabling factor for every attack [110]. For example, a man-in-the-middle (MITM) attack can

be performed on protocols used for data communication in smart grids (e.g., IEC61850). With the lack of authentication facilities, the attacker tricks the communication nodes into believing they are directly talking to each other. A successful attack allows the attacker to "sniff" network traffic, alter network packets, drop network packets, or even inject false network packets. For any successful multistage attack, the common threat of the attacker, who wishes to penetrate a smart grid, will always the utilization of vulnerabilities in the smart grid communication infrastructures. Vulnerabilities exist in devices and services (such as routers, switches, and protocol gateways) supporting the function in the network. Meanwhile, a growth in networks and communication protocols used throughout ICS networks posing vulnerabilities has been observed [111]. The possible number of attack steps and the complexity of conducting an effective and successful attack depend on the criticality of the target and thus its cyber security protections. For example, a ICS cyber kill chain is composed of two stages and several steps in each stage [112]. Figure 4.1 shows the general stages involved in a multistage cyber attack in smart grids, which exploit vulnerabilities in the communication network. Each stage shown in Figure 4.1 is elaborated in the following, with examples of an attacker planning to pursue his/her (sub)target.

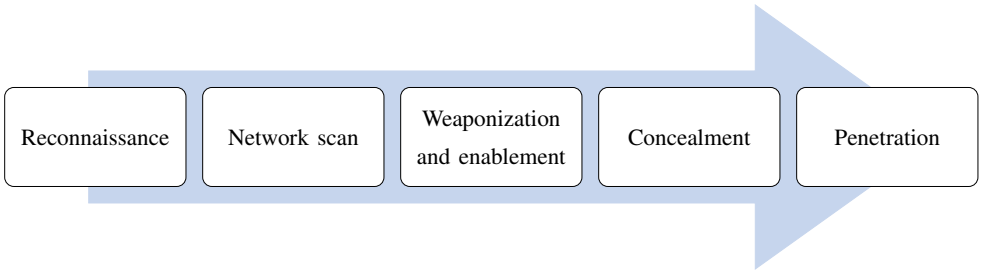


Figure 4.1: General stages involved in a multistage cyber attack.

Reconnaissance: It is the first step in any cyber attack to gather as much information as possible (including organizational structure, operation system and software versions, operator personnel, and vulnerable hosts in the network) about the target without engaging with the target infrastructure. A list of manufacturer default passwords for over 100 ICS products was released in January 2016 [113]. Many of these products were from big-name vendors (such as Allen-Bradley, Schneider Electric, and Siemens). Those products could be found in most utility ICS, while their passwords were left unchanged by utility operators. This step is the identification of a suitable entry point(s), which is either inside or connected to the targeted system.

Network scan: Once an entry point is (or entry points are) identified, the attacker will scan the network architecture to identify assets and hosts in the network. Besides, an attacker would perform network mapping and discovery (e.g., network connectivities, open ports, protocols in use, and exploitable vulnerabilities) in order to determine which tool is (or tools are) needed to reach a (sub)target. Internet Control Message Protocol (ICMP) can be used to gather additional system information [110].

Weaponization and enablement: The weaponization step focuses on the Trojanization of a genuine application, document or file with malicious code. An attacker can exploit a chosen attack vector, for example Metasploit [1]. Alongside technical means, social engineering techniques such as spear phishing (a technique whereby an attacker uses emails to lure a victim to open attachment files or links to download malware, or the attacker is provided with unauthorized access to a computer, an application or even a network), are often successful (spear vectors accounted for the most common attack vectors in 2014 and 2015, according to ICS-CERT [109]; meanwhile, it has been claimed that, in 2016, 91% of cyber attacks started with a phishing email[2]). The BlackEnergy attack on Ukrainian power companies was based on spear phishing. An attacker often establishes multiple additional paths, via network connectivity exploration, to ensure access in case one of the paths is detected or removed.

Concealment: Once malware is successfully injected and executed, the next step is to be disguised and remain undetected by defence mechanisms or the targeted system. Concealments guarantee enough time for an attacker to make use of findings about discovered ICS equipment to "tailor" an attack capability, and to test and validate the selected attack capabilities before final execution in order to get the best results. Many companies lack effective intrusion detection and/or are unaware of these kinds of activities in their systems. A 2016 SANS survey reported that 26.6% of respondents were not aware of any infection or infiltration in their control system networks, while only 27% of respondents indicated that their control system network had been infected or infiltrated [114].

Penetration: This concerns the actual execution of various attack vectors to penetrate and disrupt the smart grid. An attacker can launch a MITM attack in the context of smart grid communications. Based on a MITM attack, the attacker can perform eavesdropping, modification, injection, and DoS. An effective attack on the smart grid can result in the loss of electricity

[1] http://www.metasploit.com/ (Retrieved: 23/06/2017)

[2] http://www.darkreading.com/endpoint/91–of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704 (Retrieved: 23/06/2017)

generation or transmission for a long period, while an extreme consequence could involve the loss of life.

The above-mentioned multiple stages of an attack are covered by the prerequisite that there is only one decision maker, the attacker, while all the security countermeasures are assumed to be either ineffective or not deployed at all. Hence, the attacker can successfully perform all stages and finally obtain his/her target. However, in realistic scenarios of smart grids, security operators are more and more aware of cyber security in smart grid communication networks, while corresponding security countermeasures are deployed and operational in specific places. Therefore, the attacker has the probability to be detected or removed by the defender at every stage of his/her attack process. The issue between the attacker and the defender is how to select their attack/defence actions against each other. This naturally goes to a game between the attacker and the defender.

4.3 Attacker-defender Stochastic Game-theoretic Model

To assess threats of multistage attacks, the strategic interaction of the attacker and the defender is modelled as a stochastic game (which covers the step occurrence dependency in multistage attacks). The goal is to design an attacker-defender stochastic game-theoretic model to capture the characteristics of the interactions of the attacker and the defender in smart gird communication networks. In such a game, the possible actions of the players are restricted, such that there exists an equilibrium point in which the attacker has no chance to successfully obtain his/her ultimate goal. This section introduces node vulnerability, action spaces, state spaces, and state transition probabilities of the game between the attacker and the defender. This work designs the attacker-defender stochastic game-theoretic model by a description of an existing stochastic game model and an extension of this model according to the characteristics of the interactions of the attacker and the defender.

4.3.1 Node Connectivity and Vulnerability Identification

Understanding the network connectivity and the interaction between nodes in a complex system, such as smart grids, is crucial, as node connectivities/interactions are the main enablers for malware propagation and network-based attacks. A connectivity exists if two nodes engage in any form of data exchange, either physically or logically. A physical connectivity exists if there is a physical medium between those two nodes, while a logical connectivity may include

the file transfer from an external node (e.g., computer) to a node in the corporate network using a USB flash drive. A general way to identify nodes and their connectivities is the application of a conditional connectivity graph or the analysis of the smart grid architecture diagram provided by the utility provider.

Underlying the model presented here is the concept of vulnerability exploitation. Vulnerability alone does not introduce any risk, but vulnerability under threats is another story. A vulnerability is a flaw or weakness in a system's design, implementation, or operation and management, which can be exploited to compromise the information security of a node [115, 116]. In this work, vulnerabilities refer to software vulnerabilities, which include publicly known and zero-day vulnerabilities. For example, a buffer overflow vulnerability with an identifier of CVE-1999-0018 is one kind of vulnerability covered in this work. Other vulnerabilities caused by disgruntled employees or natural disasters are not taken into account. Additionally, social engineering vulnerabilities are not exclusive to this thesis. A vulnerability can be exploited by an attacker or patched by a defender. Due to the complexity of a communication network (e.g., complex mix of legacy systems and new components) in smart grids, it is difficult to guarantee that a node does not contain any vulnerabilities. A node in a communication network in smart grids may associate with a set of vulnerabilities. The vulnerability data can be collected by active and/or passive scanners (e.g., Nessus and Snort). If a vulnerability is too difficult for an attacker to exploit, or the perceived benefit for an attacker is too small, this vulnerability is tolerable [117]. Removing all vulnerabilities is usually impractical; on the other hand, leaving vulnerabilities unattended may cause significant damage to critical security assets in a networked environment. A vulnerability could be discovered by the attacker, who can exploit it in order get closer to his/her ultimate target. It could also be discovered by security researchers (security operators) or the software company itself, who may publicly disclose the existence of the vulnerability and quickly release a patch. Exploitations can still be developed for vulnerabilities that have been disclosed or patched. It is also possible that an exploit discovered by the attacker may go undisclosed and unpatched for a significant amount of time. Once an exploit is developed, a system running the vulnerable software can potentially be compromised by attackers until a patch is created and applied to the system. It is assumed that this attacker-defender stochastic game-theoretic model does not account for the time interval of any two vulnerability exploitations. However, whether the vulnerability exploits lead to the node compromise depends not only on the capabilities of the attacker, but also on the defence countermeasures (e.g., intrusion prevention/detection systems, firewalls) of the system. Multistage

attacks, taking advantages of interdependency among vulnerabilities, exploit several vulnerabilities across multiple hosts in the system before reaching their ultimate target. An example of multiple vulnerability exploitation across multiple stages/hosts can be a Stuxnet-like attack, which targets Siemens programmable logic controller (PLC). For the sake of simplicity, this work only considers a subset of the complex capabilities of Stuxnet-like attacks (targeting a PLC), as presented in Figure 4.2. In this figure, each node represents a host, with the solid edges without text in the middle denoting network connection links (a bidirectional communication link is considered as a pair of incoming and outgoing edges) and the solid edges with text in the middle being vulnerability exploitations with corresponding vulnerability, associated with either or both communicating node(s).

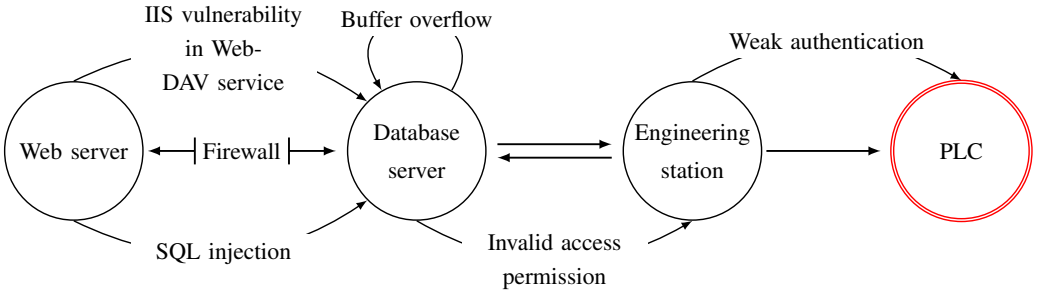


Figure 4.2: A Stuxnet-like attack exploits multiple vulnerabilities to target at PLC.

4.3.2 Players

An attacker and a defender are the key "players" in the designed stochastic game-theoretic model. There could be many attackers who are trying to launching attacks and many defenders in the network to protect the system, but this work abstracts those attackers and defenders as one attacker and one defender, respectively. The attacker attains his/her ultimate target via multiple stages. The concept of the defender denotes the security operator (security operator and system administrator are used interchangeably in this thesis) who has the task of deploying available defence countermeasures to protect the underlying system, while the attacker attempts to reach the target or the most critical assets located at the centre of the smart grid. This model considers that each of the players has some finite resources to perform actions at each stage of the game. The attacker is considered to be a resource-constrained, determined and rational player. In this way, the attacker will give up when he/she finds it is out of his/her capability to launch any further attacks. Furthermore, it is assumed that once an attack is initiated, the

attacker him/herself will never revert the system to any of the previous state (for example, to recover the system from a malfunctioning state to a normal operational state). In this work, the attacker is only able to perform a single action in his/her turn. It is also assumed that the defender does not know whether or not there is an attacker, as that in real systems. Furthermore, the attacker is assumed to be always aware of the active defence mechanisms. Moreover, the defender does not know the objectives and strategies of an attacker. A successful attack may or may not be observable to the defender. The attacker strategically and dynamically chooses his/her targets and attack methods in order to achieve his/her goals, while the defender defines security policies and implements security measures (including email filtering, detection software, patches to prevent and detect attacks, and repairing the system after disruption). In this thesis, to keep matters of presentation simple, the (non-exhaustive) action space AS_1 for the defender is assumed to be AS_1 = {Email-filter configuration, IDS deployment, Patch} and the corresponding (non-exhaustive) action space AS_2 for the attacker is assumed to be AS_2 = {Exploit, Do nothing}, which will be elaborated in detail in the following paragraphs.

4.3.2.1 Defender's Actions

A security operator has a (non-exhaustive) selection of security countermeasures to perform on a day-to-day basis: "Email-filter configuration", "IDS deployment", and "Patch".

Email-filter configuration: Email filtering is the processing of email organisation according to specified criteria. This refers mostly to the automatic processing of incoming emails, but the term can also be applied to outgoing emails, as well as those being received. Email filtering software takes emails as inputs, while its outputs may include (i) passing the message through as unchanged for delivery to the user's mailbox, (ii) redirecting the message for delivery elsewhere, or (iii) throwing the message away. Some email filters are even able to edit messages during processing.

IDS deployment: An IDS, which can be deployed in a network-based or node-based way in a smart grid communication networks, effectively monitors the application layer data in the smart grid communication network or even the state of the network. When the system is undergoing other non-security related tasks, an IDS can help the defender to identify whether there has been any activity that could result in the compromise of the monitored nodes.

Patch: If vulnerability (e.g., buffer overflow) exists in a piece of software, and a patch has been developed for that vulnerability, the defender can choose to apply patch. When the defender chooses to patch the system, the defender removes the option for the attacker to

use an exploit for that vulnerability. This means that when the attacker attempts to exploit a vulnerability that is going to be patched, he/she will fail to compromise the node. However, it should be noted that, if there is another vulnerability that can be exploited on the same node, patching one will not necessarily stop the attacker from compromising the node. It is assumed that an attacker can only exploit one vulnerability by taking one action. However, while a patch is available, there are many devices in the communication network that cannot easily be patched with security updates. Patch management in smart grids is currently the topic of much debate and attention [118]. Nevertheless, This thesis assumes "Patch" is one action that the defender can take to protect his/her system.

4.3.2.2 Attacker's Actions

The attacker in this model is assumed to have only two different actions. The attacker can do nothing or he/she can launch an attack by exploiting a vulnerability.

Exploit: Once an exploit has been developed, the attacker use the exploit to advance his/her way through the system towards the data (e.g., sensitive or confidential information), which he/she wishes to steal or sensitive systems (e.g., defense contractors) to which he/she wishes to gain access. In this model, an attacker can only use one single attack at a time, no matter whether there are one or multiple exploits available.

Do nothing: The attacker can choose to take no action, which in turn requires no use of resources by the attacker. This action will typically be taken by the attacker when he/she does not want to use an exploit, has no remaining usable exploits or is concealing him/herself to guarantee enough time to test and validate attack capabilities for the next exploits. It is noteworthy that, by taking this action, the attacker remains active.

However, it is easy to understand why both players will pursue probabilistic strategies (i.e., mixed strategies, which will be defined later in Section 4.3.5), as the playing of a strategy with certainty can facilitate the other player to take advantage of such a choice.

4.3.3 State Space

Based on the actions taken by both players, the system goes from one state to another in a probabilistic manner. All the possible states of involved network nodes constitute the state space. In general, the state of the network contains various kinds of features, such as hardware and software configurations, network connectivities, and user privilege levels. The more features of the

network status we model, the more accurately we present the network and, at the same time, the more complex and difficult the analysis becomes. This thesis views the communication network in smart grids as a graph (see an example network in Figure 4.3). A node in the graph is a physical entity, such as a server or a computer. An edge (reflecting network connectivity) in the graph represents a direct information flow path (by considering a bidirectional communication path as a pair of information incoming and outgoing edges). An attacker can exploit the vulnerability on a node by taking advantage of the presence of a vulnerability, network connections, and an attacker's level of privilege on that node. Hence, for the ℓth node in the communication network, there is a working state $\phi_N(\ell)$ and a defence state $\theta_N(\ell)$ at any stage $N \in \mathbb{N}$ of the system. This work assumes "normal" and "malfunctioning" are two working states, meaning that the node has a normal functional state and is malfunctioning, respectively. The defence state $\theta_N(\ell)$ is the defence countermeasure assigned to the node (e.g., $\theta_N(\ell)$ can be "Intrusion detection with effective access policies").

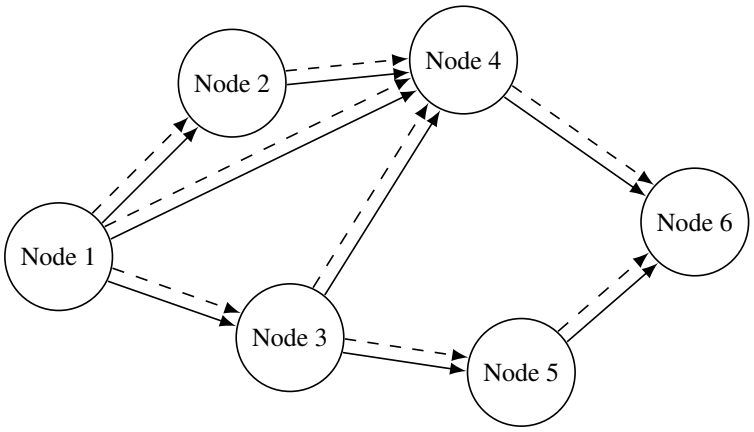


Figure 4.3: A sample network graph with information flow paths.

Therefore, the system state s_N at stage N is

$$s_N = \Big\{ \big(\phi_N(1), \theta_N(1)\big), \cdots, \big(\phi_N(\ell), \theta_N(\ell)\big), \cdots, \big(\phi_N(n_C), \theta_N(n_C)\big) \Big\},$$

where n_C is the total number of nodes in the involved communication network. Taking the six nodes network in Figure 4.3 for instance, at the initial stage, all the nodes are assumed to be normal functional nodes and all nodes are deployed with an IDS. And at the second stage, the attacker uses external sources to remotely exploit a vulnerability and compromises node 1, while the deployed IDS is not effective enough to detect such an attack. Other nodes remain

normal functioning nodes, while the IDS deployed previously is not changed. Therefore, the state space S is $S = \{s_1, s_2\}$, where s_1 = {(normal, IDS),(normal, IDS),(normal, IDS),(normal, IDS),(normal, IDS),(normal, IDS) } and s_2 = {(malfunctioning, IDS),(normal, IDS),(normal, IDS),(normal, IDS),(normal, IDS),(normal, IDS)}. It is not difficult to observe that the system state is determined by the previous state, vulnerability exploitation, and the current actions of both the attacker and the defender.

4.3.4 State Transition Probabilities

A multistage attack, by exploiting vulnerabilities, makes the network system transition from one state to another. However, such a transition also depends on the active defence mechanisms. For example, during the concealment step of a general multistage cyber attack (see Figure 4.1), if IDSs are properly deployed, the attacker will be detected and the attack chain will be "broken". Therefore, the probability that the state will transition from one to another depends on the joint actions of both players. Unlike accidental failures, an attacker will consider the consequences of his/her actions and compare the reward versus the cost of each elementary attack action [119]. Therefore, the transition probabilities from one state to another depend not only on the decisions by both players to take action, but also the *success* probability of an attacker going through with his/her action. The probability of success for the attacker at state s is denoted as $p_{suc}(y_{s,b})$ (this work assumes the second player to be the attacker and $y_{s,b}$ (which will be defined later in Equation (4.4)) to be the probability that his/her b action is taken at state $s \in S$). Obviously, whether an action by an attacker succeeds depends on the available exploitable vulnerabilities of an asset. For example, attacking an asset with no exploitable vulnerability has zero probability of success. In the attacker-defender stochastic game-theoretic model, success probabilities of an attacker's actions are assigned, based on the intuition and experience (e.g., case studies, common vulnerability scoring system (CVSS), knowledge engineering). Principally, the action of the defender also involves a success probability (e.g., IDSs have detection rates); to simplify the underlying problem, however, such a success probability of the defender with his/her actions is always assumed to be one.

The probability for player 1 (player 1 is the defender) to take action $a \in AS_1$ at state s is denotes as $x_{s,a}$ (which will be defined later in Equation (4.3)), while the probability for player 2 (player 2 is the attacker) to take action $b \in AS_2$ at state s is denoted as $y_{s,b}$. Both players take actions simultaneously, meaning that both players take action independently of one another. Thus,

when actions $a \in AS_1$ and $b \in AS_2$ are taken from both players, the state transition probability from game state $s \in S$ to state $s' \in S$ can be calculated as

$$q(s'|s,a,b) = x_{s,a} y_{s,b} p_{suc}(y_{s,b}).$$

For example, if the probability for player 1 to take action"IDS deployment" is 0.5, the probability for player 2 to take action "Exploit" is 0.4, and the probability that the attacker will successful obtain his/her (sub)goal is 0.2, the game will move from state "normal" to state "malfunctioning" with a state transition probability of

$$q(\text{malfunctioning}|\text{normal}, \text{IDS deployment}, \text{Exploit}) = 0.5 \cdot 0.4 \cdot 0.2 = 0.04.$$

Depending on the exploitable vulnerabilities, it may be that there is no transition between certain game states. For example, it may not be possible for the network to transition from a normal functioning state to a totally failed state without going through any intermediate states. In this work, infeasible state transitions are assigned with a transition probability of zero and hence ignored. Both players make their moves simultaneously, with state transition probabilities being common knowledge to both players.

4.3.5 Game Formalization

In the previous subsections, this thesis sets out the action spaces of players. At each stage of the game for multistage attacks, the play is in a given state,, with every player choosing an action from his/her available action space. With a state transition probability (which is jointly controlled by both players), the current state of the game, and the collection of actions that the players choose, the game will go to another state with an immediate payoff received by each player. Each player has his/her own costs of executing actions, thus the payoff of the game cannot only be described by rewards. Although there may be a dependence of rewards and losses among player's payoffs, because of players' own action execution costs, the payoffs of the attacker and the defender do not sum up to zero. Therefore, the interaction between the attacker and the defender is non-zero-sum. The game is also played with positive stop probabilities in each game state, since the game will end when the attacker decides to stop his/her attacks (completely inactive) and the defender keeps his/her defence countermeasures unchanged. Besides, this thesis notices that none of the players knows the exact state of the system, while both players have different kinds of private information about the state and action

processes over time. Therefore, in order to apply game theory to assess multistage attacks in smart grid communication networks, the asymmetric information, non-zero-sum, and positive stop probability characteristics of the interaction between the attacker and the defender should be taken into account.

The next concern is on the game type that appropriately captures the players' interactions in the case of multistage cyber attacks. Both players do not know the exact state of the game, but maintain a belief about the current state of the game (where a belief is a probability distribution over the possible states of the game). Taking a two-player non-zero-sum two-stage game for instance, suppose the game has two states and both players do not know the current state of the game (either in state s_1 or state s_2), but they have a belief $\rho_1 = (\rho_1(s_1), \rho_1(s_2)) = (0.8, 0.2)$ about the current state, that is , there is a 80% likelihood that the current game at stage 1 is in state s_1, while there is a 20% likelihood that the current game at stage 1 is in state s_2. The most relevant existing game model that can partially solve this problem is the stochastic game with lack of information on one side (SGLIOS) with positive stop probabilities. Thus, this thesis considers SGLIOS with positive stop probabilities as a basic game model and extends it to include the non-zero-sum and information asymmetry of the interactions of the attacker and the defender in smart grid communication networks.

This work starts with the definition of SGLIOS with positive stop probabilities described in [120]. The model of SGLIOS with positive stop probabilities is a two-person zero-sum game and states are a finite set $S = \{s_1, s_2, \cdots, s_\ell, \cdots, s_{k_C}\}$ ($k_C = |S|$ denotes the number of states). Associated with each state s_ℓ ($\ell \in \{1, 2, \cdots, k_C\}$) is a matrix game $\mathbf{G}_{\{s_\ell\}}$ of size $m_1 \times m_2$, where $m_1 = |AS_1|$ (the number of actions of player 1), $m_2 = |AS_2|$ (the number of actions of player 2), and $\mathbf{G}_{\{s_\ell\}} = \{g_{\{s_\ell\}}(a,b) : AS_1 \times AS_2 \to \mathbb{R} | a = 1, 2, \cdots, m_1; b = 1, 2, \cdots, m_2; \ell = 1, 2, \cdots, k\}$. Additionally, $\emptyset$ is adjoined to S, where $\emptyset$ represents the end of the game. In SGLIOS with positive stop probabilities, at any stage N, there is a probability distribution over states in S. Player 1 is informed about such a probability distribution at every game stage, but player 2 is never informed about that. There is a probability $\rho_1 \in \Delta(S)$ about the initial state, where $\Delta(S)$ is the set of all probability distributions on S. State transition probabilities are denoted as $q(\cdot|s,a,b)$, which depends on the current state s and actions a and b taken by the defender and the attacker, respectively. Because of the positive stop probability assumption, the sum of transition probabilities from state s to all possible next game state s' is less than one, i.e., $\sum_{s' \in \{S - \emptyset\}} q(s'|s,a,b) < 1$, $\forall a \in AS_1$, $b \in AS_2$. Both players make their moves simultaneously

and both of them are informed of their choices (a,b). The game will either end with a probability of $q(\emptyset|s,a,b) > 0$ or transition to a new state s' with a probability of $q(s'|s,a,b) > 0$. Although both players remember actions taken by them, player 2 is not informed of the received immediate payoff $g_{\{s\}}(a,b)$ (which only player 1 knows) of the game. SGLIOS with positive stop probabilities is played with perfect recall (i.e., at each stage each player remembers all past actions chosen by all players and player 1 knows all *past* states that have occurred). There is a common knowledge among both players before they move at stage N and such a common knowledge is a sequence of the form $h_N = \{(a_1,b_1),(a_2,b_2),\cdots,(a_{N-1},b_{N-1})\}$ (where $a_\ell \in AS_1$ is the action chosen from player 1 at the ℓ stage, $b_\ell \in AS_2$ is the action chosen from player 2 at the ℓ stage, and $\ell \in \{1,2,\cdots,N-1\}$). The common knowledge h_N is also called *history* and it represents the choices of actions (i.e., pure strategies) of the two players up to (and excluding) stage N. SGLIOS with positive stop probabilities restricts its attention to behavioural strategies [121].

When the game is in the state of s at stage N, the action chosen by the players can be deterministic or randomised. A mixed strategy corresponds to a distribution over actions (i.e., pure strategies). Let $\mathbf{x}_s$ $(s \in S)$ denote the mixed strategy of player 1 in state s and $\mathbf{y}_s$ $(s \in S)$ denote the mixed strategy of player 2 at state s. The strategies $\mathbf{x}_s$ and $\mathbf{y}_s$ in state s are used to assign probabilities over the action set AS_1 and AS_2 with cardinality m_1 and m_2, respectively. And the mixed strategies $\mathbf{x}_s$ and $\mathbf{y}_s$ are defined as

$$\mathbf{x}_s := \{(x_{s,1},\cdots,x_{s,a},\cdots,x_{s,m_1}) \in \mathbb{R}_+^{m_1} | \sum_{a=1}^{m_1} x_{s,a} = 1, 0 \leq x_{s,a} \leq 1\}, \tag{4.1}$$

$$\mathbf{y}_s := \{(y_{s,1},\cdots,y_{s,b},\cdots,y_{s,m_2}) \in \mathbb{R}_+^{m_2} | \sum_{b=1}^{m_2} y_{s,b} = 1, 0 \leq y_{s,b} \leq 1\}, \tag{4.2}$$

where

$$x_{s,a} := \mathbb{P}(a|s,h_N), \tag{4.3}$$

$$y_{s,b} := \mathbb{P}(b|s,h_N), \tag{4.4}$$

and $x_{s,a}$ and $y_{s,b}$ represent the probability that action a of player 1 and action b of player 2 will be taken. It is to be noted that actions of players are independently chosen among each other, since both players are playing simultaneously. Let $\mathbf{x} = (\mathbf{x}_{s_1},\mathbf{x}_{s_2},\cdots,\mathbf{x}_{s_\ell},\cdots,\mathbf{x}_{s_k})$ be a vector of mixed strategies for player 1 and $\mathbf{x} \in \Omega^{m_1}$ (Ω^{m_1} is the set of all probability vectors of

length m_1). Correspondingly, let $\mathbf{y} = (\mathbf{y}_{s_1}, \mathbf{y}_{s_2}, \cdots, \mathbf{y}_{s_\ell}, \cdots, \mathbf{y}_{s_k})$ be a vector of mixed strategies for player 2 and $\mathbf{y} \in \Omega^{m_2}$ (Ω^{m_2} is the set of all probability vectors of length m_2). Let E be a random variable representing the stage the game ends and h_N be the common knowledge among players up to (and excluding) stage N. At each stage N, if player 1 took action a and player 2 took action b, player 1 receives an immediate payoff $g_{\{s_N\}}(a,b)$, let $\mathcal{A}_N(\cdot)$ denote the expected immediate payoff function (with strategies from both players as parameters) at stage N, provided that the game does not end, for player 1, we have [120]

$$\mathcal{A}_N(\mathbf{x},\mathbf{y}) := \mathbb{E}_{\mathbf{x},\mathbf{y}}\big(\rho_N(s)\mathbf{G}_{\{s\}}|E > N\big),$$

where $\rho_N(s) \in \rho_N$ is a probability that player 1 believes the current game state is s at stage N, where ρ_N is a belief (i.e., a probability distribution) on game states at N stage. This belief about states will be discussed later. The expectation operator $\mathbb{E}_{\mathbf{x},\mathbf{y}}\big(\cdot\,|E > N\big)$ is used to mean that player 1 plays strategy $\mathbf{x}$ and player 2 plays strategy $\mathbf{y}$, under the condition that the game does not end at stage N. By defining $\mathcal{R}_N(\cdot)$ as

$$\mathcal{R}_N(\mathbf{x},\mathbf{y}) := \mathcal{A}_N(\mathbf{x},\mathbf{y}) \cdot \mathbb{P}(E > N),$$

where $\mathbb{P}(E > N)$ means that the game does not end at stage N and the stage E where game ends is longer than N. The total payoff function $\mathcal{H}(\cdot)$ (with strategies from both players as parameters) in SGLIOS with positive stop probabilities is given as

$$\begin{aligned}\mathcal{H}(\mathbf{x},\mathbf{y}) &= \sum_{N=1}^{\infty} \mathcal{R}_N(\mathbf{x},\mathbf{y}) \\ &= \sum_{N=1}^{\infty} \mathbb{E}_{\mathbf{x},\mathbf{y}}\big(\rho_N(s)\mathbf{G}_{\{s\}}|E > N\big) \cdot \mathbb{P}(E > N).\end{aligned} \tag{4.5}$$

Equation (4.5) assumes that the game stage can go to infinite (∞). However, because of the positive stop probability assumption, the game will end after a finite number of stages [97]. Therefore, the game of SGLIOS with positive stop probabilities is a finite game. The fundamental tool in SGLIOS with positive stop probabilities is an updating mechanism which gives at each stage N the belief ρ_N, the posterior distribution on the state space given the history h_N up to stage N. Player 1 is informed about the belief ρ_N but player 2 does not. The updating mechanism for the belief ρ_N is working in this way: initially both players choose strategies $\mathbf{x}$ and $\mathbf{y}$ and give them to chance (chance is a special player, who can be the environment of the system) who then at stage 1 chooses s_1 according to ρ_1. Then the action pair (a_1,b_1) is chosen according to $(\mathbf{x}_{s_1},\mathbf{y}_{s_1})$ and an immediate payoff $g_{\{s_1\}}(a_1,b_1)$ is received by

player 1. Provided that the game does not end, chance chooses another state s_2 according to $\rho_2(s_2) := \mathbb{P}(s_2|a_1, b_1, E > 2)$ or decides to end the game according to $\mathbb{P}(E = 2|a_1, b_1)$. At stage N, chance decides the game to go to state s_N according to $\rho_N(s_N) := \mathbb{P}(s_N|h_N, E > N)$ or ends the game according to $\mathbb{P}(E = N|E > N-1, h_N)$. The value $\rho_N(s)$ represents that the chance believes that the current game state is $s \in S$. And the belief value $\rho_N(s)$ (the chance's belief about the current game state) is updated with (see [120] and [122] for more details)

$$\rho_N(s) := \frac{\sum_{s' \in S} q(s|s', a_{N-1}, b_{N-1}) x_{s,a_{N-1}} \rho_{N-1}}{\sum_{s \in S} \sum_{s' \in S} q(s|s', a_{N-1}, b_{N-1}) x_{s,a_{N-1}} \rho_{N-1}}. \tag{4.6}$$

It is proved in [120] that the value of the game of SGLIOS with positive stop probabilities exists and is a continuous function on the state space; and there exists also a stationary optimal strategy for the informed player — player 1. The optimal strategy of player 1 depends only on the updated probability of the current state which he/she independently knows.

Since the interaction between the attacker and the defender in smart grid use cases is non-zero-sum, it is needed to extend SGLIOS with positive stop probabilities (which is zero-sum) to non-zero-sum cases. The game matrices should be first identified. Each player (player 1 or player 2) has his/her own game matrix $\{\mathbf{G}_{\{1,s_1\}}, \mathbf{G}_{\{1,s_2\}}, \cdots, \mathbf{G}_{\{1,s_\ell\}}, \cdots, \mathbf{G}_{\{1,s_k\}}\}$ (for player 1) or $\{\mathbf{G}_{\{2,s_1\}}, \mathbf{G}_{\{2,s_2\}}, \cdots, \mathbf{G}_{\{2,s_\ell\}}, \cdots, \mathbf{G}_{\{2,s_k\}}\}$ (for player 2), which is composed of two parts: his/her reward/loss as the result of an attack and the cost of carrying out his/her action. Essentially, both two players are with contradictory objectives and they are competing with each other. The objective of each player is to maximise his/her own total payoff with strategies $\mathbf{x}$ and $\mathbf{y}$

$$\mathcal{H}_1(\mathbf{x}, \mathbf{y}) = \sum_{N=1}^{\infty} \mathcal{R}_{1,N}(\mathbf{x}, \mathbf{y}) = \sum_{N=1}^{\infty} \mathbb{E}_{\mathbf{x},\mathbf{y}}\big(\rho_N(s)\mathbf{G}_{\{1,s\}}|E > N\big) \cdot \mathbb{P}(E > N), \tag{4.7}$$

$$\mathcal{H}_2(\mathbf{x}, \mathbf{y}) = \sum_{N=1}^{\infty} \mathcal{R}_{2,N}(\mathbf{x}, \mathbf{y}) = \sum_{N=1}^{\infty} \mathbb{E}_{\mathbf{x},\mathbf{y}}\big(\rho_N(s)\mathbf{G}_{\{2,s\}}|E > N\big) \cdot \mathbb{P}(E > N). \tag{4.8}$$

The reason why both the attacker and the defender share the same belief value $\rho_N(s)$ will be given out in Section 4.4.1. Another characteristic of the interaction between the defender and the attacker is the information asymmetry, where each player has private information about the state of the network system and the private information among players is asymmetric. The asymmetry stems from the fact that the attacker has knowledge of a particular vulnerability which can be exploited; while the defender knows how to use resources to defend against all possible attacks. In other words, one player either deliberately distorts or does not disclose all the relevant information to another player, during their interaction phases. Since no player

completely knows the exact state s of the game, it is assumed that each player (player 1 or player 2) observes a private local state $s_{\{1\}}$ or $s_{\{2\}}$ of the game and the state of the game is composed of both private local states $s = \{s_{\{1\}}, s_{\{2\}}\}$. Each player has to form a belief about the exact state s up to stage N. It is assumed that each player knows all *past* states that have occurred, which means when the game goes to next state, the previous one state will be publicly known to all players. Provided that the game has not ended, the history h_N is common information available to both players whereas private information is available to only that specific player.

According to [120], players can forget the sequence of previous states. So without loss of generality, it is assumed that the state of the two-player game at $N+1$ stage (assuming that the game does not end at N stage) evolves according to the current state s_N and all previous strategies from both players. Similarly, the private local state of each player is evolving according to the current local state $s_{\{1,N\}}$ for player 1 or $s_{\{2,N\}}$ for player 2 and all previous strategies from both players. It is obviously that, at any stage N, the local state $s_{\{1,N\}}$ for player 1 is independent of the local state $s_{\{2,N\}}$ for player 2. Therefore, when both players have taken actions $a \in AS_1$ and $b \in AS_2$, the state transition probability in the case of information asymmetry among players is defined as

$$\begin{aligned} q(s_N|s_{N-1}.a,b) &:= \mathbb{P}(s_N|s_{N-1},a,b) \\ &= \mathbb{P}(s_{\{1,N\}}|s_{\{1,N-1\}},a,b) \cdot \mathbb{P}(s_{\{2,N\}}|s_{\{2,N-1\}},a,b). \end{aligned} \tag{4.9}$$

The choice of actions for each player at stage N may depend on all past strategies from both players and the player's current local state (the local state is one part of the game state $s_N = \{$ $s_{\{1,N\}}$, $s_{\{2,N\}}$ $\}$), which is consistent with Equations (4.3) and (4.4). Given the fact that either player can observe the current game state s_N ($s_N \in S$) at stage N and each player observes only a private local current game state $s_{\{1,N\}}$ or $s_{\{2,N\}}$, the probability for player 1 to choose action a and the probability for player 2 to choose action b at stage N are defined as

$$x_{s_{\{1,N\}},a} := \mathbb{P}(a|s_{\{1,N\}},h_N) \tag{4.10}$$

and

$$y_{s_{\{2,N\}},b} := \mathbb{P}(b|s_{\{2,N\}},h_N), \tag{4.11}$$

respectively.

It is to be noted that by knowing the strategy of the other player, one player can make inference about the other player's private information $s_{\{1,N\}}$ (if this player is player 2) or

$s_{\{2,N\}}$ (if this player is player 1) from observing their actions. If a player knows the local private state of the other player, he/she can further predict the action would be taken by the other player at next stage. Provided that the game continues, state s_N is chosen according to $\rho_N(s_N) = \mathbb{P}(s_N|h_N, E > N)$, the immediate payoff $g_{\{1,s_N\}}(a_N, b_N)$ is received at player 1(correspondingly, $g_{\{2,s_N\}}(a_N, b_N)$ is received at player 2), and both two players computes his/her belief $\rho_{N+1}(s_{N+1})$ on next game state s_{N+1}.

In order to facilitate game analysis of the attacker-defender game, provided that the game continues (i.e., $E > N$, the stage E when the game ends is longer than stage N), this thesis defines a stage game for each stage N as follows.

Definition 1. (Stage game Γ_N) An attacker-defender non-zero-sum game with asymmetric information and positive stop probabilities is a tuple (AS_1,AS_2, $S, Q, \rho_N, \mathcal{H}_1, \mathcal{H}_2$):

– AS_1 and AS_2 are the action spaces of the strategic player 1 and 2, respectively and m_1 $= |AS_1|$, $m_2 = |AS_2|$. The action spaces of player 1 and player 2 are assumed to be the same in all game states.

– S consists of a finite set of states and $S = \{s_1, s_2, \cdots, s_\ell, \cdots, s_{k_C}\}$ (k_C is the number of states in S). Associated with each state s_ℓ, there are two payoff matrices $\mathbf{G}_{\{1,s_\ell\}}$ and $\mathbf{G}_{\{2,s_\ell\}}$ and each payoff matrix is of size $m_1 \times m_2$. Player 1 knows his/her own payoff matrices $\left\{\mathbf{G}_{\{1,s_1\}}, \mathbf{G}_{\{1,s_2\}}, \cdots, \mathbf{G}_{\{1,s_\ell\}}, \cdots, \mathbf{G}_{\{1,s_k\}}\right\}$ and player 2 knows his/her own payoff matrices $\left\{\mathbf{G}_{\{2,s_1\}}, \mathbf{G}_{\{2,s_2\}}, \cdots, \mathbf{G}_{\{2,s_\ell\}}, \cdots, \mathbf{G}_{\{2,s_k\}}\right\}$. For each payoff matrix $\mathbf{G}_{\{1,s_\ell\}}$ or $\mathbf{G}_{\{2,s_\ell\}}$, it is defined as $\mathbf{G}_{\{1,s_\ell\}} = (g_{\{1,s_\ell\}}(a,b) \in \mathbb{R} | a = 1,2,\cdots,m_1; b = 1,2,\cdots,m_2; \ell = 1,2,\cdots,k)$ or $\mathbf{G}_{\{2,s_\ell\}}$ $= (g_{\{2,s_\ell\}}(a,b) \in \mathbb{R} | a = 1,2,\cdots,m_1; b = 1,2,\cdots,m_2; \ell = 1,2,\cdots,k)$.

– Q: $S \times AS_1 \times AS_2 \times S \rightarrow [0,1]$ is a matrix which describes state transition probabilities and $Q = (q(s'|s,a,b) | s', s \in S; a = 1,2,\cdots,m_1; b = 1,2,\cdots,m_2)$.

– ρ_N is a belief which is a probability distribution on game states at stage N.

– $\mathcal{H}_1(\cdot)$ and $\mathcal{H}_2(\cdot)$ are player 1's and player 2's total payoff functions, respectively. Both functions take strategies of both players as parameters.

4.4 Game Analysis

This section analyses the previously specified game model and finds Nash equilibria to construct an attack scenario in which the adversary cannot succeed in performing multistage cyber attacks and arriving at his/her ultimate target. In the previously specified game model, players have asymmetric information about the current state of the game, therefore, each player has

to form a belief about the current state of the game. In SGLIOS with positive stop probabilities, player 1 (who can be assumed to be the defender) is informed about the belief value on the current game state but player 2 (who can be assumed to be the attacker) does not. Under the assumption that the true state of the game is independent of the action taken by player 2, the belief value in SGLIOS with positive stop probabilities is not conditional on the strategy taken by player 2 (see Equation (4.6)). However, this assumption is not applicable in attacker-defender games where strategies from both player decide the state and the process of the game. Therefore, new belief system updating mechanisms should be described and belief system updates account for a central technical contribution in this thesis. To assist equilibria computation of the designed attacker-defender stochastic game-theoretic model, this section first provides the belief update mechanism and then elaborates an easy-to-follow method for Nash equilibria computation.

4.4.1 Belief System Updates

It can be seen that the actions taken by both players can be summarised through a belief ρ_N of game states. For example, in SGLIOS with positive stop probabilities, under the assumption that the current state of the game is independent of player 2's actions, the belief ρ_N in Equation (4.6) summarises actions taken by player 1. In the game of asymmetric information, at stage N, the current game state is unknown to both players; player 1 privately observes a local state $s_{\{1,N\}}$ and player 2 privately observes another local state $s_{\{2,N\}}$. To consist with [120] and the recent work on stochastic game with asymmetric information [106, 108], in this work, belief ρ_N on the current state s_N of the game is defined as $\rho_N(s_N) := \mathbb{P}(s_N|h_N, E > N)$.

Provided that the game does not end at N stage, which means the condition $\mathbb{P}(E > N)$ equals to one, for any history $h_N = \big\{(a_1,b_1),(a_2,b_2),\cdots,(a_{N-1},b_{N-1})\big\}$, it can be observed that player's belief about the current game state s_N is

$$\begin{aligned}\rho_N(s_N) &:= \mathbb{P}(s_N|h_N)\\ &= \mathbb{P}(s_{\{1,N\}}, s_{\{2,N\}}|h_N).\end{aligned} \tag{4.12}$$

Because of the independence of private local states $s_{\{1,N\}}$ and $s_{\{2,N\}}$, Equation (4.12) can be

further written as

$$\begin{aligned}\rho_N(s_N) &= \mathbb{P}(s_{\{1,N\}}, s_{\{2,N\}}|h_N) \\ &= \mathbb{P}(s_{\{1,N\}}|h_N) \cdot \mathbb{P}(s_{\{2,N\}}|h_N).\end{aligned} \tag{4.13}$$

The probability $\mathbb{P}(s_{\{1,N\}}|h_N)$ can be viewed as the probability that player 2 believes that player 1 will be in state $s_{\{1,N\}}$ based on the history h_N of past actions taken from both players. Player 2 might also derive this probability $\mathbb{P}(s_{\{1,N\}}|h_N)$ at N stage based on his/her private local states $(s_{\{2,1\}}, s_{\{2,2\}}, \cdots, s_{\{2,N-1\}})$. however, since the private local states $s_{\{1,N\}}$ and $s_{\{2,N\}}$ ($N \in \mathbb{N}$) are independent, the probability $\mathbb{P}(s_{\{1,N\}}|h_N, s_{\{2,1\}}, s_{\{2,2\}}, \cdots, s_{\{2,N-1\}})$ would be the same as the probability $\mathbb{P}(s_{\{1,N\}}|h_N)$. Therefore, knowledge of $(s_{\{2,1\}}, s_{\{2,2\}}, \cdots, s_{\{2,N-1\}})$ does not affect the probability $\mathbb{P}(s_{\{1,N\}}|h_N)$. For player 2, the probability $\mathbb{P}(s_{\{2,N\}}|h_N)$ can be viewed as the probability that player 2 believes that his private local state at stage N is $s_{\{2,N\}}$ based on the history of actions from both players. It is to be noted that player 2 knows his current private local state $s_{\{2,N\}}$. However, this thesis assumes that after taking any action and before arriving in state $s_{\{2,N\}}$, player 2 can also has a probability $\mathbb{P}(s_{\{2,N\}}|h_N)$ about his/her private local state $s_{\{2,N\}}$. Based on probabilities that player 1 will in state $s_{\{1,N\}}$ and he/she him/herself will be in state $s_{\{2,N\}}$ at stage N, player 2 can derive the probability $\rho_N(s_N)$ that next game state is s_N at stage N. Similarly, player 1 can also derive the probability that player 2 will be in state $s_{\{2,N\}}$ at stage N with probability $\mathbb{P}(s_{\{2,N\}}|h_N)$ and the probability that he/she himself/herself will be in state $s_{\{1,N\}}$ with probability $\mathbb{P}(s_{\{1,N\}}|h_N)$. Therefore, both players can obtain the same belief value that the game play is in state s_N at stage N.

Let's analyse the probability $\mathbb{P}(s_{\{1,N\}}|h_N)$ first and present a conclusion about the belief value $\rho_N(s_N)$ later in Equation (4.20). The probability $\mathbb{P}(s_{\{1,N\}}|h_N)$ that player 2 believes that player 1 will be in state $s_{\{1,N\}}$ at stage N can be further written as

$$\mathbb{P}(s_{\{1,N\}}|h_N) = \sum_{s_{\{1,N-1\}}} \mathbb{P}(s_{\{1,N\}}|s_{\{1,N-1\}}, h_N) \cdot \mathbb{P}(s_{\{1,N-1\}}|h_N). \tag{4.14}$$

Now, let's analyse the probability $\mathbb{P}(s_{\{1,N\}}|h_N)$ term by term. Because of the dynamics of the system (i.e., the current state depends on the previous one state and the action profile taken in the previous one state), the first term of Equation (4.14) can be written as

$$\mathbb{P}(s_{\{1,N\}}|s_{\{1,N-1\}}, h_N) = \mathbb{P}(s_{\{1,N\}}|s_{\{1,N-1\}}, a_{N-1}, b_{N-1}). \tag{4.15}$$

Since all stages before the N stage determine the probability distribution of the private local state $s_{\{1,N\}}$ of player 1 only through $s_{\{1,N-1\}}$, a_{N-1} (i.e., player 1's action taken at $N-1$ stage, which is common information to both players), the second term of Equation (4.14) can be

$$\mathbb{P}(s_{\{1,N-1\}}|h_N) = \mathbb{P}(s_{\{1,N-1\}}|h_{N-1}, a_{N-1}).$$

If there exists any local state $s'_{\{1,N-1\}} \in S$ (the existence will be argued below) at stage $N-1$ with $\mathbb{P}(s'_{\{1,N-1\}}|h_{N-1}) > 0$, $x_{s'_{\{1,N-1\}},a_{N-1}} > 0$, then, for all $s_{\{1,N-1\}} \in S$, there exists

$$\begin{aligned}\mathbb{P}(s_{\{1,N-1\}}|h_{N-1}, a_{N-1}) &= \frac{\mathbb{P}(s_{\{1,N-1\}}|h_N - 1) \cdot \mathbb{P}(a_{N-1}|s_{\{1,N-1\}}, h_{N-1})}{\sum_{s'_{\{1,N-1\}}} \mathbb{P}(s'_{\{1,N-1\}}|h_{N-1}) \cdot \mathbb{P}(a_{N-1}|s'_{\{1,N-1\}}, h_{N-1})} \\ &= \frac{\mathbb{P}(s_{\{1,N-1\}}|h_N - 1) \cdot x_{s_{\{1,N-1\}},a_{N-1}}}{\sum_{s'_{\{1,N-1\}}} \mathbb{P}(s'_{\{1,N-1\}}|h_{N-1}) \cdot x_{s'_{\{1,N-1\}},a_{N-1}}},\end{aligned} \tag{4.16}$$

where $x_{s'_{\{1,N-1\}},a_{N-1}}$ is the probability that player 1 will take action a_{N-1} in state $s'_{\{1,N-1\}}$. See Appendix B for a detailed derivation of Equation (4.16). Substituting Equations (4.15) and (4.16) into Equation (4.14), we can get

$$\mathbb{P}(s_{\{1,N\}}|h_N) = \frac{\mathbb{P}(s_{\{1,N\}}|s_{\{1,N-1\}}, a_{N-1}, b_{N-1}) \cdot \mathbb{P}(s_{\{1,N-1\}}|h_{N-1}) \cdot x_{s_{\{1,N-1\}},a_{N-1}}}{\sum_{s'_{\{1,N-1\}}} \mathbb{P}(s'_{\{1,N-1\}}|h_{N-1}) \cdot x_{s'_{\{1,N-1\}},a_{N-1}}}. \tag{4.17}$$

It can be seen from Equation (4.17) that player 2 can make inference about player 1's private local state $s_{\{1,N\}}$ from observing player 1's actions. The phenomenon is called signaling in games with asymmetric information [106]. Given that the history h_N is observable (i.e., the game does not end at $N-1$ stage), there always exists a local state $s'_{\{1,N-1\}} \in S$ and the probability of choose action a_{N-1} at $N-1$ stage is greater than zero. Therefore, the probability $\mathbb{P}(s_{\{1,N\}}|h_N)$ defined in Equation (4.17) is continuous and the continuity claim can be found in [122]. Similarly, the probability $\mathbb{P}(s_{\{2,N\}}|h_N)$ that player 2's belief about his/her own private local state $s_{\{2,N\}}$ at N stage can also be derived from the same procedures by replacing the index "1" with "2", the action "a_{N-1}" with "b_{N-1}" and the symbol "x" with "y" in Equation (4.16). Therefore, we have

$$\begin{aligned}\rho_N(s_N) = &\frac{\mathbb{P}(s_{\{1,N\}}|s_{\{1,N-1\}}, a_{N-1}, b_{N-1}) \cdot \mathbb{P}(s_{\{1,N-1\}}|h_{N-1}) \cdot x_{s_{\{1,N-1\}},a_{N-1}}}{\sum_{s'_{\{1,N-1\}}} \mathbb{P}(s'_{\{1,N-1\}}|h_{N-1}) \cdot x_{s'_{\{1,N-1\}},a_{N-1}}} \cdot \\ &\frac{\mathbb{P}(s_{\{2,N\}}|s_{\{2,N-1\}}, a_{N-1}, b_{N-1}) \cdot \mathbb{P}(s_{\{2,N-1\}}|h_{N-1}) \cdot y_{s_{\{2,N-1\}},a_{N-1}}}{\sum_{s'_{\{2,N-1\}}} \mathbb{P}(s'_{\{2,N-1\}}|h_{N-1}) \cdot y_{s'_{\{2,N-1\}},b_{N-1}}},\end{aligned} \tag{4.18}$$

where $\mathbb{P}(s_{\{1,N\}}|s_{\{1,N-1\}},a_{N-1},b_{N-1})\cdot\mathbb{P}(s_{\{2,N\}}|s_{\{2,N-1\}},a_{N-1},b_{N-1})$ is the state transition probability $\mathbb{P}(s_N|s_{N-1},a_{N-1},b_{N-1})=q(s_N|s_{N-1},a_{N-1},b_{N-1})$, as defined in Equation (4.9). The product of $\mathbb{P}(s_{\{1,N-1\}}|h_{N-1})\cdot\mathbb{P}(s_{\{2,N-1\}}|h_{N-1})$ is $\rho_{N-1}(s_{N-1})$ according to the definition of the belief in Equation (4.12). Therefore, the Equation (4.18) can be further written as

$$\rho_N(s_N)=\frac{\sum_{s_{N-1}}q(s_N|s_{N-1},a_{N-1},b_{N-1})\cdot\rho_{N-1}(s_{N-1})\cdot x_{s_{\{1,N-1\}},a_{N-1}}\cdot y_{s_{\{1,N-1\}},b_{N-1}}}{\sum_{s'_{N-1}}\rho_{N-1}(s_{N-1})\cdot x_{s'_{\{1,N-1\}},a_{N-1}}\cdot y_{s'_{\{2,N-1\}},b_{N-1}}},$$

and until now, $\rho_N(s_N)$ is computed by assuming the condition that the game does not end at N stage is satisfied. Suppose the game will go to state $\emptyset$ after $N-1$ stage (i.e., game will end at N stage, such that $N=E$), we have

$$\begin{aligned}&\mathbb{P}(\emptyset|h_N,E>N-1)=\\&=\frac{\sum\limits_{s_{N-1}}q(\emptyset|s_{N-1},a_{N-1},b_{N-1})\cdot\rho_{N-1}(s_{N-1})\cdot x_{s_{\{1,N-1\}},a_{N-1}}\cdot y_{s_{\{2,N-1\}},b_{N-1}}}{\sum\limits_{s'_{N-1}}\rho_{N-1}(s'_{N-1})\cdot x_{s'_{\{1,N-1\}},a_{N-1}}\cdot y_{s'_{\{2,N-1\}},b_{N-1}}},\end{aligned}\tag{4.19}$$

and $q(\emptyset|s_{N-1},a_{N-1},b_{N-1})>0$, which describes the likelihood that the game with stop after $N-1$ stage is positive. Therefore, similar to that in [120], the belief $\rho_N(s_N):=\mathbb{P}(s_N|h_N,E>N)$ of the current game state for stochastic game with asymmetric information and positive stop probabilities is conditioned on that the game does not end. Therefore, taking into consideration that the game will end at N stage, a belief about the game state s_N at the N stage can be computed as

$$\begin{aligned}\rho_N(s_N)&=\frac{1}{1-\mathbb{P}(\emptyset|h_N,E>N-1)}\cdot\\&\quad\frac{\sum\limits_{s_{N-1}}q(s_N|s_{N-1},a_{N-1},b_{N-1})\cdot\rho_{N-1}(s_{N-1})\cdot x_{s_{\{1,N-1\}},a_{N-1}}\cdot y_{s_{\{2,N-1\}},b_{N-1}}}{\sum\limits_{s'_{N-1}}\rho_N(s'_{N-1})\cdot x_{s'_{\{1,N-1\}},a_{N-1}}\cdot y_{s'_{\{2,N-1\}},b_{N-1}}}\\&=\frac{\sum\limits_{s_{N-1}}\rho_{N-1}(s_{N-1})\cdot q(s_N|s_{N-1},a_{N-1},b_{N-1})\cdot x_{s_{\{1,N-1\}},a_{N-1}}\cdot y_{s_{\{2,N-1\}},b_{N-1}}}{\sum\limits_{s'_N}\sum\limits_{s_{N-1}}\rho_{N-1}(s_{N-1})\cdot q(s'_N|s_{N-1},a_{N-1},b_{N-1})\cdot x_{s_{\{1,N-1\}},a_{N-1}}\cdot y_{s_{\{2,N-1\}},b_{N-1}}}.\end{aligned}\tag{4.20}$$

It can be seen that the belief that the player forms about next state s_N at N stage depends in general both state transition probabilities and decisions a_{N-1} and b_{N-1} ($x_{s_{\{1,N-1\}},a_{N-1}}$ and

$y_{s_{\{2,N-1\}},b_{N-1}}$ are probabilities for taking actions a_{N-1} and b_{N-1}, respectively). The decisions of a_{N-1} and b_{N-1} depend on players' private local information at $N-1$ stage (see Equations (4.10) and (4.11)). However, since the game is played with perfect recall, when updating the belief about the game state s_N at N stage, such decisions a_{N-1} and b_{N-1} are already *past* actions and are common information for all players. It can be seen from Equation (4.13) that both players have the same belief under the assumption that the game does not stop at stage N. For example, player 1 has a belief about player 2's state (which is $\mathbb{P}(s_{2,N}|h_N)$), and knows his/her private state $s_{1,N}$ precisely. Also, player 1 knows what player 2 believes, i.e., $\mathbb{P}(s_{1,N}|h_N)$ is available to player 1. Since the situation is symmetric (player 2 knows the respective information about player one), the belief is the same for both players. When the non-stopping assumption is relaxed, both players can also obtain the same belief. Therefore, in the game setting, due to the independence of game states and simultaneously moving of both players, both players can share the same belief value $\rho_N(s_N)$ about the current game state s_N at N stage. Provided that the game continues, state s_N is chosen according to $\rho_N(s_N) = \mathbb{P}(s_N|h_N, E > N)$, the immediate payoff $g_{\{1,s_N\}}(a_N, b_N)$ is received at player 1 and the immediate payoff $g_{\{2,s_N\}}(a_N, b_N)$ is received at player 2. Then, both two players compute their belief $\rho_{N+1}(s_{N+1})$ on next game state s_{N+1} at $N+1$ stage.

4.4.2 Cost and Reward Analysis

Each player has a payoff matrix at each state of the non-zero-sum game. The payoff includes costs (negative values) and rewards (positive values) associated with the actions of the attacker and the defender. The attacker's actions mostly involve rewards (otherwise, the attacker has no motivation to launch an attack), which are qualified in terms of the amount of damage he/she does to the network. Different from conventional ICT systems, smart grids are cyber-physical systems; hence, cyber attacks on smart grids can cause not only cyber damage in the communication network, but also physical damage to the power grid, i.e., damage beyond the communication network. Furthermore, due to the interdependency of the power grid and other critical infrastructures, a disruptive event in the power grid can lead to the disruption of other critical infrastructures, resulting in a cascading failure. Such rewards, however, are difficult to quantify.

In the game model, the reward for an attacker's action is defined as a function of dysfunctional (dysfunctional and malfunctioning are interchangeable in this thesis) nodes resulted from the cyber attack's cascading effects on the interdependent power grids and communication

networks. For example, a DDoS attack happens, it can cause 10 IEDs in the communication network and one distribution substation in the power grid to become ysfunctional. Suppose that the impact of this DDoS attack on confidentiality, integrity, and availability of these 10 IEDs in the communication network is 5, the distribution substation is with a node weight of 0.6, the disruptive magnitude of this distribution substation is 9, and the time needed for bringing this disrupted distribution substation back to normal operation is 5. For the attacker, his/her reward is $5+5\cdot(9\cdot 0.6)=32$. There are certainly costs for players to carry out an action. For example, the attacker needs to explore attack tools or computers to launch an attack. For a defender, if he/she needs to deploy an IDS to nodes in the smart grid communication network to defend against DDoS attack, the company needs to calculate the financial budget for buying an IDS. Chapter 5 presents a mathematical model to capture the cascading effects caused by a cyber attack in an interdependent power grid and communication network in smart grids, quantifies disruption characterisations in power grids, and formalises the payoff matrices for the designed attacker-defender stochastic game-theoretic model.

4.4.3 Finding Nash Equilibria

When dealing with strategic players with inter-dependent payoffs (for example, the attacker's rewards might somehow be losses of the defender), investigating equilibria, mostly notably Nash equilibria, is a method of predicting their decisions. If we restrict our attention to pure strategies (i.e., actions), a Nash equilibrium may not exists, this is the reason that this work considers only behaviour strategies and the probability used by both players to choose among pure strategies. The attacker-defender game with asymmetric information has finite states and the action spaces AS_1 and AS_2 (see Section 4.3.2) are finite. The major differences between this attacker-defender game and the SGLIOS with positive stop probabilities are that this attacker-defender game is a non-zero-sum one and the belief system updates in this attacker-defender game are jointly conditioned on strategies from both players. In the SGLIOS with positive stop probabilities, the belief is conditioned only on the strategy of the informed player; while in the attacker-defender game, the belief is conditioned on strategies of both players. If the probability that taking action b_{N-1} is zero (where the denominator of Equation (4.20) will also be zero), the history h_N will not be observed, which will not happen under the assumption that the game does not end at $N-1$ stage. It was said that the belief in the SGLIOS with positive stop probabilities is continuous [122]. The same continuity property extends to the belief in the proposed attacker-defender game. In the designed attacker-defender game, both players

are informed about the belief of game states. Hence, each player can be taken as the informed player in the SGLIOS with positive stop probabilities. It is proved in [120] that the informed player has a stationary optimal strategy (the interested reader is referred to [120, 122] for proof details and this thesis is not going to repeat them here again). However, [120] does not provide a systematic way to find such optimal strategies.

The designed attacker-defender game is non-zero-sum. It is stated in [96] that every non-zero-sum stochastic game has at least one (not necessary unique) Nash equilibrium in stationary strategies and finding these equilibria is non-trivial. The attacker-defender game with uncertainty about current game state for both players makes it extremely challenging. Given the strategies of both players, players continue to accumulate the immediate payoffs. Once the end state of the game is reached, the game is over and no more accumulations are possible. Each player wishes to maximise his/her expected payoff at state s_N. This maximisation, in turn, yields player's value of the game. Hence, if the value of the game Γ_N exists, let the vector of values for player 1 be $\mathbf{v}_1$, where $\mathbf{v}_1 = (v_{1,s_1}, v_{1,s_2}, \cdots, v_{1,s_\ell}, \cdots, v_{1,s_{k_C}})$ (v_{1,s_ℓ} ($\ell \in \{1,2,\cdots, k_C\}$) is player 1's value of the game in state $s_{1,\ell}$ and $v_{1,s_\ell} \in \mathbb{R}$) and the vector of values for player 2 be $\mathbf{v}_2$, where $\mathbf{v}_2 = (v_{2,s_1}, v_{2,s_2}, \cdots, v_{2,s_\ell}, \cdots, v_{2,s_{k_C}})$ (v_{2,s_ℓ} ($\ell \in \{1,2,\cdots, k_C\}$) is player 2's value of the game in state s_ℓ and $v_{2,s_\ell} \in \mathbb{R}$). The value of each player (either the attacker or the defender) includes both short-term (i.e., immediate) payoff and long-term payoff (which is given by the expected value of the sum of state payoffs from the current state) [123]. Taking the value for player 1 for instance, his/her value can be recursively defined as (that for player 2 can be defined in the same way)

$$v_{1,s_N}(\rho_N(s_N)) := \max_{\mathbf{x}_N} \min_{\mathbf{y}_N} \sum_{\mathbf{x}_N, \mathbf{y}_N} \left(\rho_N(s_N)\mathbf{G}_{\{1,s_N\}} + \mathbf{T}_1(s_N, \mathbf{v})\right), \tag{4.21}$$

where matrix $\mathbf{T}_1(s_N, \mathbf{v})$ is the matrix $[[q(s_1|s_N, a_N, b_N)\cdots q(s_\ell|s_N, a_N, b_N)\cdots]^T \mathbf{v}]_{a_N \in AS_1, b_N \in AS_2}$ and $\{s_1, \cdots, s_\ell, \cdots\}$ is the set of states that state s_N can move to with the state transition probability $q(s_\ell|s_N, a_N, b_N)$ ($a_N \in AS_1$ and $b_N \in AS_2$ are actions that player 1 and player 2 take at stage N, respectively). The vector $\mathbf{v}$ is a value vector (a sub-vector of the game value vector that is defined above) for player 1 and it depends on the states that the current state s_N can transition to. The matrix $\mathbf{T}_1(s_N, \mathbf{v})$ represents the long-term payoff (i.e.,future payoff) in a game matrix form. For example, suppose that in a game, there are two players. One player (the row player and also the first player) has two actions: "T" and "B" and another player (the column player and also the second player) has two actions: "L" and "R". The payoffs and transition

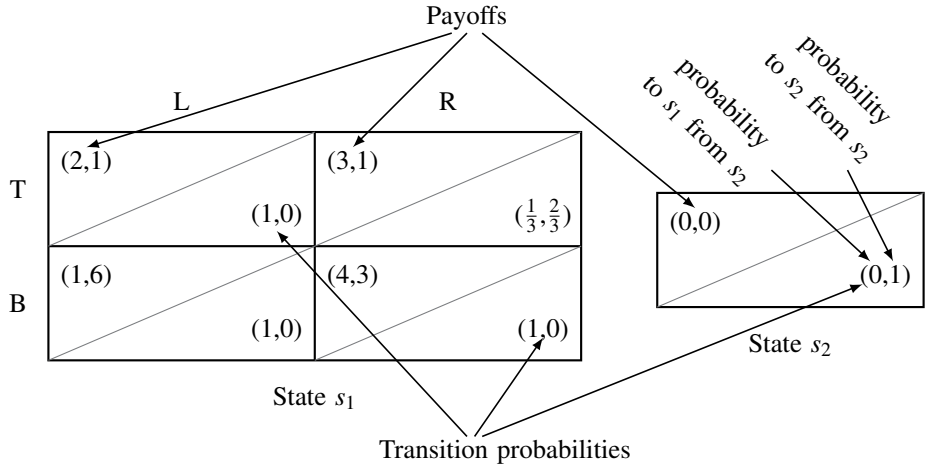


Figure 4.4: A sample stochastic game with two states.

probabilities are shown in Figure 4.4 (this style of representation in Figure 4.4 is based on that in [98]). For the first player, his/her value for state s_1 can be calculated as

$$v_{1,s_1} = \max_{\mathbf{x}_{s_1}} \min_{\mathbf{y}_{s_1}} \left(\begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} + \begin{bmatrix} 1 \cdot v_{1,s_1} & \frac{1}{3} \cdot v_{1,s_1} \\ 1 \cdot v_{1,s_1} & 1 \cdot v_{1,s_1} \end{bmatrix} \right),$$

where $\begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix}$ is the matrix $\mathbf{G}_{\{1,s_1\}}$, $\begin{bmatrix} 1 \cdot v_{1,s_1} & \frac{1}{3} \cdot v_{1,s_1} \\ 1 \cdot v_{1,s_1} & 1 \cdot v_{1,s_1} \end{bmatrix}$ is the matrix $\mathbf{T}(s_1, \mathbf{v})$, and the vector $\mathbf{v}$ in this example is the vector $[v_{1,s_1} \;\; v_{1,s_1} \;\; v_{1,s_1} \;\; v_{1,s_1}]$.

A pair of strategy sequence $(\mathbf{x}^*, \mathbf{y}^*)$ forms (Nash) equilibria with strategy pair $(\mathbf{x}^*_{s_N}, \mathbf{y}^*_{s_N})$ if

$$\mathcal{H}_1(\mathbf{x}^*, \mathbf{y}^*) \geq \mathcal{H}_1(\mathbf{x}, \mathbf{y}^*), \forall \mathbf{x} \in \Omega^{m_1},$$
$$\mathcal{H}_2(\mathbf{x}^*, \mathbf{y}^*) \geq \mathcal{H}_2(\mathbf{x}^*, \mathbf{y}), \forall \mathbf{y} \in \Omega^{m_2},$$

where $\geq$ is used to mean at every stage N, the left-hand-side with strategy profile $(\mathbf{x}^*_{s_N}, \mathbf{y}^*_{s_N})$ is greater than the right-hand-side with strategy $(\mathbf{x}_{s_N}, \mathbf{y}^*_{s_N})$ or strategy $(\mathbf{x}^*_{s_N}, \mathbf{y}_{s_N})$. Therefore, the pair of strategy profile $(\mathbf{x}^*_{s_N}, \mathbf{y}^*_{s_N})$ $(N \in \mathbb{N})$ is said to be a Nash equilibrium strategy. At this equilibrium, there is no incentive for either player to deviate from his/her equilibrium strategy $\mathbf{x}^*_{s_N}$ or $\mathbf{y}^*_{s_N}$ at any stage N of the game. In each pair of equilibrium strategies, a strategy for one player is a best-response to the other player and vice versa. A deviation means that one or both of them may have a lower expected payoff, i.e., $\mathcal{H}_1(\mathbf{x}, \mathbf{y}^*)$ or $\mathcal{H}_2(\mathbf{x}^*, \mathbf{y})$.

A one-player game with uncertainty about state due to imperfect information is equivalent to the well-known partially observable Markov decision process (POMDP). Solving those processes gives a strategy that describes the optimal action to take for a given belief about the current state. POMDPs mainly formulate centralised stochastic control problem with non-strategic decision makers [108] and there is no much room for strategic interplays. While asymmetric information leads to an interesting strategic play, allows models to be formulated within the framework of game theory [124]. The standard POMDP solvers cannot directly applied to solve Equation (4.21), which does not have a linear structure. [125] transformed the stochastic game with asymmetric information to another game with symmetric information. Consequently, a backward induction algorithm is provided to find Markov perfect equilibria (MPE) of the transformed game, with is equivalent to Nash equilibria of the original game with asymmetric information. A methodology based on a two-step backward-forward recursion is developed to find structured Bayesian perfect equilibria (SPBE) for dynamic games with asymmetric information [126]. An illustrative example of a two-stage public goods game is given to present the application of the proposed game model and the computation of SPBE. [127] introduced a subclass of perfect Bayesian equilibria (PBE) called common information based perfect Bayesian equilibria (CIB-PBE) and provided a sequential decomposition (which leads to a backward induction algorithm) to find such equilibria. [127] illustrated the developed sequential decomposition with a two-agent multiple access broadcast game. In the game problem of this thesis, it can be seen from Equation (4.20) that the belief $\rho_N(s_N)$ about next game state s_N at stage N is updated according to strategies from both players. However, the belief $\rho_N(s_N)$ cannot be updated from Baye's rule. Therefore, the *consistency* requirements [71, 92, 128] of PBE is not satisfied and the Nash equilibria, if exist, are no longer PBE.

The authors of [129] formulated a stochastic game problem as a nonlinear programming and it is shown in [130] that stationary equilibria in discounted and limiting average finite state/action space stochastic games are equivalent to global optima of certain non-linear programs. In order to find Nash equilibria for the designed attacker-defender non-zero-sum game in smart grid communication networks, based on the formed work [129, 130], this thesis studies NLP formulation of the attacker-defender non-zero-sum stochastic game with finite number of strategies and asymmetric information from one-stage and two-stage games, and then extends the results to M-stage games ($M \in \mathbb{N}$). The theorem and proof of a global minimum to be a (Nash) equilibrium with equilibrium payoff can be found in [130, 131], this work is not go-

ing to repeat them here again, whereas it provides here an easy-to-follow method to find such (Nash) equilibria in the designed attacker-defender game.

A. One-Stage Games

A one-stage game Γ_1 is a game which ends after the first stage (where the state space $S = \{s_1, \emptyset\}$ (the state $\emptyset$ is adjoined to the set of spaces S, but $\emptyset$ is not a real state of the game)). The state s_1 is associated with two payoff matrices : $\mathbf{G}_{\{1,s_1\}}$ for player 1 and $\mathbf{G}_{\{2,s_1\}}$ for player 2. Such an one-stage game has values of

$$v_{1,s_1} = \max_{\mathbf{x}_{s_1}} \min_{\mathbf{y}_{s_1}} \mathbf{x}_{s_1} \cdot \rho_1(s_1) \cdot \mathbf{G}_{\{1,s_1\}} \cdot \mathbf{y}_{s_1}^T, \tag{4.22}$$

$$v_{2,s_1} = \max_{\mathbf{y}_{s_1}} \min_{\mathbf{x}_{s_1}} \mathbf{x}_{s_1} \cdot \rho_1(s_1) \cdot \mathbf{G}_{\{2,s_1\}} \cdot \mathbf{y}_{s_1}^T. \tag{4.23}$$

The equilibrium payoffs v_{1,s_1} and v_{2,s_1} in game Γ_1 can be written as the following NLP problem, which is named as NLP-1:

$$\begin{aligned} \text{minimize } \big(& v_{1,s_1} - \mathbf{x}_{s_1} \cdot \rho_1(s_1) \cdot \mathbf{G}_{\{1,s_1\}} \cdot \mathbf{y}_{s_1}^T \\ & + v_{2,s_1} - \mathbf{x}_{s_1} \cdot \rho_1(s_1) \cdot \mathbf{G}_{\{2,s_1\}} \cdot \mathbf{y}_{s_1}^T \big), \end{aligned}$$

subject to

$$\begin{aligned} &\text{(i)} \quad \rho_1(s_1)\mathbf{G}_{\{1,s_1\}}\mathbf{y}_{s_1}^T \leq v_{1,s_1}\mathbf{J}_{m_1}^T, \\ &\text{(ii)} \quad \rho_1(s_1)\mathbf{G}_{\{2,s_1\}}^T\mathbf{x}_{s_1}^T \leq v_{2,s_1}\mathbf{J}_{m_2}^T, \\ &\text{(iii)} \quad \sum_{a=1}^{m_1} x_{s_1,a} = 1 \quad \forall a \in AS_1, \\ &\text{(iv)} \quad x_{s_1,a} \geq 0 \quad \forall a \in AS_1, \\ &\text{(v)} \quad \sum_{b=1}^{m_2} x_{s_1,b} = 1 \quad \forall b \in AS_2, \\ &\text{(vi)} \quad x_{s_1,b} \geq 0 \quad \forall b \in AS_2, \end{aligned}$$

where the value $\rho_1 > 0$ is the prior belief of the initial state (i.e., the only one state in the one-stage game) and is provided by the system. Throughout this thesis, $\mathbf{J}_\ell$ is the $1 \times \ell$ ($\ell \in \{m_1, m_2\}$) row vector with all 1s. Constraints (i) and (ii) are the value bounds for the attacker-defender game, which are satisfied for any pair of strategy profile. The mixed strategies $\mathbf{x}_{s_1}$ and $\mathbf{y}_{s_1}$ are defined in Equations (4.1) and (4.2), respectively. Constraints (iii) - (vi) are conditions that

the probability $x_{s_1,a}$ to select action a for player 1 in state s_1 and the probability $y_{s_1,b}$ to select action b for player 2 in state s_1 is greater than zero and the sum of all such probabilities for each player is one. Any pair of strategy profile satisfies constraints (iii) - (vi). For one-stage games, the game ends after both players taking their strategies $(\mathbf{x}_{s_1}, \mathbf{y}_{s_1})$. In this one-stage game, each player (either the attacker or the defender) would play with the stationary strategy that maximises his/her expected immediate payoff at the current game stage. Hence $(\mathbf{x}^*_{s_1}, \mathbf{y}^*_{s_1})$ will be one optimal strategy profile.

There can be mutiple stationary Nash equilibria at each game state and hence there will be multiple global minima. For example, for a stochastic game with one stage and the payoff matrix for player 1 (who has three actions: A, B and C) and player 2 (who has two actions: D and E) is $\mathbf{G}_{\{1,s_1\}}$ and $\mathbf{G}_{\{2,s_1\}}$ respectively (to be noted that those values in payoff matrices are artificial numbers for illustration)

$$\mathbf{G}_{\{1,s_1\}} = \begin{array}{c|cc} & \text{D} & \text{E} \\ \hline \text{A} & 6 & 2 \\ \text{B} & 1 & 3 \\ \text{C} & 5 & 4 \end{array}, \text{and} \quad \mathbf{G}_{\{2,s_1\}} = \begin{array}{c|cc} & \text{D} & \text{E} \\ \hline \text{A} & 4 & 3 \\ \text{B} & 1 & 5 \\ \text{C} & 2 & 2 \end{array}.$$

This is a one-stage game. Presuming that each player knows that the probability distribution $\rho_1(s_1)$ is 1, and the game value for player 1 (the row player) and player 2 (the column player) are denoted as v_{1,s_1} and v_{2,s_1}, respectively. Therefore, the NLP-1 formulation of this one-stage game can be expressed as

$$\text{minimize} \left(v_{1,s_1} - \mathbf{x}_{s_1} \cdot \begin{bmatrix} 6 & 2 \\ 1 & 3 \\ 5 & 4 \end{bmatrix} \cdot \mathbf{y}^T_{s_1} + v_{2,s_1} - \mathbf{x}_{s_1} \cdot \begin{bmatrix} 4 & 3 \\ 1 & 5 \\ 2 & 2 \end{bmatrix} \cdot \mathbf{y}^T_{s_1} \right),$$

subject to

$$\text{(i)} \quad \begin{bmatrix} 6 & 2 \\ 1 & 3 \\ 5 & 4 \end{bmatrix} \mathbf{y}_{s_1}^T \leq v_{1,s_1} \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}^T,$$

$$\text{(ii)} \quad \begin{bmatrix} 4 & 3 \\ 1 & 5 \\ 2 & 2 \end{bmatrix}^T \mathbf{x}_{s_1}^T \leq v_{2,s_1} \begin{bmatrix} 1 & 1 \end{bmatrix}^T,$$

$$\text{(iii)} \quad \sum_{a=1}^{3} x_{s_1,a} = 1 \quad \forall a \in \{A,B,C\},$$

$$\text{(iv)} \quad x_{s_1,a} \geq 0 \quad \forall a \in \{A,B,C\},$$

$$\text{(v)} \quad \sum_{b=1}^{2} x_{s_1,b} = 1 \quad \forall b \in \{D,E\},$$

$$\text{(vi)} \quad x_{s_1,b} \geq 0 \quad \forall b \in \{D,E\}.$$

There are three stationary mixed equilibria available for this one-stage game (by solving a constrained minimisation problem), which are shown in Table 4.1 with their corresponding values for each player. All Nash equilibria and game values in Table 4.1 are further verified by the Gambit software tool [95]. Suppose that the first player is the defender of a system and the second player is the attacker. For the first Nash equilibrium in Table 4.1, to obtain maximum payoffs ("6" for the defender and "5" for the attacker, as shown in Table 4.1), the defender is suggested play the pure strategy "A" with a probability of 1 (i.e., play the action "A" in all game repetitions) and the attacker play the pure strategy "D" with a probability of 1. The same interpretation can be applied to the third Nash equilibrium, i.e., the defender plays the pure strategy "C" with a probability of 1 and the attacker plays the pure strategy "E" with a probability of 1 to maximise their payoffs. Regarding the second Nash equilibrium, the game suggests that the defender play his/her pure strategy "C" with a probability of 1, while it suggests that the the attacker play his/her pure strategy "D" with a probability of approximately 0.67 and his/her pure strategy "E" with a probability of approximately 0.33. If actions (i.e., pure strategies) are continuously and taking daily (24h), the mixed Nash equilibrium strategy $\left(\frac{2}{3}, \frac{1}{3}\right)$ for the attacker can also be interpreted that the attacker temporarily runs the pure strategy "D" for approximately 16h and runs the pure strategy "E" for the remainder of the

day. If the actions "D" and "E" are instantaneous actions (which are taken at discrete time instants), the mixed Nash equilibrium strategy $\left(\frac{2}{3}, \frac{1}{3}\right)$ for the attacker can be interpreted as the (asymptotic) frequency with which the strategies "D" and "E" are chosen in the game. After obtaining the mixed Nash equilibrium, the defender and the attacker can subsequently use it in the following way: when the game begins, both players (the defender and the attacker) randomly choose actions (i.e., pure strategies) from their corresponding action spaces, a game payoff from the chosen action pair will be received at each player. When the game is played again, both players again randomly choose actions from their corresponding action spaces in this round. It is to be noted that the actions from both players in this round may be different from that taken in the previous round. A game payoff will again be received at each player. The actions in each round are chosen randomly, however, the player should be aware of that the (asymptotic) frequency of chosen actions must be that suggested from the mixed Nash equilibrium. Therefore, when averaging payoffs in all repetitions of the game, the average payoff is optimal for each player only if the actions are chosen with their frequencies that are prescribed by the equilibrium strategy. For example, for the attacker, in any game round, he/she should always aware of that the (asymptotic) frequencies of choosing actions "D" and "E" in all game repetitions should be $\frac{2}{3}$ and $\frac{1}{3}$, respectively.

# of Nash equilibrium	Player 1			Player 2		Game value	
	A	B	C	D	E	Player 1	Player 2
1	1	0	0	1	0	6	4
2	0	0	1	2/3	1/3	14/3	2
3	0	0	1	0	1	4	2

Table 4.1: Nash equilibria and their corresponding game values in the sampled game.

Though there may be many stationary Nash equilibria for one game, the objective of this work is to find one global minimum and its corresponding one stationary Nash equilibrium.

B. Two-Stage Games

A two-stage game ends after the second stage and the state space for a two-stage game is $S = \{s_1, s_2, \emptyset\}$ and each state is associated with two payoff matrices: state s_1 is associated with payoff matrices $\mathbf{G}_{\{1,s_1\}}$ and $\mathbf{G}_{\{2,s_1\}}$; state s_2 is associated with payoff matrices $\mathbf{G}_{\{1,s_2\}}$ and $\mathbf{G}_{\{2,s_2\}}$). The game has a non-negative probability to end at the first stage (from the assumption of positive stop probabilities). A two-stage game has values of

$$v_{1,s_2} = \max_{\mathbf{x}_{s_2}} \min_{\mathbf{y}_{s_2}} \mathbf{x}_{s_2} \cdot \rho_2(s_2) \cdot \mathbf{G}_{\{1,s_2\}} \cdot \mathbf{y}_{s_2}^T, \tag{4.24}$$

$$v_{2,s_2} = \max_{\mathbf{y}_{s_2}} \min_{\mathbf{x}_{s_2}} \mathbf{x}_{s_2} \cdot \rho_2(s_2) \cdot \mathbf{G}_{\{2,s_2\}} \cdot \mathbf{y}_{s_2}^T, \tag{4.25}$$

$$v_{1,s_1} = \max_{\mathbf{x}_{s_1}} \min_{\mathbf{y}_{s_1}} \mathbf{x}_{s_1} \cdot \left(\rho_1(s_1) G_{\{1,s_1\}} + \mathbf{T}_1(s_1, \mathbf{v})\right) \cdot \mathbf{y}_{s_1}^T,$$

$$v_{2,s_1} = \max_{\mathbf{y}_{s_1}} \min_{\mathbf{x}_{s_1}} \mathbf{x}_{s_1} \cdot \left(\rho_1(s_1) G_{\{2,s_1\}} + \mathbf{T}_2(s_1, \mathbf{v})\right) \cdot \mathbf{y}_{s_1}^T,$$

where matrices $\mathbf{T}_1(s_1, \mathbf{v})$ and $\mathbf{T}_2(s_1, \mathbf{v})$ denote the long term payoff that can be achieved in state s_1 for player 1 and player 2, respectively. Those matrices $\mathbf{T}_1(s_1, \mathbf{v})$ and $\mathbf{T}_2(s_1, \mathbf{v})$ have the same meaning as the matrix $\mathbf{T}_1(s_N, \mathbf{v})$ introduced in Equation (4.21). Therefore, the equilibrium solution $(\mathbf{x}^*, \mathbf{y}^*)$ for a two-stage game is $(\mathbf{x}^*, \mathbf{y}^*) = (\mathbf{x}_{s_1}^*, \mathbf{y}_{s_1}^*, \mathbf{x}_{s_2}^*, \mathbf{y}_{s_2}^*)$. And the equilibrium solution $(\mathbf{x}^*, \mathbf{y}^*)$ can be obtained by the following nonlinear program problem, which is denoted as NLP-2:

$$\begin{aligned} \text{minimize } & \left(v_{1,s_2} - \mathbf{x}_{s_2} \cdot \rho_2(s_2) \cdot \mathbf{G}_{\{1,s_2\}} \cdot \mathbf{y}_{s_2}^T + v_{2,s_2} - \mathbf{x}_{s_2} \cdot \rho_2(s_2) \cdot \mathbf{G}_{\{2,s_2\}} \cdot \mathbf{y}_{s_2}^T + v_{1,s_1}\right. \\ & \left. - \mathbf{x}_{s_1} \cdot \left(\rho_1(s_1) G_{\{1,s_1\}} + \mathbf{T}_1(s_1, \mathbf{v})\right) \cdot \mathbf{y}_{s_1}^T + v_{2,s_1} - \mathbf{x}_{s_1} \cdot \left(\rho_1(s_1) G_{\{2,s_1\}} + \mathbf{T}_2(s_1, \mathbf{v})\right) \cdot \mathbf{y}_{s_1}^T\right), \end{aligned}$$

subject to

$$\begin{aligned} &\text{(i)} \quad \rho_2(s_2) \mathbf{G}_{1,s_2} \mathbf{y}_{s_2}^T \leq v_{1,s_2} \mathbf{J}_{m_1}^T, \\ &\text{(ii)} \quad \rho_2(s_2) \mathbf{G}_{2,s_2}^T \mathbf{x}_{s_2}^T \leq v_{2,s_2} \mathbf{J}_{m_2}^T, \\ &\text{(iii)} \quad \rho_1(s_1) \mathbf{G}_{1,s_1} \mathbf{y}_{s_1}^T + \mathbf{T}_1(s_1, \mathbf{v}) \mathbf{y}_{s_1}^T \leq v_{1,s_1} \mathbf{J}_{m_1}^T, \\ &\text{(iv)} \quad \rho_1(s_1) \mathbf{G}_{2,s_1}^T \mathbf{x}_{s_1}^T + \mathbf{T}_2(s_1, \mathbf{v})^T \mathbf{x}_{s_1}^T \leq v_{2,s_1} \mathbf{J}_{m_2}^T, \\ &\text{(v)} \quad \sum_{a=1}^{m_1} x_{s_N,a} = 1 \quad \forall a \in AS_1, N \in \{1,2\}, \end{aligned}$$

$$\text{(vi)} \quad x_{s_N,a} \geq 0 \quad \forall a \in AS_1, N \in \{1,2\},$$

$$\text{(vii)} \quad \sum_{b=1}^{m_2} y_{s_N,b} = 1 \quad \forall b \in AS_2, N \in \{1,2\},$$

$$\text{(viii)} \quad y_{s_N,b} \geq 0 \quad \forall b \in AS_2, N \in \{1,2\},$$

$$\text{(ix)} \quad \rho_2(s_2) = \mathbb{P}(s_2|h_2, E > 2),$$

where (ix) is a prior belief constraint and other constraints are similar to those described in the one-stage game. According to Equation (4.20), the beliefs on the current state s_N depends on the belief value of the previous one state and the action profile in the previous one stage. Such dependencies make NLP-2 complex. The objective of a player is to maximise his/her total expected payoff (see Equation (4.7)). If a player knew how to play optimally from the next stage on, then, at the current stage, he/she would play with such strategies to not only maximise the expected immediate payoff at the current stage but also maximise the expected payoff possibly incurred in future stages. In the two-stage game Γ_2, the belief values for both states are correlated. The game ends after the second stage, however, the value of the second state depends on the belief value from the first state (see Equations (4.24) and (4.25)). Moreover, the value of the first state depends partially on that of the second state as a long-term payoff. Additionally, the state transition probability (see Section 4.3.4) depends on the action profile of the current game stage. Therefore, each player (either the attacker or the player) is not only concerned with the immediate outcome of his/her action but also the future consequences of his/her strategies for the current game state. NLP-2 finds global minima by embodying all the information (including belief values and state transition probabilities) through its computation.

C. M-Stage Games

The two-stage games can be extended to M-stage games where the game ends after the M stage (i.e., $E > M$ and $M > 2$). The payoff of the both players at stage M ($M \in \mathbb{N}$) can be written as that shown in Equation (4.21). Analogously, the equilibrium solution $(\mathbf{x}^*, \mathbf{y}^*) = (\mathbf{x}_{s_1}, \mathbf{y}_{s_1}, \mathbf{x}_{s_2}, \mathbf{y}_{s_2}, \cdots, \mathbf{x}_{s_N}, \mathbf{y}_{s_N}, \cdots, \mathbf{x}_{s_M}, \mathbf{y}_{s_M})$ for M-stages games can be obtained by solving the

following nonlinear program problem, which is denoted as NLP-M:

$$\begin{aligned}\text{minimize} \quad & \sum_{N=1}^{M-1} \big(v_{1,s_M} - \mathbf{x}_{s_M} \cdot \rho_M(s_M) \cdot \mathbf{G}_{1,s_M} \cdot \mathbf{y}_{s_M}^T + v_{2,s_M} - \mathbf{x}_{s_M} \cdot \rho_M(s_M) \cdot \mathbf{G}_{2,s_M} \cdot \mathbf{y}_{s_M}^T \\ & + v_{1,s_N} - \mathbf{x}_{s_N} \cdot (\rho_N(s_N)\mathbf{G}_{1,s_N} + \mathbf{T}_1(s_N, \mathbf{v})) \cdot \mathbf{y}_{s_N}^T + v_{2,s_N} - \\ & \mathbf{x}_{s_N} \cdot (\rho_N(s_N)\mathbf{G}_{2,s_N} + \mathbf{T}_2(s_N, \mathbf{v})) \cdot \mathbf{y}_{s_N}^T \big),\end{aligned}$$

subject to

$$\begin{aligned}
&\text{(i)} \quad \rho_M(s_M)\mathbf{G}_{1,s_M}\mathbf{y}_{s_M}^T \leq v_{1,s_M}\mathbf{J}_{m_1}^T, \\
&\text{(ii)} \quad \rho_M(s_M)\mathbf{G}_{2,s_M}^T\mathbf{x}_{s_M}^T \leq v_{2,s_M}\mathbf{J}_{m_2}^T, \\
&\text{(iii)} \quad \rho_N(s_N)\mathbf{G}_{1,s_N}\mathbf{y}_{s_N}^T + \mathbf{T}_1(s_N, \mathbf{v})\mathbf{y}_{s_N}^T \leq v_{1,s_N}\mathbf{J}_{m_1}^T, \forall N \in \{1,2,\cdots,M-1\}, \\
&\text{(iv)} \quad \rho_N(s_N)\mathbf{G}_{2,s_N}^T\mathbf{x}_{s_N}^T + \mathbf{T}_2(s_N, \mathbf{v})^T\mathbf{x}_{s_N}^T \leq v_{2,s_N}\mathbf{J}_{m_2}^T, \forall N \in \{1,2,\cdots,M-1\}, \\
&\text{(v)} \quad \sum_{a=1}^{m_1} x_{s_N,a} = 1 \quad \forall a \in AS_1, N \in \{1,2,\cdots,M\}, \\
&\text{(vi)} \quad x_{x_N,a} \geq 0 \quad \forall a \in AS_1, N \in \{1,2,\cdots,M\}, \\
&\text{(vii)} \quad \sum_{b=1}^{m_2} y_{s_N,b} = 1 \quad \forall b \in AS_2, N \in \{1,2,\cdots,M\}, \\
&\text{(viii)} \quad y_{s_N,b} \geq 0 \quad \forall b \in AS_2, N \in \{1,2,\cdots,M\}, \\
&\text{(ix)} \quad \rho_N(s_N) = \mathbb{P}(s_N|h_N, E > M), N \in \{1,2,\cdots,M\}.
\end{aligned}$$

Because of the recursion definition of belief values of constraint (ix) and the recursive optimization involved in the long-term payoff (i.e., $\mathbf{T}_1(s_N, \mathbf{v})$ or $\mathbf{T}_2(s_N, \mathbf{v})$) of constraints (iii) and (iv), it is non-trivial to find global minima. Chapter 6 will give out an instantiation of game equilibrium finding with a standard nonlinear program solver.

4.5 Summary

This chapter investigated the designing of a stochastic game-theoretic model to assess the threat of multistage cyber attacks in smart grid communication networks. Firstly, the general stages of a multistage cyber attack on smart grids was described. Those stages were generalized in terms of reconnaissance, network scan, weaponization and enablement, concealment, and penetration. In order to assess threats of multistage cyber attacks, an attacker-defender stochastic game-theoretic model was designed according to the characteristics of the interactions between

the attacker and the defender in smart grid communication networks. The ingredients of the designed stochastic game-theoretic model was elaborated in detail in this chapter. Due to the information asymmetry of the interactions between the attacker and the defender in the stochastic game-theoretic model, either of both players knows the exact current game state. Therefore, this chapter proposed a belief-updating mechanism for both players to form a common belief about the current state of the game. This chapter briefly analysed the cost and reward of players' actions to formulate payoff matrices for the designed attacker-defender stochastic game-theoretic model. It further discussed the computation of Nash equilibria for the designed attacker-defender stochastic game-theoretic model. In the next chapter, a cost and reward analysis beyond smart grid communication networks will be discussed in detail with a view to formulating players' payoffs for the designed stochastic game-theoretic model.

Chapter 5

Cost and Reward Analysis Beyond Smart Grid Communication Networks

5.1 Introduction

The most critical component in a game-theoretic analysis is to formulate a payoff (or a utility) of the players in ways that mimic the desirability of an outcome for players. Payoffs can be a combination of costs (e.g., how many resources an attacker needs) and rewards (e.g., the amount of damage an attacker does to the system) associated with the actions of the attacker and the defender. The designed attacker-defender stochastic game-theoretic model is restricted to the scope of an attack event and the consequences of certain actions on information security (i.e., confidentiality, integrity, and availability), physical damage, and the cost of launching each action. This thesis considers those consequences as important factors in payoff formulation. The behaviour of the game must follow intuitive observations about the players and their consequences on the whole system. As discussed in Chapter 1, a cyber attack on the communication network in smart grids can cause physical damage to power nodes in smart grids, owning to the interdependency of the communication network and the power grid. Therefore, the reward for an attacker's action is mostly defined as the amount of service disruption when the system is brought from one state to another. Moreover, a failed power node can also cause the dysfunctionality of dependent nodes in the communication network. This may happen repeatedly and lead to a cascade of failures. Smart grids are highly heterogeneous, with failure in one facility leading to damage or failure in another nearby facility. It has been shown that interdependent networks are more vulnerable to failures than individual networks in isolation

[39, 132, 133], while cascading failures are rarely triggered by random breakdowns [35, 134]. The strategical removal of one single node with a relatively small capacity parameter can affect more than 60% of the nodes in the network [134]. In fact, the removal of one single node of a communication network in the smart grid can cause local dysfunctionality and potentially lead to the complete malfunction of a power network [132], [134], [135]. In addition, human factors may also contribute to cascading events, for instance, inadequate behaviours from operators and a lack of untimeliness in power unit maintenance.

Failures propagating in one single network (either a communication network or a power network) are regarded as horizontal failures, whereas failures from a communication network to a power network, or vice versa, are regarded as vertical failures. Recent critical infrastructure readiness surveys have confirmed that cyber attacks can result in physical damage to critical infrastructures [136]. To prevent physical components from damage caused by cyber security events, protection systems are typically deployed in the electrical grid. These protection components are used to disconnect affected parts (e.g., lines, cables) in order to minimize the impact on the rest of the system. However, the protection system itself is not "failure proof". In fact, as pointed out in [137] , protection system malfunction has played a significant role in some of the largest blackout events, such as the very recent blackout in Ukraine [1]. Severe consequences of disruptions, such as loss of supply to a district or part of the city, are most likely caused by a combination of failure events [133, 138]. This chapter focuses on both vertical failure (i.e., interdependency failure) and horizontal failure (e.g., node overloading failure) propagation on functional interdependent communication networks and power networks in smart grids. This work studies the load redistribution rule among nodes in the power grid and analyses the robustness of interdependent networks, which are composed of directed networks. Specifically, it quantifies the rewards and costs of players by characterizing service disruption, as well as quantifying the impact of players' actions on information security, where all service disruptions and impacts on security information are resulted from cascading effects of targeted dysfunctional nodes in communication systems on interdependent power and communication systems.

To understand cascading effects in interdependent infrastructures, modelling and simulation approaches have been largely proposed in the literature [139]. The reason for this may be the lack of publicly available data on cyber security incidents. Complex networks [140] have been applied to model different types of networks, such as social networks, biological

[1] https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf (Retrieved:20/06/2017)

processes, the spread of diseases, the Internet, power grids, and citation networks [140]. Interdependent networks are complex networks that consist of two or more networks, which are interconnected and mutually dependent. Interdependency cascading failures have been copiously studied recently [35, 36, 37, 38, 39, 43, 141]. Previous studies on two interdependent coupled networks are restricted by the condition that each node in one network domain depends on one, and only one node in the other network domain, and vice versa [35, 36, 132]. However, in the real world, this assumption may not be valid. In the scenario of coupled power grids and communication networks, one power station provides power to more than one communication station, and one communication station controls more than one power station. As long as a communication station can obtain power from any power station, it can still function properly. One communication station is sufficient to make one power station functional. However, without any power, the communication station will fail; and, without control, the power station will also be dysfunctional. The work of [37] considered smart grids as interdependent complex networks. In the smart grid model of [37], each communication node has only one support link from the power grid, while each power station has multiple support links to provide power to communication nodes. The cause of cascading is the random attack or system failures in one network. [43] studied multiple support-dependent relations between two coupled networks under random attacks. Targeted attacks on interdependent networks have been studied in [35, 142]. A node with a higher link degree has a higher probability to be attacked and fail. In a power grid, when one node fails, its load will shift to nearby nodes, which may become overloaded and fail, leading to another kind of cascading failures, known as load overloading cascading failures or load propagation cascading failures [134, 143]. Such a phenomenon cannot be described simply by a pure topological model. [38] studied both load propagation cascading failures and interdependent cascading failures in a percolation-based mathematical model. In [38], both the power grid and the communication network were modelled as undirected networks, while the load of failed power nodes was *uniformly* distributed to the neighbouring power nodes. However, in real life, due to the heterogeneity of power grids, the load of failed nodes (if any) will hardly be redistributed at uniform randomness. To take this diversity (i.e., *non-uniformity* of load redistribution) into account, in the work, the load of failed nodes was *non-uniformly* redistributed to its direct neighbours, according to the weight of neighbouring power nodes. In turn, both the power grid and the communication network were modelled as fully directed networks, where nodes are heterogeneous.

This thesis presents a detailed percolation-like mathematical method for analysing cascading failure propagation in an interdependent power and communication network in order to measure its robustness against disruption. The ultimate goal of this chapter is to formulate the payoff (i.e., a cost-reward analysis) of both players (the attacker and the defender) in smart grids. One of the most important rewards for the attacker is his/her disruptive effects on power grids. This chapter mathematically quantifies the characterizations of disruptive effects from cyber attacks on a power grid using a cascading failure propagation model (including both horizontal and vertical cascading failures). In contrast to what has been presented on the existing literature, the initial failure is initiated by targeted attacks, resulting from actions of both the defender and the attacker. This thesis formulates players' payoffs in the form of objective utility functions, which describe the nature of the players, where the effect of a cyber attack on the physical power grid is regarded as a significant component.

5.2 Theoretical Model of Interdependent Power and Communication Networks

As described above, a smart grid is composed of a communication network G_C and a power network G_P. This work assumes all power generators (power plants or renewable energy generators), substations, IEDs, control centres, etc, to be nodes, especially communication nodes and power nodes. A graph representation $G = (Z, L)$ of the interdependent power and communication network structure is shown in Figure 5.1, where Z is the set of nodes and L is a set of links (links and edges are used interchangeably in this thesis). It is to be noted that links in Figure 5.1 are bidirectional. The interdependent networks consist of a communication network $G_C = (Z_C, L_C)$ and a power network $G_P = (Z_P, L_P)$, where $n_P = |Z_P|$ and $n_C = |Z_C|$ are the number of nodes in the power and communication networks, respectively, and $\xi_P = |L_P|$ and $\xi_C = |L_C|$ are the number of links (including both incoming and outgoing links) inside the power and communication networks, respectively.

There are two different types of nodes in the communication network G_C: *information relay nodes* and *control centres*. Control centres are responsible for monitoring and operating power nodes in the power network G_P, while information relay nodes are responsible for data communications and monitoring power nodes. This work models the power grid at the medium and low voltage network, and therefore, the nodes in G_P include generators (most of them are

renewable energy resources) and distribution substations. This work assumes that there are totally n_d distribution substations in the power network G_P.

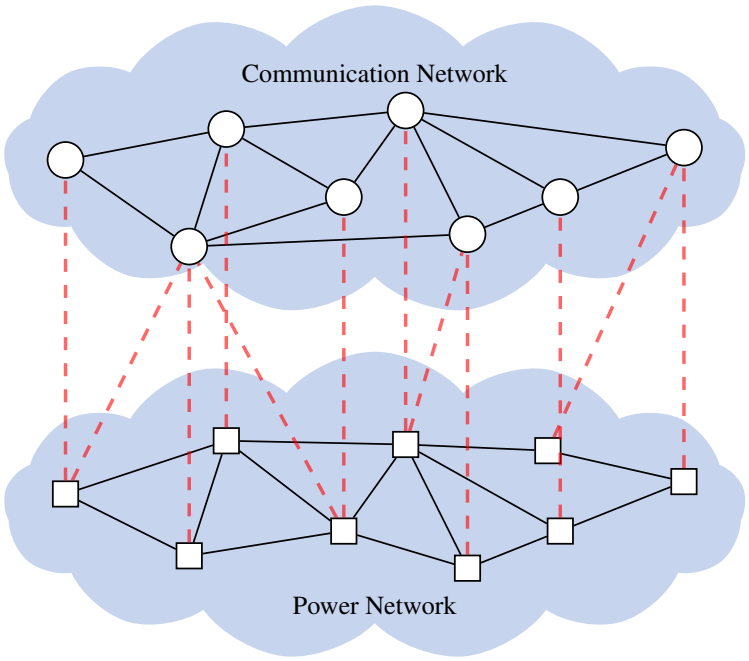


Figure 5.1: An example of interdependent power and communication networks.

In this work, both power and communication networks are modelled as directed network graph, where the direction stands for the direction of information flow or the direction of energy flow [144]. In a network G_ℓ ($G_\ell \in \{G_N, G_P\}$), nodes are connected with directed links using a degree distribution $p_\ell(j,k)$ (i.e., an arbitrary node in network G_ℓ has j incoming and k outgoing edges). This thesis refers to the links connecting nodes within the same network as *intra-links* (e.g., those solid lines in either the communication network or the power network in Figure 5.1) and those connecting nodes from two different networks as *inter-links* (also called support links [43], such as the dashed lines in Figure 5.1). The inter-links between communication network G_C and power network G_P are directed edges from one network to the other. In such case, G has a combined number of nodes $Z_C \cup Z_P$, a combined number of intra-links $L_C \cup L_P$ and a set of inter-links $L_{CP} \cup L_{PC}$ that connects G_C and G_P. Therefore, the total set of nodes in the interdependent network G is $Z = Z_C \cup Z_P$ and the total set of links $L = L_C \cup L_P \cup L_{CP} \cup L_{PC}$.

In a single isolated network, the giant cluster is used as an important metric to measure interdependent networks after cascading failures occur. In this thesis, the term "component" is used to refer to connected groups of nodes on the original network before any nodes have

failed and "cluster" refers to those after removing failed nodes. The avalanche size of cascade is measured by the relative size of the giant cluster. If there is a giant cluster, the members of that giant cluster, who are a finite fraction of all nodes in the network, are connected and functional, although the remaining nodes of the network are dysfunctional. A set of functional nodes V_C in a network G_C forms a giant cluster if (i) each pair of nodes in V_C is connected by a path (either forward or backward) leads to nodes in V_C of network G_C and (ii) each node has at least one support node in network G_P. Similarly, a set of functional node V_P in a network G_P forms a giant cluster if (i) each pair of nodes in V_P is connected by a path (either forward or backward) leads to nodes in V_P of network G_P and (ii) each node has at least one support node in network G_C.

This thesis is interested in the fraction of power nodes that can be removed at the end, i.e., the number of dysfunctional power nodes. However, since a node in a network has only two states: functional and dysfunctional. Therefore, instead of directly calculating the number of dysfunctional nodes, this thesis investigates the fraction of nodes that can survive at the end. There are studies that indicate a communication node can start to run on uninterruptible power supply (UPS) backup systems, instead of becoming dysfunctional immediately after losing its power supply from the grid system [36]. However, if the UPS runs out before the grid has recovered, the communication node will also fail. Therefore, this thesis considers the worst case such that the time when a node will fail does not make any difference. This work takes discrete time steps to describe the evolution of the system. In this thesis, a node is assumed to be functional only if it satisfies the following conditions [38, 132, 145]:

(i) it has at least one inter link with a node that functions,

(ii) and it belongs to the giant cluster of its own network, and meanwhile, it is not overloaded (if it is a power node).

Thus, the presence of a giant cluster is an indicator of a network that is at least partly performing its intended function, while the size of the giant cluster tells us the catastrophic consequences of cascading failures.

5.2.1 Intra Links in Individual Networks

This thesis assumes that the communication network G_C is part of the Internet backbone, extended with some wireless links. Internet have been extensively studied from complex network perspective. A significant part of networks in real life includes Erdős-Rényi networks, *scale-free* networks, and *small-world* networks [140]. A large number of research data shows that

the Internet is a scale-free network [140] and its nodes are *autonomous systems*. Node degree distribution follows a power law, which is denoted as $\mathbb{P}(\ell) \propto \ell^{-\gamma_C}$, where $\mathbb{P}(\ell)$ is the probability that a node has ℓ links and γ_C is the *power law coefficient*. This work assumes the communication network is a subclass of scale-free networks [35, 146] whose node degree strictly follows the power law degree distribution. Edges connecting nodes in power grid (including power generators and substations) are mediate and low voltage distribution lines. The power grid can be studied and modelled as a scale-free network without losing generality [147, 148] and node degree distribution follows the relation: $\mathbb{P}(\ell) \propto \ell^{-\gamma_P}$, where γ_P is the power law coefficient of the specific network considered.

5.2.2 Description of Interdependence Relations

In order to quantify the service disruption facilitated by the interdependent relations of a smart grid, we need to understand the interdependence relation between nodes in both interdependent power and communication networks. In this thesis, control-dependency links, energy-dependency links, and info-access links form the inter links. Control-dependency links are assigned from control centres in the communication network to power nodes in the power network. This work assumes "ℓ-to-m" interdependence for control-dependency link assignment: each power node in G_P is supported by ℓ control centres and each control centre of the communication network G_C supports m power nodes. In this thesis, a node in the communication network G_C has one energy-dependency link with nodes in G_P from which it receives electricity. Similar to the work in [149], only distribution nodes can provide electric supply to the communication nodes (including both control centres and relay nodes). According to the load *capacity*, there is a limit number of communication nodes that a distribution node can support [38]. Thus, in this model, the number of communication nodes that each power node supports is maximum two. Although a power node is controlled by a control centre, this control is only possible if the power node can access the communication network and can receive information-exchange from a relay node. For this reason, this model assigns one information access link for one power node in G_P to access a relay node in G_C. It is assumed that a relay node can always reach at least one control centre (either wired or wireless). This work assumes interdependencies using geographic criteria. In particular, power nodes provide electricity to the nearest communication nodes, while relay nodes exchange information with their nearest power nodes. This work assumes the number of power nodes a relay node can support is unlimited and such a number is determined by the geographic criteria. Therefore, the famous *Balls*

and *Bins* interdependency link allocation approach [35, 38] does not applicable in this thesis. Interdependencies are directional and asymmetric, so if a node $v_C^{\{i\}}$ ($i \in \{1,2,\cdots,n_C\}$) in the communication network depends on a node $v_P^{\{i\}}$ ($i \in \{1,2,\cdots,n_P\}$) in the power grid, it does not necessarily imply that $v_P^{\{i\}}$ depends on $v_C^{\{i\}}$. Figure 5.2 gives a sketch of the interdependence model. As shown in Figure 5.2, each distribution substation provides electricity to two communication nodes (relay nodes and control centres are all communication nodes). There are two control centres in the communication network G_C, and each of them operates three nodes (generators and distribution substations) in the power grid. Each distribution substation receives information from only one relay node in close proximity, as shown in Figure 5.2.

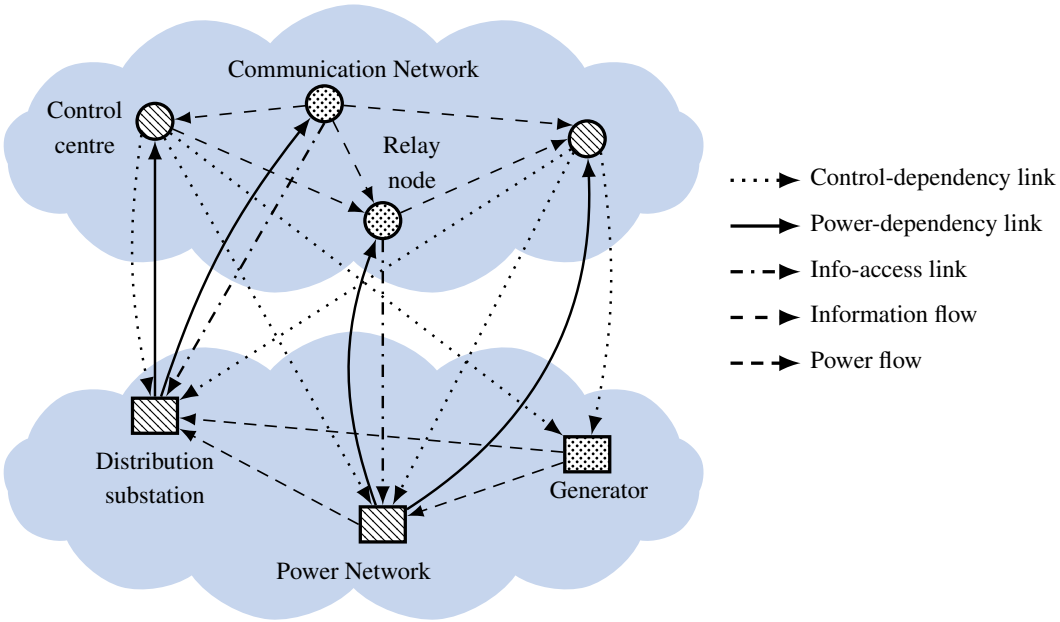


Figure 5.2: The interdependence model for interdependent power and communication networks.

5.2.3 Power Network in Smart Grids

In power system, the energy flow between any pair of nodes depends on the electrical characteristics of the nodes and the link carrying the power. However, it is reasonable to consider the initial load of a node $v_P^{\{i\}}$ ($i \in \{1,2,\cdots,n_P\}$) is related to the number of shortest paths [150, 151] that passing through the node [134, 147]. Taking this into account, this thesis defines the initial load $L_{P(0)}^{\{i\}}$ of a power node $v_P^{\{i\}}$ as a function of its betweenness [152]

$$L_{P(0)}^{\{i\}} = B_{P(0)}^{\{i\}},$$

where $B_{P(0)}^{\{i\}}$ is the *betweenness* of node $v_P^{\{i\}}$. The betweenness counts the fraction of shortest paths between any pair of nodes that passed through a given node $v_P^{\{i\}}$. It is shown in [153] that betweenness can be well approximated in a local manner to reduce its computational complexity. Additionally, Brandes's highly efficient algorithm [154] can also be used as an alternative to compute betweenness centrality.

Nodes with higher betweenness may have higher influence within a network in terms of services provided and their controls over energy passing between others. In a directed network, the betweenness of a power node $v_P^{\{i\}}$ at time $t = 0$ is defined by [155]

$$B_{P(0)}^{\{i\}} := \sum_{r,h;h\neq r\neq i} \frac{s_{hir}}{s_{hr}} / \big((N'-1)(N'-2)\big),$$

where s_{hr} is the number of shortest paths from node $v_P^{\{h\}}$ to node $v_P^{\{r\}}$, and s_{hir} is the number of shortest paths from node $v_P^{\{h\}}$ to node $v_P^{\{r\}}$ that pass through node $v_P^{\{i\}}$. N' is the number of nodes in the giant cluster. Initially, all nodes in the power network are in the giant cluster and thus $N' = n_P$, where n_P is the initial number of nodes in the power network. This thesis defines $\frac{s_{hir}}{s_{hr}} = 0$, if either s_{hir} or s_{hr} is zero. In this thesis, it is also assumed that the weight of a power node $v_P^{\{i\}}$ at any time t ($t \in \mathbb{R}_+$) is its betweenness, i.e., $w_P^{\{i\}} = B_{P(0)}^{\{i\}}$.

The load $L_{P(t)}^{\{i\}}$ on node $v_P^{\{i\}}$ at time t ($t \in \mathbb{R}_+$) reflects the total amount of load connected to power node $v_P^{\{i\}}$ at time t. In reality, each distribution substation has a maximum load it can tolerate, which is called *load capacity*. This work assumes the capacity $C_P^{\{i\}}$ of node $v_P^{\{i\}}$ to be proportional to its initial load $L_{P(0)}^{\{i\}}$ (where loads of two supported communication nodes are excluded):

$$C_P^{\{i\}} = T_p \cdot L_{P(0)}^{\{i\}}, \quad T_p \geq 1, \quad i = 1,2,\cdots,n_P, \tag{5.1}$$

where constant T_p is the *tolerance parameter* that controls the tolerance of the power system. This is a reasonable assumption, since the capacity cannot be infinitely large because of cost constraints. $C_P = \{C_P^{\{1\}}, C_P^{\{2\}}, \cdots, C_P^{\{n_d\}}\}$ is a set of load constraints of nodes and denotes the largest load capacity allowed (expect loads of two supported communication nodes). While the load of each node may change over time, the load capacity of each node remains the same. If the actual load $L_{P(t)}^{\{i\}}$ of a node $v_P^{\{i\}}$ at time t exceeds its capacity $C_P^{\{i\}}$, the node $v_P^{\{i\}}$ fails. While when the current load $L_{P(t)}^{\{i\}}$ does not exceed its load capacity, i.e., $L_{P(0)}^{\{i\}} \leq L_{P(t)}^{\{i\}} < C_P^{\{i\}}$, node $v_P^{\{i\}}$ will stay in a normal functional state.

5.3 Mathematical Analysis of Cascading Failures

To analyse the cascading failure in interdependent power and communication networks, this thesis constructs a model to describe failed loads propagation in both a single network and in interdependent networks. The model begins by removing $p \cdot n_C$ of nodes in the communication network G_C, i.e., a fraction p of nodes in the communication network G_C is attacked. As a result, the intra and inter links of these failed nodes are also removed. Owing to the interdependency, nodes in the power network G_P lose their inter links. As nodes and links are removed and neighbours of the removed nodes overloaded, the power network G_P begins to fragment into clusters. The fragmentation in the power network G_P might lead to further failures in the communication network G_C. At each stage, the nodes which do not have any currently functional supporting nodes from their interdependent network and the nodes which are separated from the giant cluster of their corresponding network, are considered to be failed. This interdependency cascading failure continues recursively between the two networks until no further node failure in either network occurs. Moreover, in the power network, due to the load capacity, the node which is overloaded because of load redistribution from failed neighbours will also fail. This overloading failure continues until no node is overloaded. Finally, at the end of a cascading failure, the functional nodes in both networks satisfy conditions (i) and (ii) listed in Section 5.2. Here it is assumed that the probability an arbitrary node in network G_ℓ ($G_\ell \in \{G_C, G_P\}$) has j incoming and k outgoing edges is $p_\ell(j,k)$. The *generating function* [156] for the degree distribution $p_\ell(j,k)$ is the polynomial

$$\mathcal{G}_{00}(x,y) = \sum_{j,k=0}^{\infty} p_\ell(j,k) x^j y^k,$$

where x and y are arbitrary complex variables. Giving the generating function, the degree distribution $p_\ell(j,k)$ can be constructed by differentiating

$$p_\ell(j,k) = \frac{1}{j!k!} \frac{\partial^j \partial^k \mathcal{G}_{00}}{\partial x^j \partial y^k}\bigg|_{x,y=0}.$$

Thus the generating function $\mathcal{G}_{00}(x,y)$ encapsulates all the information contained in the discrete probability distribution $p_\ell(j,k)$. The function $\mathcal{G}_{00}(x,y)$ "generates" the probability distribution $p_\ell(j,k)$. Since the degree distribution must be normalized according to $\sum_{j,k=0}^{\infty} p_\ell(j,k) = 1$, the generating function satisfies

$$\mathcal{G}_{00}(1,1) = \sum_{j,k=0}^{\infty} p_\ell(j,k) = 1,$$

and the average in- and out-degrees of nodes in network i are given by [152]

$$\langle j\rangle_l = \sum_{j,k=0}^{\infty} j p_\ell(j,k) = \left.\frac{\partial \mathcal{G}_{00}}{\partial x}\right|_{x,y=1} = \mathcal{G}_{00}^{(1,0)}(1,1),$$

$$\langle k\rangle_l = \sum_{j,k=0}^{\infty} k p_\ell(j,k) = \left.\frac{\partial \mathcal{G}_{00}}{\partial y}\right|_{x,y=1} = \mathcal{G}_{00}^{(0,1)}(1,1).$$

The notation $\mathcal{G}_{00}^{(e,f)}$ indicates differentiation of $\mathcal{G}_{00}$ with respect to its two arguments (i.e., x and y) e and f times, respectively. For example, $\mathcal{G}_{00}^{0,1}(x,y)$ means one time differentiation of the parameter y in $\mathcal{G}_{00}$. In a directed network, since every outgoing directed edge must also be an incoming edge for an another node, the average in- and out-degrees are equal and

$$\mathcal{G}_{00}^{(1,0)}(1,1) = \mathcal{G}_{00}^{(0,1)}(1,1).$$

The average in- and out-degrees are denoted by $\bar{c}$ and thus $\langle j\rangle_\ell = \langle k\rangle_\ell = \bar{c}$.

We can also write down generating functions for the excess degree distribution of nodes reached by following an edge in the network. Excess degree distribution is the probability distribution, for a node reached by following an edge, of the number of other edges attached to that node. There are two different ways of following a directed edge, either forward or backward [152]. For the forward case, when the network is infinitely large $n_\ell \to \infty$, the generating function for this excess degree distribution is [140]

$$\begin{aligned}\mathcal{G}_{10}(x,y) &= \sum_{j,k=0}^{\infty} \frac{(j+1)p_l(j+1,k)}{\bar{c}} x^j y^k \\ &= \frac{1}{\bar{c}} \sum_{j,k=0}^{\infty} j p_l(j,k) x^{j-1} y^k = \frac{\mathcal{G}_{00}^{(1,0)}(x,y)}{\mathcal{G}_{00}^{(1,0)}(1,1)}.\end{aligned}$$

Similarly, the generation function for excess degree distribution in the backward case can be defined as [140]

$$\begin{aligned}\mathcal{G}_{01}(x,y) &= \sum_{j,k=0} \frac{(k+1)p_l(j,k+1)}{\bar{c}} x^j y^k \\ &= \frac{1}{\bar{c}} \sum_{j,k=0}^{\infty} k p_l(j,k) x^j y^{k-1} = \frac{\mathcal{G}_{00}^{(0,1)}(x,y)}{\mathcal{G}_{00}^{(1,0)}(1,1)}.\end{aligned}$$

It is assumed that when a node is not connected to a giant cluster, it is not functioning and has failed. When a fraction p of nodes in the communication network is initially removed due to attack, the resulting cascading failure spreads dynamically as follows.

5.3.1 Step I: Attack on Communication Network

When a fraction p of nodes in the communication network G_C fails (alternatively, a fraction of $1-p$ of the nodes is remained), as nodes and links are sequentially removed, each inter-dependent network begins to fragment into connected components. The degree distribution of remaining nodes will be changed. For example, nodes with initial j in-degree and k out-degree will have, after the random removal of nodes, a different number of connections, depending on the number of removed neighbours. The new number of connections of a communication node will be binomially distributed. If we begin with a distribution of degrees $p_C(j,k)$, the new degree distribution will be

$$p_{C1} = \sum_{j\geq j_i}^{\infty}\sum_{k\geq k_i}^{\infty} p_C(j,k)\binom{j}{j_i}p^{j_i}(1-p)^{j-j_i}\binom{k}{k_i}p^{k_i}(1-p)^{k-k_i}.$$

Then the degree probability generating function can be defined as

$$\begin{aligned}
\mathcal{G}'_{00}(x,y) &:= \sum_{j_i=0}^{\infty}\sum_{k_i=0}^{\infty}\left[\sum_{j=j_i}^{\infty}\sum_{k=k_i}^{\infty} p_C(j,k)\binom{j}{j_i}p^{j_i}(1-p)^{j-j_1}\binom{k}{k_i}p^{k_i}(1-p)^{k-k_i}x^{j_i}y^{k_i}\right] \\
&= \sum_{j,k=0}^{\infty} p_C(j,k)\left[\sum_{j_i=0}^{j}\binom{j}{j_i}(xp)^{j_i}(1-p)^{j-j_i}\sum_{k_i=0}^{k}\binom{k}{k_i}(yp)^{k_i}(1-p)^{k-k_i}\right] \\
&= \sum_{j,k=0} p_C(j,k)(1-p+xp)^j(1-p+yp)^k \\
&= \mathcal{G}_{00}(1+(x-1)p, 1+(y-1)p).
\end{aligned}$$

Similarly, the generating function for the excess distribution for both forward and backward cases can be defined as

$$\mathcal{G}'_{10}(x,y) := \mathcal{G}_{10}(1+(x-1)p, 1+(y-1)p),$$

and

$$\mathcal{G}'_{01}(x,y) := \mathcal{G}_{01}(1+(x-1)p, 1+(y-1)p).$$

Let v denote the probability that a node to which a randomly chosen link leads has no path to the giant cluster. If a node has an out-degree k, the probability that it does not have path to the giant cluster is v^k. But j and k are distributed according to the excess distribution $q_C(j,k)$ and hence, averaging over both, we find that

$$v = \sum_{j,k=0}^{\infty} q_C(j,k)v^k = \mathcal{G}_{10}(1,v),$$

where the degree distribution $q_C(j,k)$ is defined as

$$q_C(j,k) = \frac{(j+1)p_C(j+1,k)}{\bar{c}}.$$

Analogously, let u be the probability that there is no path from the giant cluster to the node from which a randomly chosen link originates, then u is the solution to

$$u = \mathcal{G}_{01}(u,1).$$

The node itself has the probability of $1-p$ not being removed. Thus, μ_{C1}, the fraction of nodes belong to the giant cluster is given by [35, 157, 158]

$$\begin{aligned}\mu_{C1} &:= (1-p)\left[\sum_{j,k=0}^{\infty} p_{C1}(1-u^j)(1-v^k)\right] \\ &= (1-p)\Big[1-\mathcal{G}_{00}(pu+1-p,1)-\mathcal{G}_{00}(1,pv+1-p) \\ &\quad +\mathcal{G}_{00}(pu+1-p,pv+1-p)\Big],\end{aligned}$$

and v satisfies $v = \mathcal{G}_{10}(1,pv+1-p)$. Similarly, u satisfies $u = \mathcal{G}_{01}(pu+1-p,1)$.

5.3.2 Step II: Cascading Effects on Power Network

Due to the attack on communication nodes, the power network is affected. A node in the power network G_P is functional, if it has at least one info-access link and one control-dependency link from the communication network G_C and it is not overloaded. At this step, any node does not have any supporting node from the communication network G_C will become disconnected from the giant cluster. From Section 5.3.1, it can be seen that the number of functional nodes in the communication network decreases from n_C to $n_C \cdot \mu_{C1}$ and the probability that a node is not in the giant cluster is $1-\mu_{C1}$. If a node in the communication network fails, the power node it supports, will also fail. A power node is relying on one relay node in the communication network G_C for information exchange services. The probability that its supporting relay node is not in the giant cluster is $1-\mu_{C1}$, thus, the fraction of a node in the power network G_P disconnected due to attack on the communication network G_C is given by

$$\lambda_{P_2} = 1-\mu_{C1}, \tag{5.2}$$

and the degree probability of an arbitrary node in G_P is given by

$$p_{P2} = \sum_{j \geq j_i}^{\infty} \sum_{k \geq k_i}^{\infty} p_P(j,k) \binom{j}{j_i} \lambda_{P2}^{j_i} (1-\lambda_{P2})^{j-j_i} \binom{k}{k_i} \lambda_{P2}^{k_i} (1-\lambda_{P2})^{k-k_i}.$$

Once a power node is failed at time $t-1$, to ensure continuous services, the power system will redistribute the load of this failed node at time t. There are two ways to distribute load: one is distributing the load to all the distribution nodes left in the network and the other is distributing the load to the neighbouring distribution nodes of the failed node $v_P^{\{i\}}$. This thesis studies the case where the load of the failed node $v_P^{\{i\}}$ is redistributed to its upstream distribution nodes. When a distribution node $v_P^{\{i\}}$ is removed from the grid, its load(s) will be returned to its functional upstream distribution nodes and diverted to other downstream nodes of these upstream nodes [144]. Suppose a node $v_P^{\{r\}}$ is one upstream distribution node of the failed node $v_P^{\{i\}}$, The load redistribution probability that is received by the distribution node $v_P^{\{r\}}$ can be defined as the ratio of its weight to the sum of weights of all upstream neighbours of $v_P^{\{i\}}$

$$q_P^{\{r\}} = \frac{w_P^{\{r\}}}{\sum_{\ell \in \Theta_i^{in}} w_P^{\{\ell\}}},$$

where Θ_i^{in} is the set of functional upstream distribution nodes that the node $v_P^{\{i\}}$ has and $w_P^{\{\ell\}}$ presents the weight of the node $v_P^{\{\ell\}}$. Such that, the incremental of node $v_P^{\{r\}}$ received from its failed neighbouring node $v_P^{\{i\}}$ is $\triangle_1 L_{P(t)}^{\{r\}} = L_{P(t-1)}^{\{i\}} q_P^{\{r\}}$, and when $L_{P(t)}^{\{r\}} = L_{P(t-1)}^{\{r\}} + \triangle_1 L_{P(t)}^{\{r\}} \leq C_P^{\{r\}}$, node $v_P^{\{r\}}$ does not fail and maintains its normal function. Otherwise, once $L_{P(t-1)}^{\{r\}} + \triangle_1 L_{P(t)}^{\{r\}} > C_P^{\{r\}}$, node $v_P^{\{r\}}$ fails and causes an overload attack. All the overloaded nodes are removed simultaneously from the network, which may cause other nodes to be overloaded and removed, resulting in a cascade of overloading failures [143, 159], as the one happened on August 10, 1996 in the western United States power grid [160]. If a node $v_P^{\{i\}}$ and one or many of its upstream neighbouring nodes fail at the same time, the load of node $v_P^{\{i\}}$ will be redistributed to its functional and yet not overloaded upstream neighbouring nodes. A load will be lost if none of upstream neighbouring distribution nodes is functional. If c out of n downstream neighbouring nodes of node $v_P^{\{r\}}$ are failed, the *load incremental factor* $\triangle_c L_{P(t)}^{\{r\}}$ of node $v_P^{\{r\}}$ is

$$\triangle_c L_{P(t)}^{\{r\}} = \underbrace{\frac{w_P^{\{r\}}}{\sum_{\ell \in \Theta_{h_1}^{in}} w_P^{\{\ell\}}} L_{P(t-1)}^{\{h_1\}} + \frac{w_P^{\{r\}}}{\sum_{\ell \in \Theta_{h_2}^{in}} w_P^{\{\ell\}}} L_{P(t-1)}^{\{h_2\}} + \cdots + \frac{w_P^{\{r\}}}{\sum_{\ell \in \Theta_{h_c}^{in}} w_P^{\{\ell\}}} L_{P(t-1)}^{\{h_c\}}}_{c \text{ neighboring nodes are dysfunctional}}. \tag{5.3}$$

And the new load of node $v_P^{\{r\}}$, after taking load from its c failed downstream nodes, is correspondingly defined as

$$L_{P(t)}^{\{r\}} := L_{P(t-1)}^{\{r\}} + \triangle_c L_{P(t)}^{\{r\}}. \tag{5.4}$$

Let $O_P^{\{r\}}$ be a be a random variable (r.v.) which denotes node $v_P^{\{r\}}$ is overloaded by taking excessive load shifted from its downstream neighbouring power nodes. Let Θ_r^{out} and C_r^{out} be two r.v.s representing the number of node $v_P^{\{r\}}$'s downstream nodes and the number of downstream nodes that failed simultaneously because of the failed interdependent communication nodes in the communication network, respectively. Certainly, $\Theta_r^{out} > C_r^{out}$. To calculate the probability $\mathbb{P}(O_P^{\{r\}}|\Theta_r^{out} = k)$, it is required to compute $\mathbb{P}(O_P^{\{r\}}|C_r^{out} = c)$ first, which is the probability that node $v_P^{\{r\}}$ will be overloaded when its c downstream power nodes are failed [38]. By applying Equations (5.1) and (5.4) we have

$$\begin{aligned}\mathbb{P}(O_P^{\{r\}}|C_r^{out} = c) &= \mathbb{P}\left(\left(L_{P(t)}^{\{r\}} = L_{P(t-1)}^{\{r\}} + \triangle_c L_{P(t)}^{\{r\}}\right) > C_P^{\{r\}}\right) \\ &= \begin{cases} 1, & L_{P(t-1)}^{\{r\}} + \triangle_c L_{P(t)}^{\{r\}} > T \cdot L_{P(0)}^{\{r\}} \\ 0, & \text{Otherwise} \end{cases}.\end{aligned}$$

The probability that node $v_P^{\{r\}}$'s c out of k downstream nodes are failed because of interdependency cascading is given by

$$\mathbb{P}\left(C_r^{out} = c|\Theta_r^{out} = k\right) = \binom{k}{c}/2^k. \tag{5.5}$$

Therefore, $\mathbb{P}\left(O_P^{\{r\}}|\Theta_r^{out} = k\right)$ can be calculated as

$$\mathbb{P}\left(O_P^{\{r\}}|\Theta_r^{out} = k\right) = \sum_{c=0}^{k} \mathbb{P}\left(O_P^{\{r\}}|C_r^{out} = c\right) \cdot \mathbb{P}\left(C_r^{out} = c|\Theta_r^{out} = k\right). \tag{5.6}$$

Therefore, the probability that a node is survived from the load propagation cascading is given by $1 - \mathbb{P}\left(O_P^{\{r\}}|\Theta_r^{out} = k\right)$. Since the fraction of remaining functional nodes in the power network G_P is given by $1 - \lambda_{P_2}$ (see Equation (5.2)), the fraction of nodes that still belongs to the giant cluster of the power network after both interdependency and overloading cascading can be determined as

$$\mu_{P2} := (1 - \lambda_{P2}) \left(\sum_{j,k=0}^{\infty} p_{P2}(1 - u^j)(1 - v^k) \left(1 - \mathbb{P}(O_P^{\{r\}}|\Theta_r^{out} = k)\right) \right),$$

where v satisfies $v = \mathcal{G}_{10}(1, \lambda_{P2}v + 1 - \lambda_{P2})$ and u satisfies $u = \mathcal{G}_{01}(\lambda_{P2}u + 1 - \lambda_{P2}, 1)$.

5.3.3 Step III: Further Failures on Communication Network

Every distribution node provides electricity to two communication nodes and generator nodes do not provide electricity to any communication nodes. Suppose a fraction of φ_{D2} of the nodes in the giant cluster are distribution nodes, thus, the fraction of distribution nodes that stays in the giant cluster after both interdependency and node overloading cascading failure is

$$\mu_{DP2} = \mu_{P2}\varphi_{D2}.$$

Due to the failure (from both interdependency and overloading) in the power network, their interdependent communication network would also be affected. Therefore, the fraction of nodes in the communication network G_C which fail due to failures of nodes in the power network G_P is given by

$$\lambda_{C3} = (1-\mu_{DP2})^2,$$

and the node degree distribution becomes

$$p_{C3} = \sum_{j\geq j_i}^{\infty}\sum_{k\geq k_i}^{\infty} p(j,k)\binom{j}{j_i}\lambda_{C3}^{j_i}(1-\lambda_{C3})^{j-j_i}\binom{k}{k_i}\lambda_{C3}^{k_i}(1-\lambda_{C3})^{k-k_i}.$$

Therefore, the fraction of nodes remains in the giant cluster can be calculated as

$$\begin{aligned}\mu_{C3} &:= (1-\lambda_{C3})\left(\sum_{j,k=0}^{\infty} p_{C3}(1-u^j)(1-v^k)\right)\\ &= (1-\lambda_{C3})\left(1-\mathcal{G}_{00}(\lambda_{C3}u+1-\lambda_{C3},1)-\mathcal{G}_{00}(1,\lambda_{C3}v+1-\lambda_{C3})\right.\\ &\quad\left.+\mathcal{G}_{00}(\lambda_{C3}u+1-\lambda_{C3},\lambda_{C3}v+1-\lambda_{C3})\right),\end{aligned}$$

where v satisfies $v = \mathcal{G}_{10}(1, r_{C3}v+1-r_{C3})$ and u satisfies $u = \mathcal{G}_{01}(r_{C3}u+1-r_{C3},1)$.

5.3.4 Time-varied Giant Clusters and Steady State Conditions

Steps I - III will be iteratively looped until no more new node failed in the interdependent power and communication system. After each step ℓ, $\ell \in \mathbb{N}$, one can certainly obtain the fraction of giant cluster (e.g., μ_{C1}, μ_{P2}, μ_{C3}, $\cdots$). However, these two giant clusters are mutually connected. Thus, these two giant clusters can be taken as a mutual connected set. When $\ell \to \infty$, the system arrives at a *steady state*. The steady state condition can be interpreted as no further splitting and node failure can occur, and the fraction of failed nodes at step $\ell+1$ is equal to that at step ℓ.

This work will now calculate the giant cluster at the steady state. If the fraction of nodes from the communication network G_C in the giant cluster at steady state is σ_C and the fraction of nodes from the power network G_P in the giant cluster at steady state is σ_P. This work will now discuss how σ_C and σ_P can be calculated. Let $\lambda_{C(2\ell+1)}(\ell \geq 0)$ be the fraction of nodes in the communication network G_C that are dysfunctional due to the failure (interdependency failure or node overloading failure or both) of a fraction of $\mu_{DP(2\ell)}$ distribution nodes in G_P at stage 2ℓ. Then

$$\lambda_{C(2\ell+1)} = \left(1-\mu_{DP(2\ell)}\right)^2, \tag{5.7}$$

and the fraction of nodes in the giant cluster of the communication network G_C at stage $2\ell+1$ is

$$\begin{aligned}
\mu_{C(2\ell+1)} := (1-\lambda_{C(2\ell+1)}) \Bigg(& \sum_{j,k=0}^{\infty} \sum_{j\geq j_i} \sum_{k\geq k_i} p(j,k) \binom{j}{j_i} \lambda_{C(2\ell+1)}^{j_i} (1-\lambda_{C(2\ell+1)})^{j-j_i} \\
& \binom{k}{k_i} \lambda_{C(2\ell+1)}^{k_i} (1-\lambda_{C(2\ell+1)})^{k-k_i} (1-u^j)(1-v^k) \Bigg) \\
= (1-\lambda_{C(2\ell+1)}) & \left(1-\mathcal{G}_{00}\left(\lambda_{C(2\ell+1)}u+1-\lambda_{C(2\ell+1)},1\right) - \mathcal{G}_{00}\left(1,\lambda_{C(2\ell+1)}v\right.\right. \\
& \left.\left. +1-\lambda_{C(2\ell+1)}\right) + \mathcal{G}_{00}\left(\lambda_{C(2\ell+1)}u+1-\lambda_{C(2\ell+1)},\lambda_{C(2\ell+1)}v+1-\lambda_{C(2\ell+1)}\right)\right).
\end{aligned} \tag{5.8}$$

where v satisfies $v = \mathcal{G}_{10}(1,\lambda_{C(2\ell+1)}v+1-\lambda_{C(2\ell+1)})$ and u satisfies $u = \mathcal{G}_{01}(\lambda_{C(2\ell+1)}u+1-\lambda_{C(2\ell+1)},1)$. Let $\lambda_P(2\ell+2)$ be the fraction of nodes in the power network G_P that are failed due to the failure (interdependency failure) of nodes in G_C at step $2\ell+1$, then

$$\lambda_{P(2\ell+2)} = 1-\mu_{C(2\ell+1)}. \tag{5.9}$$

Similarly, the fraction of nodes in giant cluster of G_P at stage $2\ell+2$ is

$$\begin{aligned}
\mu_{P(2\ell+2)} := (1-\lambda_{P(2\ell+2)}) \Bigg(& \sum_{j,k=0}^{\infty} \sum_{j\geq j_i} \sum_{k\geq k_i} p(j,k) \binom{j}{j_i} \lambda_{P(2\ell+2)}^{j_i} (1-\lambda_{P(2\ell+2)})^{j-j_i} \binom{k}{k_i} \lambda_{P(2\ell+2)}^{k_i} \\
& (1-\lambda_{P(2\ell+2)})^{k-k_i} (1-u^j)(1-v^k)(1-\mathbb{P}(O_P^{\{r\}}|\Theta_r^{out}=k)) \Bigg) \\
= (1-\lambda_{P(2t+2)}) \Bigg(& \sum_{j,k=0}^{\infty} \sum_{j\geq j_i} \sum_{k\geq k_i} p(j,k) \binom{j}{j_i} \lambda_{P(2t+2)}^{j_i} (1-\lambda_{P(2t+2)})^{j-j_i} \binom{k}{k_i} \lambda_{P(2t+2)}^{k_i} \\
& (1-\lambda_{P(2t+2)})^{k-k_i} (1-u^j)(1-v^k)\Big(1-\sum_{c=0}^{k} \binom{k}{c} \mathbb{P}(O_P^{\{r\}}|C_r^{out}=c)/2^k\Big) \Bigg),
\end{aligned} \tag{5.10}$$

where v satisfies $v = \mathcal{G}_{10}(1, \lambda_{P(2\ell+2)}v + 1 - \lambda_{P(2\ell+2)})$ and u satisfies $u = \mathcal{G}_{01}(\lambda_{P(2\ell+2)}u + 1 - \lambda_{P(2\ell+2)}, 1)$. If $sigma_C = \mu_{C(2\ell+1)} = \mu_{C(2\ell+3)}, \forall \ell in \mathbb{N}$ and $\sigma_P = \mu_{P(2\ell)} = \mu_{P(2\ell+2)}$, the system arrives at a steady state. This work presents the number of failed nodes in the power network G_P and the communication network G_C at the end of the cascading failure propagation process as $u_{N,\infty} = (1 - \sigma_C)n_C$ and $u_{P,\infty} = (1 - \sigma_P)n_P$, respectively.

5.4 Disruption Characterizations

After attaining the steady state, such that no node in both interdependent networks will fail, it is important to evaluate the impact of disruptive events caused by cyber attacks in physical power grids. Disruptive events, which are initialized by cyber attacks targeting physical infrastructure, are often seen as the most dangerous type of disruptive event. ENISA has already identified three primary characterizations to describe disruptive events [101]: scope (the geographic area that could be affected by the loss or unavailability of a critical infrastructure, the number of computers/equipments taken down, or the number of customers who are unable to access their required services), magnitude (the consequences of the disruption), and time distribution (the length of time without the required services, which could be days, weeks or even months). In the case of the disruption of a German steel mill (see Chapter 1 for more details about this use case): the scope of this disruptive event included small number of key controllers of physical equipment, the magnitude was directly related to the productive capacity of the number of important pieces of equipment that were destroyed or impeded; and the time to make the whole infrastructure operable again took several months (more than six). It is again confirmed in [161] that a power outage should be measured in terms of scope and the time taken to achieve full restoration. Regarding smart grids, the scope of an equipment compromise attack event can be characterized by the cascading failure analysis. The time duration of an equipment attack is longer than other types of disruptive attacks, as some pieces of physical equipment can be easily replaced, while specialist equipment may take months or even years to be fully replaced. The operator of the electric grid must be able to give out information on the expected time to recovery and delays (if any) to the start of the recovery. It is crucial that disrupted operators inform the security operator of the smart grid about the potential consequence of the cyber attack. The consequence can be environmental or economic. To support the assessment of the economic consequences of power interruptions, a blackout simulator [1] was developed

[1] http://www.blakcout-simulator.com/ (Retrieved: 20/06/2017)

in the FP7 SESAME project [1]. In this thesis, without any loss of generality, the disruption magnitude of one piece of failed equipment is assumed to have a value from 0 (no disruption) to 10 (services totally lost); and this value is provided by the disrupted utility operator. These three disruption characterisations of disruptive events are synthesized into a single measure of cyber disruption. As described in Sections 5.2.3 and 5.3.4, the number of dysfunctional power nodes at the steady state is $u_{P,\infty}$, while the power node weight for node $v_P^{\{i_\ell\}}$ is $w_P^{\{i_l\}}$ ($\ell \in u_{P,\infty}$). If we assume the disruption magnitude of a node $v_P^{\{i_\ell\}}$ in the power grid to be $m_P^{\{i_\ell\}} \in [0,10]$, and the time duration of the disruptive events is t_d,the following cyber disruption metric M_c $\in \mathbb{R}_+$ is defined to quantify the characterisations of disruptive events caused by cyber attacks:

$$M_c = t_d \cdot \underbrace{\left(w_P^{\{i_1\}} \cdot m_P^{\{i_1\}} + w_P^{\{i_2\}} \cdot m_P^{\{i_2\}} + \cdots + w_P^{\{i_\ell\}} \cdot m_P^{\{i_\ell\}} + \cdots + w_P^{\{i_{P,\infty}\}} \cdot m_P^{\{i_{n_{P,\infty}}\}} \right)}_{u_{P,\infty} \text{ failed power nodes}}.$$

5.5 Player's Payoff Formulation

This thesis represents each player's objectives and trade-offs by a payoff function, which includes reward and cost components. Although there may be a dependence of rewards and losses among the players' payoffs, there are cases that a loss to the defender is not of the same magnitude as the reward for the attacker. Therefore, the payoff for both players in the defender-attacker game does not sum up to zero. When the game play is in state s ($s \in S$), while the defender choosing his/her a ($a \in AS_1$) action and the attacker choosing his/her b ($b \in AS_2$) action, the payoff $g_{\{1,s\}}(a,b)$ of the defender and the payoff $g_{\{2,s\}}(a,b)$ of the attacker are defined as follows:

$$g_{\{1,s\}}(a,b) = \pm M_c - I_b - C_a, \tag{5.11}$$

$$g_{\{2,s\}}(a,b) = \pm M_c + I_b - C_b. \tag{5.12}$$

Equations (5.11) and (5.12) are formulated by observing the fact that players' payoffs are composed of the following three parts in the equation (in the respective order):

1. The cyber disruption metric $M_c \in \mathbb{R}_+$ (which is discussed in and derived from Section 5.4) quantifies the impact of cyber attacks (i.e., disruptive events) on the physical power

[1] https://www.sesame-project.eu/ (Retrieved: 20/06/2017)

grid. When it is a reward to one player with M_c, correspondingly, it is a corresponding loss for the other player with $-M_c$.

2. The information impact metric $I_b \in \mathbb{R}_+$ measures the impact of action b ($b \in AS_2$) from the attacker on the information security of nodes in the communication network. Similar to the work in [73, 162], this thesis also considers three important security aspects of a node, confidentiality (C), integrity (I) and availability (A), in order to measure the network information security impairment of nodes in the communication network that needs to be protected. Details of the information impact metric I_b will be discussed later.

3. The cost of action a ($a \in AS_1$) from the defender for defending and the cos of action b ($b \in AS_2$) from the attacker when attacking are defined as $C_a \in \mathbb{R}_+$ and $C_b \in \mathbb{R}_+$, respectively. As the cost is not necessarily monetary, its units are suitable for the application.

It is noteworthy that the actions of the attacker can affect the payoffs of both the attacker and the defender, due to the fact that the reward obtained by the attacker can result in losses for the defender. The impact of action b ($b \in AS_2$) of the attacker represents the ramifications of action b on the whole communication network; the information impact metric I_b is defined as follows:

$$I_b := \mathrm{Con}_b \cdot \alpha + \mathrm{Int}_b \cdot \beta + \mathrm{Ava}_b \cdot \delta, \tag{5.13}$$

where α, β, and δ are communication nodes' assets in tersm od confidentiality, integrity, and availability, respectively, and they are all values in $\{0,1,2,\cdots,\ell,\cdots,10\} \subset \mathbb{N}$; Con_b, Int_b, and Ava_b are the relative impairment degrees the action b has made in confidentiality, integrity, and availability. The relative impairment degree reflects the degree of the relative impairment of confidentiality, integrity, and availability that attack action b with regard to a particular type of communication node. Con_b, Int_b, and Ava_b are values between 0 and 1, which are, to some extent, independent. The objective of an attacker is to increase such values (i.e., to maximize his/her rewards) as much as possible. In other words, the attacker tries to impair the network security services (i.e., confidentiality, integrity, and availability) as much as he/she can. The impact of action b on communication nodes I_b is subject to expert knowledge or historical data. This thesis relies on expert knowledge to evaluate the corresponding parameters of the information impact metric I_b, the discussion of value assignment is beyond the scope of this thesis.

The cost to the attacker or the defender when carrying out an action depends on the lot of implementation costs and/or the management costs of that specific action. For example, for an attacker, the cost of exploiting a vulnerability to launch a MITM attack may involve massive programming efforts; meanwhile, for a defender, the cost of IDS deployment may include its implementation and management costs.

5.6 Simulation Results and Analysis

This section simulates the cascading failures to obtain the fraction of failed nodes $1-\sigma_C$ for the communication network G_C and the fraction of failed nodes $1-\sigma_P$ for the power network in the final steady state. The flowchart of the simulation of the investigated mathematical analysis of the cascading failure propagation (described in Section 5.3) is shown in Figure 5.3. The simulation results show how the system behaves under cyber attacks.

5.6.1 Network Setup

A specific program using the NetworkX [163] library and the TiedNets tool [149] is written to simulate the entire interdependency cascading failure propagation and load propagation process in interdependent power and communication networks. The following experimental set-up is employed:

- The synthetic power network G_P is created using a generalized Barabási-Albert model [164], which generates scale-free networks with power-law distributions. The average nodal degree of the power node is four, which is a typical value for real networks such as the power grids in North-east United States and Europe [165]. A power network with 1,000 nodes is generated, where 300 nodes are assigned as generators and 700 nodes are distribution substations.
- The communication network G_C is created using a Barabási-Albert model with its power-law coefficient set at three. Two nodes in the generated communication network are control centres, while the remaining 1,200 nodes in the communication network G_C are relay nodes.
- The two networks are coupled using the proposed interdependence model. Each control centre supports 1,000 power nodes, while each power node is controlled by two control centres. A distribution substation node provides electricity to at most, the two nearest

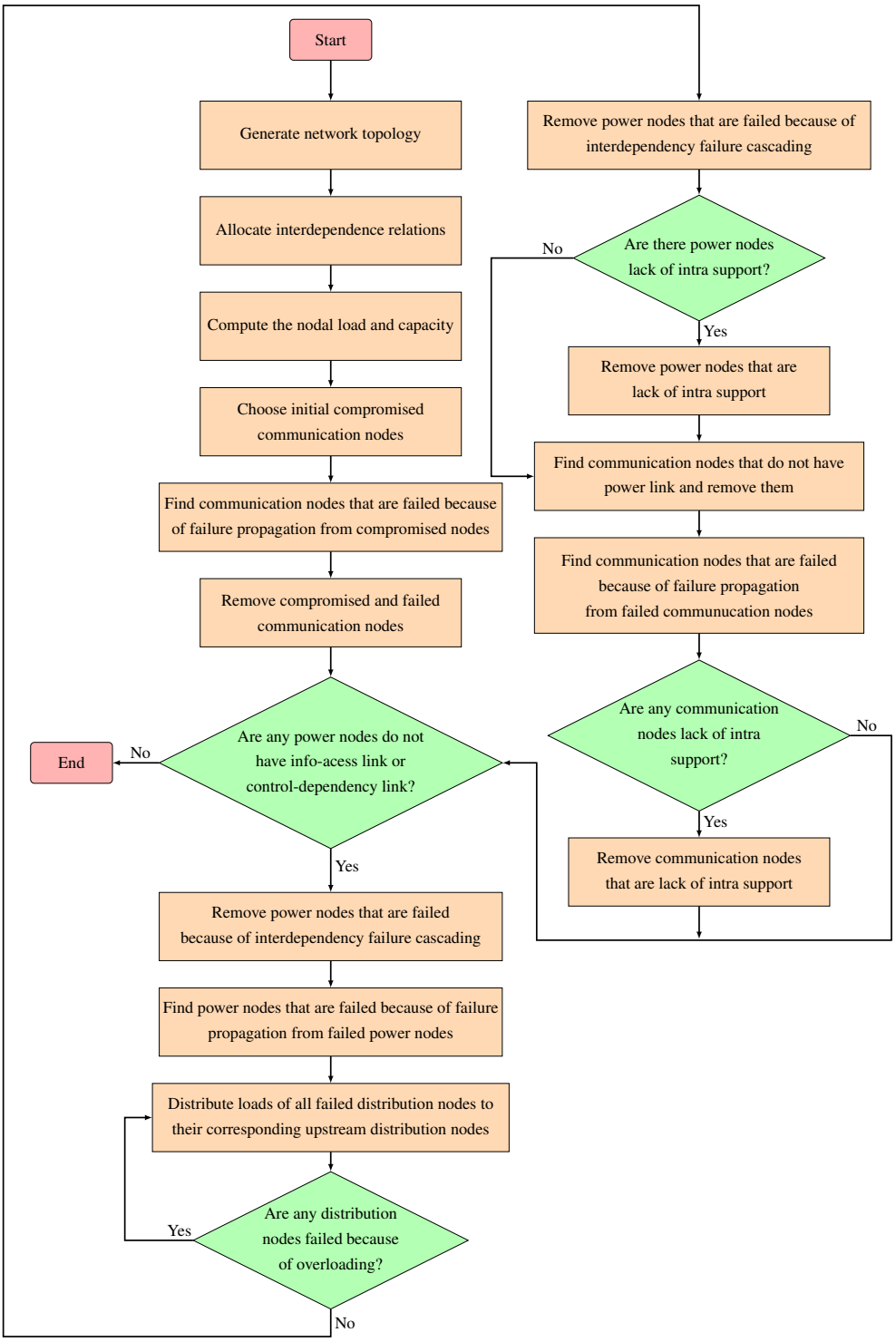


Figure 5.3: The flowchart of cascading failure propagation simulation.

communication nodes, with a relay node in the communication network G_C supporting only one power node.

- The fraction of p of compromised (i.e., failed) nodes in the communication network G_C is chosen according to whether those nodes are found on the attacker's paths to achieve his/her ultimate target. For different attack scenarios, the attacker may have different targets.
- The failure propagates within the two interdependent networks. The program simulates each step, and stores and updates the failed nodes in both the power network and the communication network.

5.6.2 Quantification of Failures

The number of failed nodes at each step of the cascading failure propagation process is clearly a random variable (r.v.). In order to quantify the failure on the network, the total number of failed nodes caused by the cyber attack in one network realization is utilised. Let F_ℓ denote the number of failed nodes in a network G_ℓ ($G_\ell \in \{G_C, G_P\}$) at a steady state, such that, the *failure ratio* f_ℓ is defined as

$$f_\ell := \frac{F_\ell}{|G_\ell|},$$

where $|G_\ell|$ is the number of nodes in the network G_ℓ. This work uses the average value of the random variable f_ℓ taken over all 100 test instances of the system (i.e., the interdependent power and communication networks), denoted by $\bar{f}_\ell$ and called *average failure ratio*, to measure the failure caused by the cyber attack.

5.6.3 Failure Propagation Results and Discussion

This work simulates the cascading failure, a joint failure from interdependency and node overloading in the interdependent power and communication network. The initial compromised nodes in the communication network G_C are not randomly chosen, instead they are targeted nodes of the attacker. The attacker chooses those nodes based on the whether they are on the his/her paths to obtain his/her goal, instead of nodes with the high load or nodes with high link degrees. To measure the average failure ratio in an interdependent power and communication network when a fraction p of nodes in the communication network G_C is failed, let us analyse the number of failed nodes at each failure propagation time step and study the variation of the

average failure ratio when multiple nodes are initial compromised by the attacker in the communication network G_C. This thesis is particularly interested in (1) the variation of the average failure ratio with the tolerance parameter T_p, (2) the variation of the average failure ratio with the fraction p of initial failed communication nodes and (3) the spatio-temporal distribution of the failure propagation.

(1) The variation of the average failure ratio with the tolerance parameter T_p

Networks are compared for various values (from 1.05 to 2.4, with a step length of 0.05) of the tolerance parameter T_p. The number of initial failed nodes is set to be 20, 40, 60, and 80 in the communication network G_C, which means that 1.7%, 3.3%, 5.5%, and 6.7% of communication nodes are initially compromised, respectively.

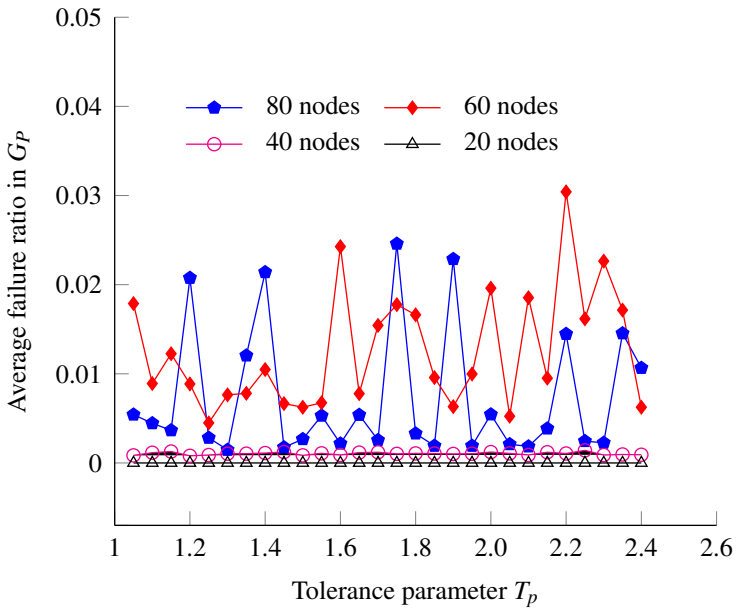


Figure 5.4: The effect of tolerance parameter upon cascading failures in power network G_P.

Figure 5.4 and Figure 5.5 show how the power network G_P and the communication network G_C perform for different values of the tolerance parameter T_p. When the number of initial failed nodes in the communication network is 20, the interdependency cascading failure is not triggered, as shown in Figure 5.4. Figure 5.4 presents that the average failure ratio for 20 initial compromised communication nodes is always zero. With the fixed initial compromised nodes (taking 60 compromised communication nodes for example) in the communication network

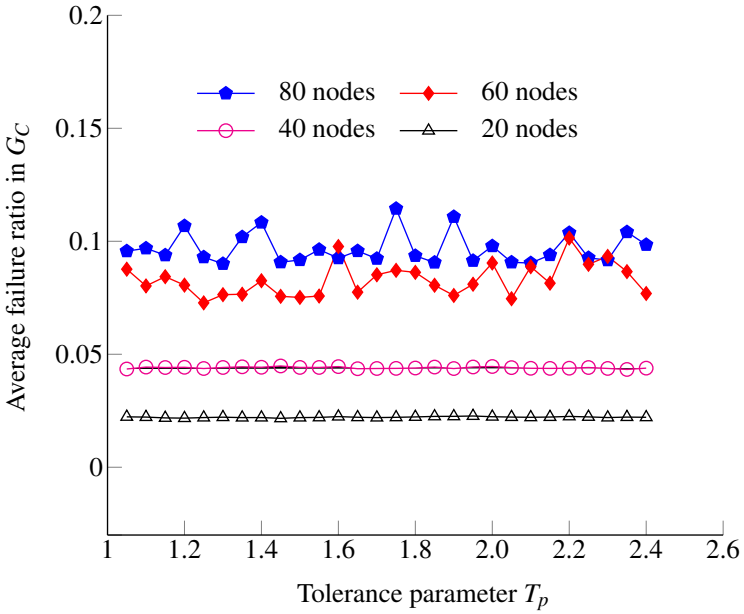


Figure 5.5: The effect of tolerance parameter upon cascading failures in communication network G_C.

G_C, the number of failed nodes in communication network G_C or power network G_P does not constantly increase or decrease with the increase of the tolerance parameter T_p. The reason behind this phenomenon is geographical criteria in allocating interdependence relations and the interdependency cascading failure.

In an isolated power network, the tolerance parameter T_p plays an important role in network resilience against a cascade and it is a critical design consideration for the power grid. A large tolerance parameter T_p will certainly prevent node overloading failures, however, it imposes higher costs to obtain a larger unused capacity. Therefore, it is significant to obtain an understanding of the impact of the tolerance parameter T_p on cascading failure propagation [38, 166]. However, the simulation results show that, due to the geographic distribution of initial compromised nodes and the use of geographic criteria in interdependence relations assignment, the impact of the tolerance parameter T_p on failure propagation in the considered interdependent power and communication network is not obvious, indicating the robustness of the modelled networks does not depend on the tolerance parameter T_p. Hence, in the following simulations, the tolerance parameter T_p of 1.5 is chosen, which, based on the simulations, appears to be neither too small nor too large.

(2) the variation of the average failure ratio with the fraction p of initial failed communication nodes

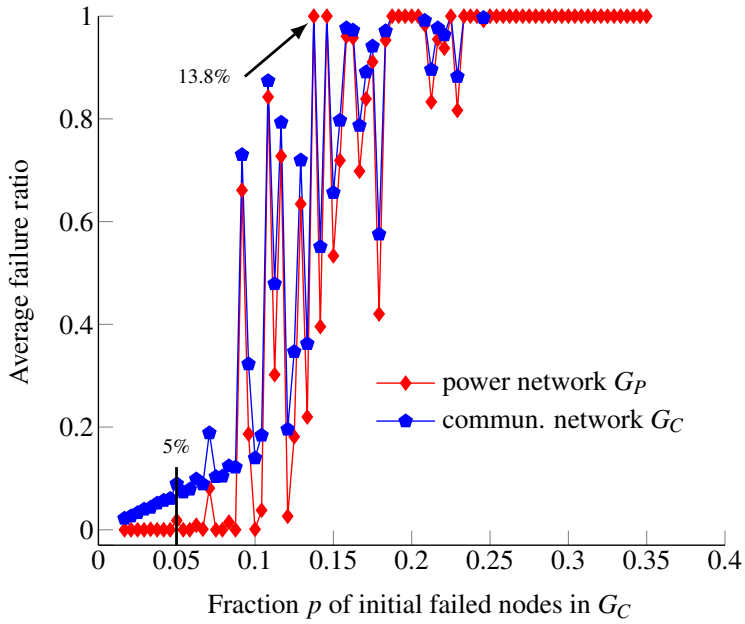


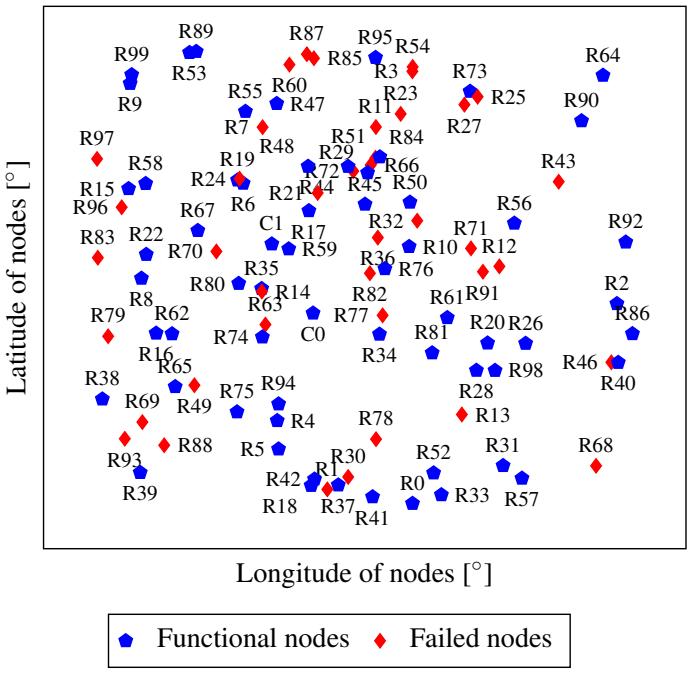
Figure 5.6: The average failure ratio versus fraction of initial failed nodes in G_C.

Figure 5.6 shows the average failure ratio in both communication network G_C and power network G_P with increasing fraction p of initial failed nodes (from 1.67% to 35%) in the communication network G_C. Recall that "average" here stands for an average taken over all test instances of the system. The simulation results show that with the increase of the fraction p of initial failed communication nodes, the average failure ratio in both power and communication networks increases, but the average number of failed power nodes is always less than that of failed communication nodes. This indicates that the power network is more robust than the communication network in the case of cyber attacks. Figure 5.6 shows that the average failure ratio in both networks is small when the fraction p of initial failed nodes in the communication network G_C is relative small (i.e., from 1.67% to 4.6%). With the increase of the faction p of initial failed communication nodes (i.e., 5% to 24.6%), the average failure ratio of both network have big fluctuations and does not have any fixed pattern for decreasing or increasing. This phenomenon may be because of the geographic distribution of the initial failed nodes in the communication network G_C. If the distribution of initial failed communication nodes is

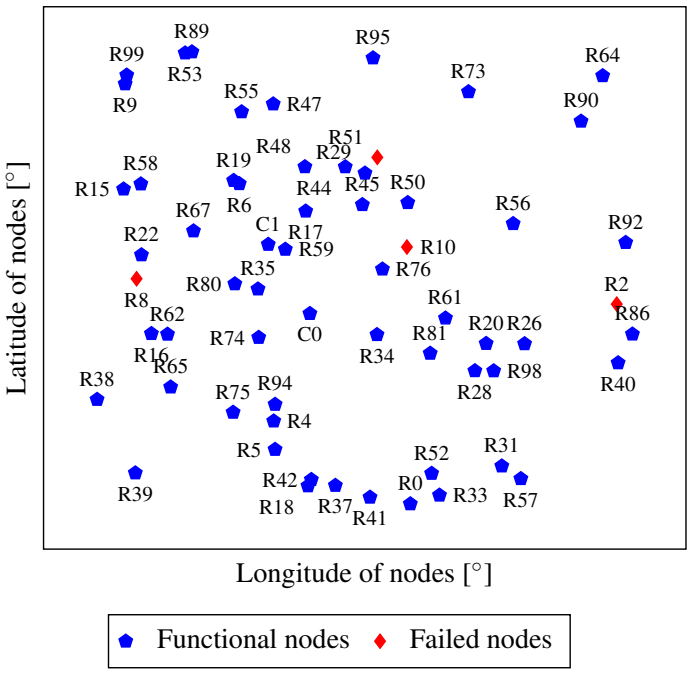
properly chosen by the attacker, a fraction of 13.8% (see Figure 5.6) initial communication failure can destroy the whole interdependent system. When the fraction p of failed communication nodes approaches 25% (300 nodes out of 1202 communication nodes), all nodes in the interdependent power and communication network fail, i.e., the average failure ratio is one and a complete outage of both the power and the communication network will be led to. Figure 5.6 shows that when the faction p of failed communication nodes is greater than 25%, no matter how those initial failed nodes are geographically distributed, the average failure ratio is always one. Therefore, on the attack perspective, an attacker can destroy the whole system by compromising a small fraction of nodes in the communication network G_C.

(3) The spatio-temporal distribution of the failure propagation

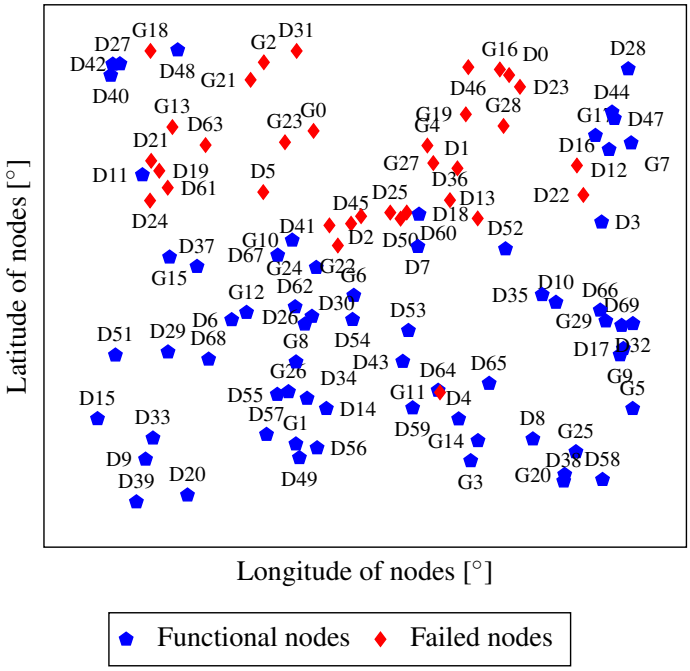
In order to show the spatial and temporal distribution of failed nodes in the failure propagation process, the communication network is reduced to include 100 relay nodes and 2 control centres; and the power network is reduced to include 30 generators and 70 distribution substations. However, all other network parameters are the same as that described in Section 5.6.1. Figure 5.7 shows the spatio-temporal characteristics of the joint effect of interdependency cascading failures and node overloading cascading failures. The x- and y-axis of Figure 5.7 are the geographic coordinates (longitude and latitude) of nodes in the simulated interdependent power and communication network. In Figure 5.7, any node (either communication node or power node) that is failed will be red (with a diamond mark) and removed from its corresponding network, and thus, is not shown at the next simulation time. Normal functional nodes (include both communication nodes and power nodes) are blue and marked with pentagon in Figure 5.7. The text shown at a proper direction of a mark in Figure 5.7 represents the name of a node in the interdependent power and communication network. For example, “R5” and “C1”denote the fifth relay node the first control centre, respectively; “G9” and “D18” represent the ninth generator and the eighteenth distribution substation node, respectively. Figure 5.7a shows the spatial distribution of the initial 40 compromised nodes (by the attacker) in the communication network G_C at simulation time 0s. The simulation time units are seconds and are denoted as “s”. Owing to the failures of those 40 compromised nodes, the communication network will fragile and the nodes that are not included in the giant cluster are considered as failed (i.e., malfunctioning). Figure 5.7b shows that, at simulation time 0.013s, 4 more communication nodes are failed because of failure propagation from those initial compromised nodes in the communication network G_C. Since the power network G_P depends on the communication network



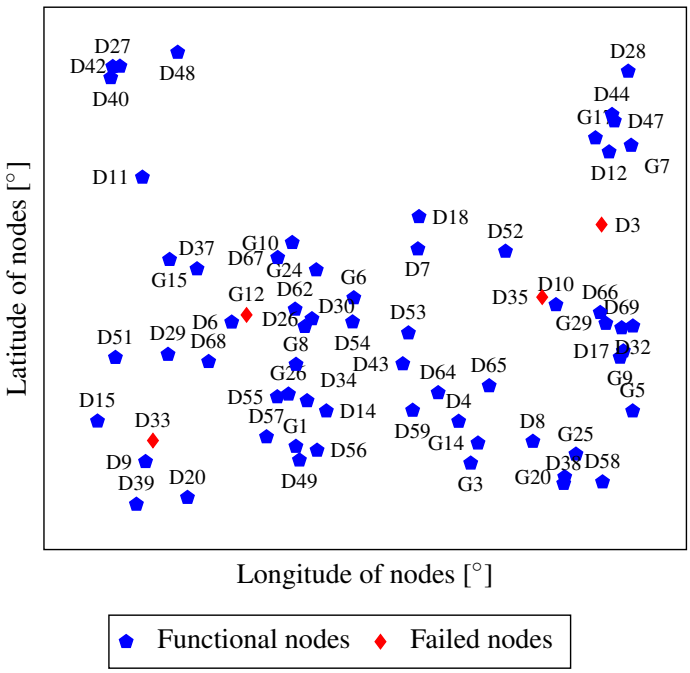
(a) Time 0s: 40 nodes are compromised in the communication network G_C.



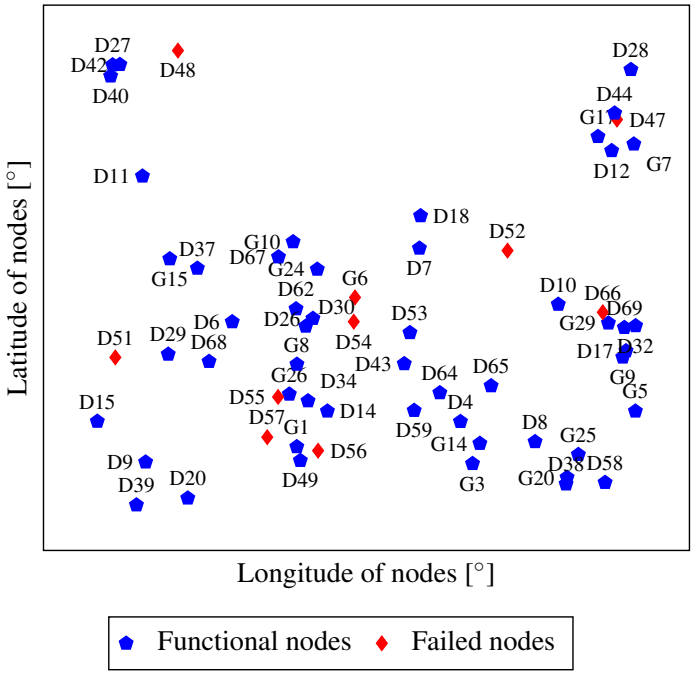
(b) Time 0.13s: 4 further communication nodes are failed because of failure propagation from initial compromised nodes.



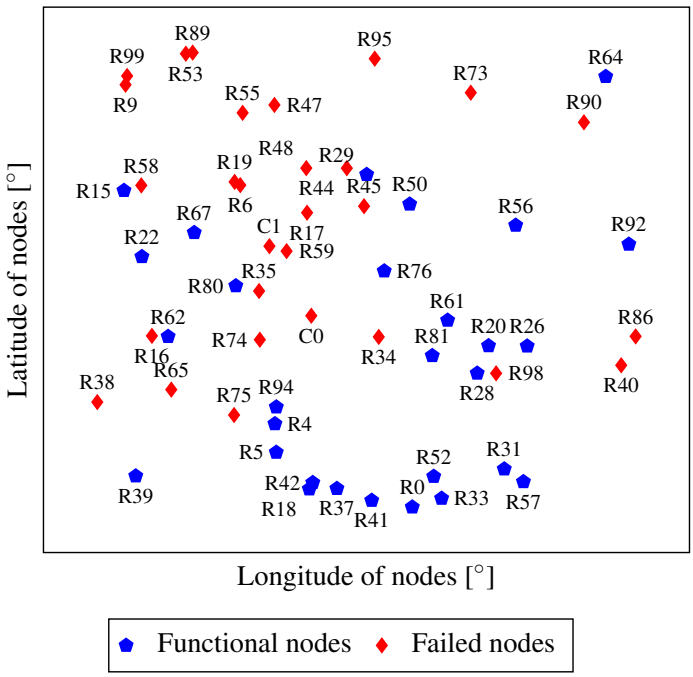
(c) Time 0.022s: 34 nodes in the power network G_P are failed because of interdependency failure cascading.



(d) Time 0.04s: 4 further nodes in the power network G_P are failed because of failure propagation from interdependency and node overloading.



(e) Time 0.05s: 10 further nodes in the power network G_P are failed because of the lack of intra support.



(f) Time 0.06s: 29 nodes in the communication network G_C are failed because of interdependency failure cascading.

Figure 5.7: Spatio-temporal characteristics of cascading failures propagation.

G_C for operations, a power node will fail if the relay node that it receives information from is failed. Figure 5.7c shows that 34 nodes in the power network G_P are failed at simulation time 0.022s because of interdependency failure cascading. The remaining power nodes in the power network G_P will be checked whether they are failed because of failure propagation from failed power nodes. Additionally, the load of those failed distribution substation nodes in the power network G_P will be redistributed and those distribution substation nodes are overloaded after load redistribution will be considered as failed. The load redistribution process will continue until no distribution substation node is overloaded. Figure 5.7d shows 4 further nodes in the power network G_P at simulation time 0.04s are failed. Those failures are caused by failure propagation from removing power nodes that are failed for lack of supported communication nodes and failure propagation from node overloading. After identifying overloaded distribution substation nodes, the remaining normal functional power nodes will be checked to see whether they are all included in the giant cluster. Figure 5.7e shows the spatial distribution of failed power nodes at simulation time 0.05s because of a lack of intra support to be connected to the giant cluster of the power network G_P. Since communication nodes are dependent on power nodes (especially distribution substations) for electricity supply, a communication node will fail if it does not have any electric support from the power network G_P. Figure 5.7f shows that 29 nodes in the communication network G_C are failed at simulation time 0.06s because of interdependency failure cascading. The failure propagation process will continue until no more interdependency cascading failures and/or node overloading cascading failures occur in the interdependent power and communication network, which denotes that the system arrives at a steady state. Parts of the failure propagation process in the simulated time (till the steady state) are shown in Figure 5.7. However, the remaining failure propagation process repeats the failure propagation steps shown from Figure 5.7b to Figure 5.7f.

5.7 Summary

This chapter analysed the costs and rewards regarding players' actions in the smart grid in order to provide a payoff formulation for the designed attacker-defender stochastic game-theoretic model. A theoretical model of interdependent power and communication networks was proposed, where both networks were viewed as fully directed networks, while interdependence relations were allocated according to physical features (i.e., geographic criteria) of the smart grid. A mathematical model was established to analyse the cascading failure propagation from

step to step, as well as realize steady state conditions in the failure propagation process. The cascading failures considered in this thesis include interdependency cascading failures and node overloading cascading failures. A load redistribution rule was proposed to non-uniformly redistribute loads of a failed distribution node among its upstream functional distribution nodes in the power grid. A cyber disruption metric was defined to quantify the characterizations (i.e., scope, magnitude, and time) of the physical impact of cyber attacks (i.e., disruptive events) on the physical power grid. Moreover, an information impact metric was defined to measure the network information security (i.e., confidentiality, integrity, and availability) impairment of communication nodes. This chapter implemented the entire interdependency cascading failure propagation and load redistribution process. The impact of the tolerance parameter T_p on the average failure ratio in power and communication networks was discussed, while the variation in the average failure ratio with different fractions of initial failed communication nodes was presented. In addition, the simulation results were found to capture the spatio-temporal characteristics of the cascading failure propagation process. The simulated cascading failure propagation process provided the type (e.g., generators, distribution substations, relay nodes) and the total number (e.g., $u_{P,\infty}$) of failed nodes needed in both the cyber disruption metric and the information impact metric, both of which are reviewed in Section 3.4.3, while an example of the compilation of simulation results into both metrics is given in Section 4.4.2. An application of the presented cost and reward analysis (in particular, the specific instantiation of the cyber disruption metric and the information impact metric) and the proposed stochastic game-theoretic cyber threat assessment framework will be presented in the next chapter.

Chapter 6

Cyber Threat Assessment Framework Analysis and Evaluation

6.1 A Sample Use Case: Multistage cyber attacks in Smart Grids

In this section, one multistage cyber attack scenario against an IEC 61850 photovoltaic (PV) inverter in smart grids will be described. This attack scenario has already been implemented and demonstrated in the course of the SPARKS project [1], under the assumption that the defence mechanism was either not present or the defence mechanism was not effective against attacks (i.e., the attacker can "sniff" traffic and identify the IP addresses and port numbers of target devices without any obstacles) [167].

IEC 61850 is a standardized data communication protocol, which is used for intelligent substation automation. Many utilities across the world have begun or are managing to deploy substation communication networks based on IEC 61850 [168]. The manufacturing message specification (MMS), which operates over a standard TCP/IP, is a communication service widely used to exchange information among IEC 61850 devices. While the MMS comes with authentication and access control functionalities, it is not designed with information security in mind [169]. The SPARKS project has derived and implemented cyber-attack capabilities based on a MITM attack on an electrical system, which uses MMS communications.

According to the demonstration cyber attacks performed in the SPARKS project, in order to modify the maximum power limit of the PV inverter or to fully shut down the PV inverter, there are many steps that the attacker should follow. The demonstration smart grid consists

[1] https://project-sparks.eu/ (Retrieved: 20/06/2017)

of an enterprise network (comprising Windows 7 office PCs), a SCADA network (including data Historian Linux machines, IEC 61850 client and other machines) and physical electric systems (comprising of PV inverter(s)). The IEC 61850 client exchanges information with the PV inverter(s).

When an attacker occurs over the Internet, he/she has a controller and a web server. To obtain his/her ultimate goal, the attacker uses a number of intermediate attack steps [2]. The attack scenario is shown in Figure 6.1. Each attack step in the demonstrated use case in Figure 6.1 is described in the following.

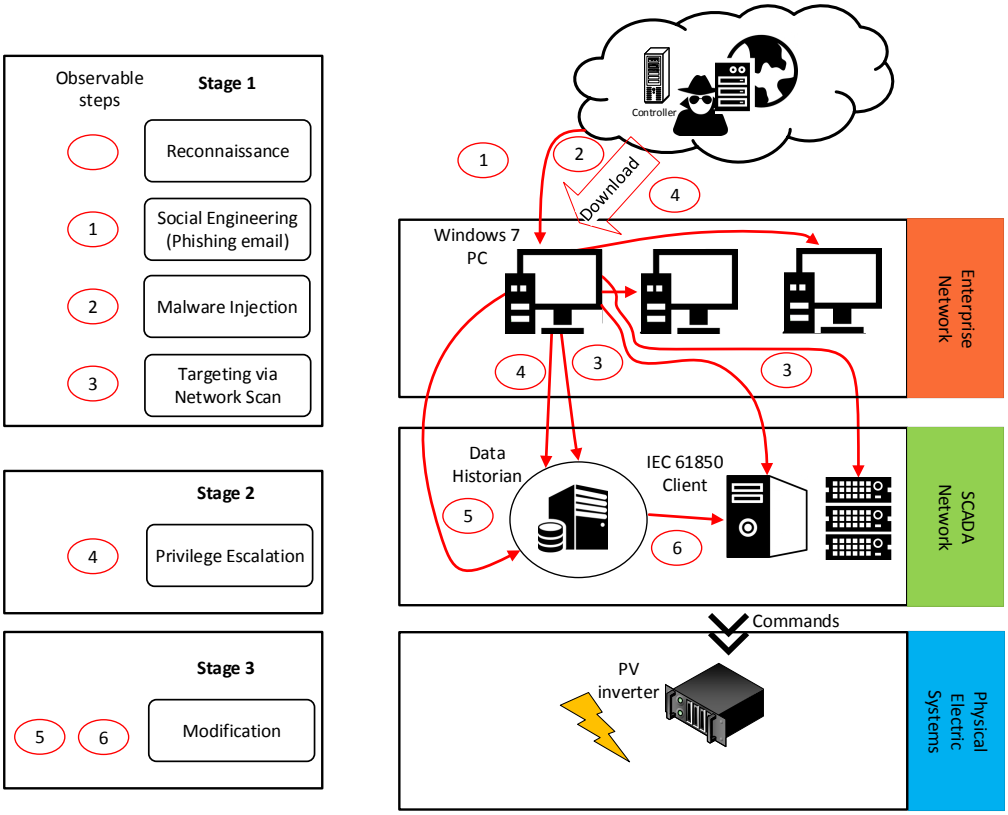


Figure 6.1: Multiple stage attack mapping chart.

Step one: The attacker sends out a phishing email to a system administrator (in the enterprise network) to request a software update installation on some of his/her systems. Before this step, the attacker has performed reconnaissance to gather information about organizational structures and operator personnels, as well as possibly obtain knowledge of assets and hosts in

the system through reconnaissance.

Step two: Once the system administrator clicks on the phishing email, the infected program is downloaded from the attacker's web server and installed on the corresponding hosts of the system (i.e., Windows 7 PCs in the enterprise network). Consequently, malware is installed. This malware downloads more malicious software, for example, remote administrator/access tool/trojan (RAT), to completely control the infected machine.

Step three: The attacker uses the compromised Windows 7 office PC to scan the network in order to identify a vulnerable machine (i.e., a web-based data Historian with an old version of Linux, who has shellshock vulnerability) as the target machine for launching further attacks in the SCADA network.

Step four: The Windows 7 office PC, which is totally under the control of the attacker, downloads Metasploit (used for penetration testing) from the attacker's controller. Then, the attacker runs Metasploit to exploit shellshock vulnerability in order to access the data Historian.

Step five: From the RAT controller, the attacker can, firstly, establish a shell connection from the office PC to the Linux machine and, secondly, instruct the data Historian to download the MITM attack tool.

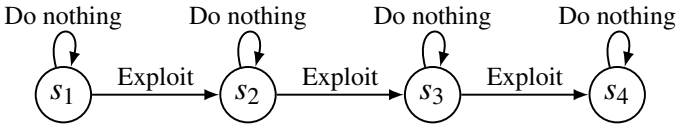
Step six: By using address resolution protocol (ARP) spoofing, the attacker launches the MITM attack on the MMS communications of the IEC 61850 client. The attacker will "sniff" IEC 61850 SCADA commands between the IEC 61850 client and the PV inverter. Based on the MITM attack, modification and injection attacks will be produced by the attacker in order to target at the PV inverter.

This thesis refers interested readers to SPARKS project and the work of [167] for an in-depth understanding of the MITM attack and attack capabilities in the demonstration multistage cyber attack scenario. SPARKS has claimed that the demonstration network scenario in Figure 6.1 can be extended to large-scale networks with many IEC 61850 clients and other machines in a SCADA network, as well as hundreds of renewable energy resources and distribution substations with loads in a physical electric system.

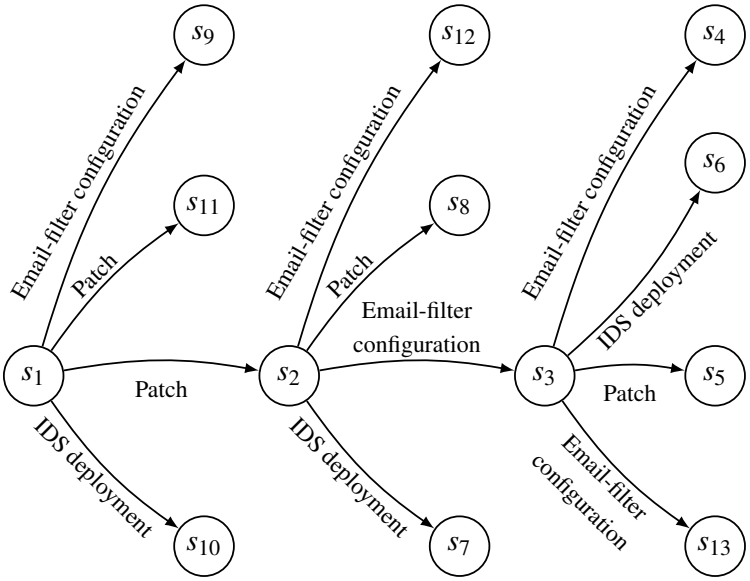
6.2 Game Setup

The above-mentioned multistage cyber attack scenario in Section 6.1 assumes that the corresponding defence mechanism is not deployed or the defence mechanism is ineffective. For example, in the first step, the email-filter is not on the Windows 7 PC; otherwise, the phishing

email would be filtered out and the attacker would compromise the Windows 7 PC with uncertainties. The attack scenario is demonstrated in a relatively small smart grid environment, but can be extended to large smart grids with medium- to low-voltage power grids. Such multistage attacks have really happened in power grids; one typical example is the Ukrainian power blackout, which took place in Christmas break in 2015. In order to avoid the recurrence of such incidents again in the future, solutions must be found to assess the threat of multistage cyber attacks and to provide the system administrator of the utility with recommendations for deploying effective defence countermeasures.



(a) Attacker's view of the game.



(b) Defender's view of the game.

Figure 6.2: Game states and transitions from each player's point of view.

According to whether the state of the network will be changed by the actions carried out by the attacker, the multistage cyber attack discussed in Section 6.1 can be viewed as a three-stage attack by the attacker to obtain his/her goal, as shown in Figure 6.1. In the first stage, the attacker exploits social engineering vulnerability to compromise the Windows 7 PC. This stage includes the first three steps of the demonstration multistage cyber attack scenario. Once the

Windows 7 PC is fully under control, the attacker exploits the shellshock vulnerability on an old version of Linux systems to in order get access to data Historian at the second stage. Finally, the attacker exploits vulnerabilities in MMS communications at the third stage, resulting in a cascading failure in a PV inverter. The attack stages in Figure 6.1 are depicted from the attacker's point of view. However, since cybersecurity in smart grids is receiving more and more attention, not only is the attacker there at every attack stage, but the defender (i.e., the system administrator) is also in place to "break" the attack vector at any stage (as long as the system administrator breaks it in any sense). Therefore, the attacker and the defender interact at every stage of the multistage cyber attack, which such an interaction can be viewed as a stage game, which is described in Chapter 4.

The game consists of two players, an attacker and a defender, as mentioned above. Both two players play a non-zero-sum game over M stages ($M = 3$ in this case). The defender is the row player (i.e., the first player) and the attacker is the column player (i.e., the second player). Each player tries to maximize his/her own expected payoffs. The set of actions available for the defender at every stage is $AS_1 = \{\text{Email-filter configuration}, \text{IDS deployment}, \text{Patch}\}$, which the set of actions available for the attacker at every stage is $AS_2 = \{\text{Exploit}, \text{Do nothing}\}$ (as defined in Section 4.3.2 of Chapter 4). The states of this three-stage game and the transitions between states are shown in Figure 6.3.

The state space is $S = \{s_1, s_2, \cdots, s_{13}\}$ in the application scenario. Figure 6.2a shows the first four game states from the attacker's point of view, Figure 6.2b shows also another nine game states (from state s_5 to state s_{13}) from the defender's point of view. The solid lines in Figure 6.2 represent possible state transitions, while the text on the solid line denotes the action profile of the attacker (in Figure 6.2a) or the defender (in Figure 6.2b). Figure 6.3 shows the game states and state transitions, where the state transition probabilities are shown in Table 6.2. The description of each state is summarized in Table 6.1.

The state in the three-stage game is defined as a combination of the operational state of the node and the defence mechanism deployed on the node, as described in Section 4.3.3 of Chapter 4. In the multistage cyber attack scenario, there are in total three kinds of communication nodes involved: Windows 7 PC, data Historian and the IEC 61850 client. The description of the state, taking state s_5 for example, includes three parts: the first part (malfunctioning, patch) shows that the Windows 7 PC is malfunctioning and a patch is applied to it; the second part (malfunctioning, Email-filter) shows that the data Historian is malfunctioning and an email

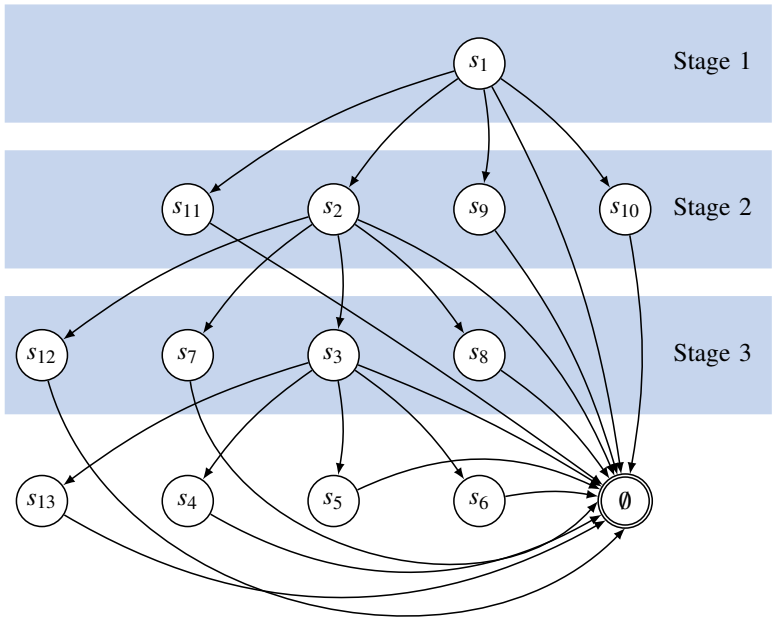


Figure 6.3: Game states and state transitions of the 3-stage game.

filter is configured on it; and the third part shows that the IEC 61850 client has a normal operational state and a patch is applied there. This work assumes that, before a threat assessment, the smart grid has no security controls in place, which is consistent with the demonstrated use case. Table 6.1 shows all states and their descriptions for the elaborated three-stage game of Figure 6.3. In Figure 6.3, the states with no direct link connection confirm that there is no state transition available between them, meaning the state transition probability is zero. In Figure 6.3, the state transition probability for any game state s ($s \in S$) to state $\emptyset$ is $1 - \sum_{s' \in \{S - \emptyset\}} q(s'|s,a,b) > 0$ (where s' is any game state that is reachable from state s). Once the attacker successfully compromised the IEC 61850 client (by attaining state s_4), he/she can send messages to shut down the PV(s).

Before the start of the game, neither the attacker nor the defender knows the real state of the game. For example, it can be the case that the attacker assumes the current game play to be in state s_1, while the defender assumes that the current game play is in state s_{11}. Nevertheless, each player presumes a probability distribution $\rho_1 \in \Delta(S)$ (S is the game state space and $S = \{s_1, s_2, \cdots, s_{13}\}$) about the initial state of the game, which is common knowledge to both players.

State name	State description
s_1	{(normal,-),(normal,-),(normal,-)}
s_2	{(malfunctioning,Patch),(normal,-),(normal,-)}
s_3	{(malfunctioning,Patch),(malfunctioning,Email-filter),(normal,-)}
s_4	{(malfunctioning,Patch),(malfunctioning,Email-filter),(malfunctioning,Email-filter)}
s_5	{(malfunctioning,Patch),(malfunctioning,Email-filter),(normal,Patch)}
s_6	{(malfunctioning,Patch),(malfunctioning,Email-filter),(normal,IDS)}
s_7	{(malfunctioning,Patch),(normal,IDS),(normal,-)}
s_8	{(malfunctioning,Patch),(normal,Patch),(normal,-)}
s_9	{(normal,Email-filter),(normal,-),(normal,-)}
s_{10}	{(normal,IDS),(normal,-),(normal,-)}
s_{11}	{(normal,Patch),(normal,-),(normal,-)}
s_{12}	{(malfunctioning,Patch),(normal,Email-filter),(normal,-)}
s_{13}	{(malfunctioning,Patch),(malfunctioning,Email-filter),(normal,Email-filter)}

"-" means nothing is configured/deployed to protect the corresponding node

Taking state s_5 ={(malfunctioning,Patch),(malfunctioning,Email-filter),(normal,Patch)} for example, the first tuple (malfunctioning,Patch) means that Windows 7 PCs are malfunctioning when patch is applied to the social engineering vulnerability; the second tuple (malfunctioning,Email-filter) denotes that the data Historian is malfunctioning when email-filter is configured; and the third tuple (normal,Patch) represents that the IEC 61850 client is normal when patch is applied to the corresponding MMS communications vulnerabilities.

Table 6.1: State names and descriptions.

Players' payoffs are composed of three parts: cyber disruption metric M_c, information impact metric I_b, and the cost of each player's action. Section 5.5 in Chapter 5 describes the payoff formulation details. Cyber disruptive metric I_b describes the consequence of a cyber attack on the physical power grid, which is a function of the scope, magnitude, and time distribution of the disruptive event (see Section 5.4 for more details). When a disruptive event affects distribution substations, the operator of the power grid should provide the disruptive magnitude (varies from 1 to 10) of the malfunctioning equipment and the expected time to recovery. The impact of action b ($b \in AS_2$) on the information security of communication nodes and the costs of players' actions are evaluated, based on expert knowledge.

Suppose the time to recover one PV inverter is 1 (as mentioned in Chapter 3, the units of

time should be chosen carefully, depending on the application; here, it is presumed that the time does not have any specific units), the disruptive magnitude of one PV inverter is 10, while the weight of this disrupted PV inverter is 0.5. In turn, the cyber disruption metric M_c can be calculated as

$$\begin{aligned} M_c &= t_d \cdot w_P^{\{i_1\}} \cdot m_P^{\{i_1\}} \\ &= 1 \cdot (0.5 \cdot 10) \\ &= 5. \end{aligned} \tag{6.1}$$

In the designed game model, the defender is assumed to have an action space of AS_1 = {Email-filter configuration, IDS deployment, Patch}, while the attacker is assumed to have an action space AS_2 = {Exploit , Do nothing}. For illustrative purposes, the relative consequences of action b ($b \in AS_2$) on the CIA of each kind of communication node are tabulated in Table C1. The relative impairment degrees (which are described in Section 5.5 of Chapter5) of any action b ($b \in AS_2$) by the attacker, in terms of confidentiality, integrity and availability, are assumed to be 0.3, 0.5, and 0.6, respectively. As discussed in Section 5.5 of Chapter 5, the impact of action b depends on expert knowledge. This thesis assumes such a value assignment to be acquirable. Thus, the impact of action b ($b \in AS_2$) on the information security on communication nodes is calculated using Equation (5.13) of Chapter 5 (it is also shown in Table C1). For example, when the attacker performs the "Exploit" action, the impact of action "Exploit" on the CIA of affected communication nodes can be calculated as

$$I_{exploit} = 0.3 \cdot 1 + 0.5 \cdot 1 + 0.6 \cdot 7 = 5. \tag{6.2}$$

As discussed in Chapter 5, the costs of actions depend on the lot of implementation costs and/or management costs of that specific action. This work assumes these costs are estimated. Table C3 presents a summary of actions' costs. It is to be noted that all the values in Table C3 are provided for illustrative purposes. Once the exact cost values are available from experts, these values shown in Table C3 can be easily replaced. After instantiating the cyber security metric M_c, the information impact metric I_b, and the cost of actions a and b ($a \in AS_1$ and $b \in AS_2$), the payoff matrices $g_{\{1,s\}}(a,b)$ and $g_{\{2,s\}}(a,b)$ ($s \in S$) can be easily calculated according to Equations (5.11) and (5.12) of Chapter 5, which is shown in Table C4. Table 6.3 presents the success probability for the attacker regarding his/her action "Exploit" at each stage and the initial belief about game states. The success probabilities shown in Table 6.3 are obtained, based on CVSS.

state s_1	state s_2	state s_3
$q(s_{11}\|s_1,3,2) = x_{s_{\{1,1\}},3} \cdot y_{s_{\{2,1\}},2}$	$q(s_{12}\|s_2,1,2) = x_{s_{\{1,2\}},1} \cdot y_{s_{\{2,2\}},2} \cdot p_{suc}(y_{s_{\{2,2\}},1})$	$q(s_{13}\|s_3,1,2) = x_{s_{\{1,3\}},1} \cdot y_{s_{\{2,3\}},2}$
$q(s_2\|s_1,3,1) = x_{s_{\{1,1\}},3} \cdot y_{s_{\{2,1\}},1} \cdot p_{suc}(y_{s_{\{2,1\}},1})$	$q(s_7\|s_2,2,1) = x_{s_{\{1,2\}},2} \cdot y_{s_{\{2,2\}},1} \cdot p_{suc}(y_{s_{\{2,2\}},1})$	$q(s_4\|s_3,1,1) = x_{s_{\{1,3\}},1} \cdot y_{s_{\{2,2\}},1} \cdot p_{suc}(y_{s_{\{2,2\}},1})$
$q(s_9\|s_1,1,1) = x_{s_{\{1,1\}},1} \cdot y_{s_{\{2,1\}},1} \cdot p_{suc}(y_{s_{\{2,1\}},1})$	$q(s_3\|s_2,1,1) = x_{s_{\{1,2\}},1} \cdot y_{s_{\{2,2\}},1} \cdot p_{suc}(y_{s_{\{2,2\}},1})$	$q(s_5\|s_3,3,1) = x_{s_{\{1,3\}},3} \cdot y_{s_{\{2,3\}},1} \cdot p_{suc}(y_{s_{\{2,3\}},1})$
$q(s_9\|s_1,1,2) = x_{s_{\{1,1\}},1} \cdot y_{s_{\{2,1\}},2}$	$q(s_7\|s_2,2,2) = x_{s_{\{1,2\}},2} \cdot y_{s_{\{2,2\}},2}$	$q(s_6\|s_3,2,1) = x_{s_{\{1,3\}},2} \cdot y_{s_{\{2,3\}},1} \cdot p_{suc}(y_{s_{\{2,3\}},1})$
$q(s_{10}\|s_1,2,1) = x_{s_{\{1,1\}},2} \cdot y_{s_{\{2,1\}},1} \cdot p_{suc}(y_{s_{\{2,1\}},1})$	$q(s_8\|s_2,3,1) = x_{s_{\{1,2\}},3} \cdot y_{s_{\{2,2\}},1} \cdot p_{suc}(y_{s_{\{2,2\}},1})$	$q(s_5\|s_3,3,2) = x_{s_{\{1,3\}},3} \cdot y_{s_{\{2,3\}},2}$
$q(s_{10}\|s_1,2,2) = x_{s_{\{1,1\}},2} \cdot y_{s_{\{2,1\}},2}$	$q(s_8\|s_2,3,2) = x_{s_{\{1,2\}},3} \cdot y_{s_{\{2,2\}},2}$	$q(s_6\|s_3,2,2) = x_{s_{\{1,3\}},2} \cdot y_{s_{\{2,3\}},2}$

For the defender (player 1), 1,2 and 3 represent his/her action "Email-filter configuration", "IDS deployment" and "Patch", respectively.

For the attacker (player 2), 1 and 2 represent his/her action "Exploit" and "Do nothing", respectively.

The success probability $p_suc(y_{2,N},1)$ ($N \in \{1,2,3\}$) describes the probability that the attacker will succeed with his/her action "Exploit".

Table 6.2: State transition probabilities.

Parameter	Value
$p_{suc}(y_{s_{\{2,1\}},1})$	0.6
$p_{suc}(y_{s_{\{2,2\}},1})$	0.1
$p_{suc}(y_{s_{\{2,3\}},1})$	0.9
belief on state s_1: $\rho_1(s_1)$	0.9
belief on state s_2: $\rho_1(s_2)$	0.1

The action "Exploit" is the 1st action of the attacker.

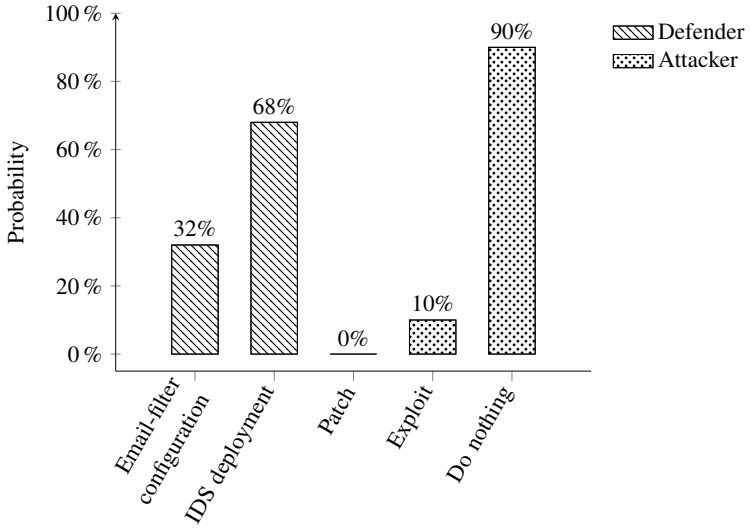
Table 6.3: Initial value of parameters.

6.3 Game Equilibrium Results

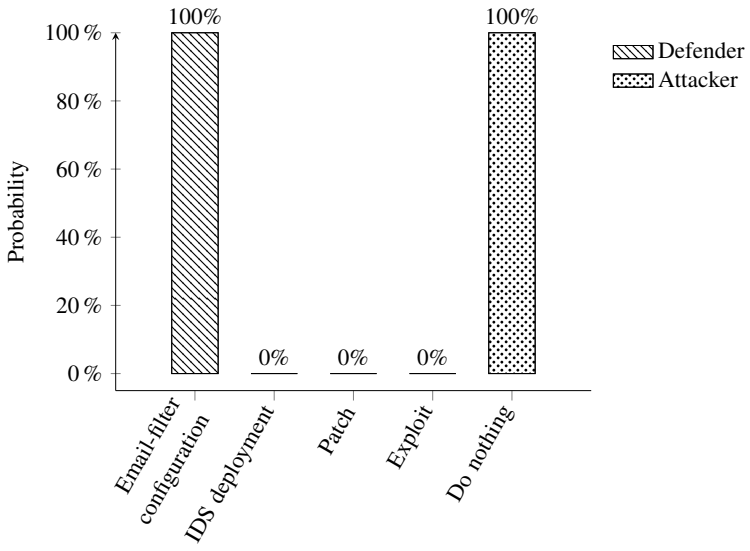
This work implemented NLP-3 (the nonlinear program problem mentioned in Chapter 4) in Maple [170] in order to find one Nash equilibrium solution for the multistage cyber attack scenario, as described in Section 6.1. Although there might be several Nash equilibria in the game, this work shall discuss the only one that is found. To run NLP-3, a complete model of the game defined in Chapter 4 is required. In the formal game model, actions carried out by both players (i.e., the attacker and the defender) are taken simultaneously. Appendix C presents the costs of actions to both players (Table C3), the impact of actions on CIA of communication nodes (Table C1), and the payoff matrices (Table C4).

While the attacker can become active at any time, the time instant for him/her to take an action can be a certain point or certain intervals in time. Thus, in this smart grid use case, this thesis imagines that both players simultaneously take action only at discrete time instants. The work ran NLP-3 on a computer equipped with a 2.83 GHz Intel(R) and 4 GB of RAM. The result of one run of NLP-3 is a set of Nash equilibria with one Nash equilibrium for each state and a set of game values for each state. Each Nash equilibrium at state s (s represents any game state and $s \in S$) is a pair of strategies $(\mathbf{x}_s^*, \mathbf{y}_s^*)$ and each set of game values is a pair of values for both players $\left(v_{\{1,s\}}, v_{\{2,s\}}\right)$ (player 1 is the defender and player 2 is the attacker). The strategy for any player consists of a probability distribution over the action space for each state s ($s \in S$). Figure 6.4 shows the Nash equilibrium pairs for the most interesting states of the game play. The game will go to end in other states, and such, these states are not shown in Figure 6.4.

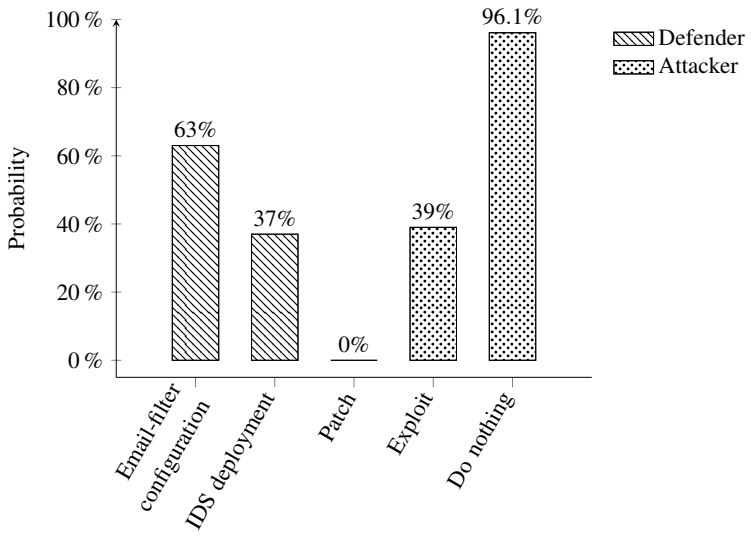
This work explains the practical meaning of the Nash equilibrium of the stochastic game-theoretic model for the most interesting states, based on the game play and payoff matrices described in Section 6.2. It is to be noted that for different payoff matrices, the game equilibria would be correspondingly different.



(a) State s_1.



(b) State s_2.



(c) State s_3.

Figure 6.4: Nash equilibria for some states of the game play.

• For Windows 7 PCs in the enterprise network, where the attacker tries to find an entry point to the smart grid, the optimal way in which to mitigate his/her risk of being compromised is to configure an email filter with a likelihood of 0.32 and deploy the IDS with a likelihood of 0.68. For the attacker, his/her optimal way of attacking Windows 7 PCs is to exploit the social engineering vulnerability with a likelihood of 0.1; to do nothing has a likelihood of 0.9. Since all the actions are instantaneous and taken at discrete time instants, the mixed Nash equilibrium suggests that, at each play round in state s_1 of the stochastic game, both players randomly choose their pure strategies (i.e., actions) from their action spaces (the actions taken in the current round of game state s_1 may not be the same actions taken in the previous round in game state s_1). However, both players should be aware of that the (asymptotic) frequencies of chosen actions must be that suggested from the mixed Nash equilibrium, for example, the (asymptotic) frequency for taking action "Email-filter configuration" in all repetitions in state s_1 of the game is 0.32. Therefore, when averaging all repetitions in state s_1 of the stochastic game, the average payoff (includes both the average immediate payoff and the average long-term payoff) is optimal. For the attacker, although exploiting the social engineering vulnerability may allow him/her to install malware and eventually totally control Windows 7 PCs, there is also a possibility that the system administrator detects the presence of the attacker and takes preventive countermeasures. The attacker will lose less if he/she simply does nothing and uses

the time to test and validate his/her attack capabilities.

• For the data Historian with an old version of Linux, the defender will not apply any patch, although it is available. The reason for this lies in the fact that the system administrator knows that the attacker will mostly "Do nothing" (by analysing the attacker's payoffs, where both actions "Exploit" and "Do nothing" let the attacker obtain the same amount of payoff). When the attacker does not launch any further attack, the defender will prefer the action of "Email-filter configuration" to be carried out in order to maximize his/her own game value. It is to be noted that although the attack can be "broken" at the first stage in the enterprise network, the defender assumes the worst, that is, the attacker succeeded at the first stage (i.e., the state of the Windows 7 PCs is (malfunctioning,Patch)) and takes corresponding countermeasures to defend against the attacker. Thus the defender will adhere to equilibrium behaviour $\tilde{\mathbf{x}}^*_{s_2} = (1,0,0)$ (i.e., configuring an email filter with a likelihood of 1) and the attacker will also adhere to his/her equilibrium behaviour $\tilde{\mathbf{y}}^*_{s_2} = (0,1)$ (i.e., doing nothing with a likelihood of 1); otherwise, neither player will have a chance of obtaining optimal payoffs (in line with the definition of Nash equilibrium [92]). Throughout this thesis, a symbol marked with a tilde means numerical approximation and that marked with an asterisk means optimality.

• For the IEC 61850 client, its vulnerabilities lie in MMS communications. By exploiting vulnerabilities found among communications between the data Historian and the IEC 61850 client, the attacker can modify/inject the command from the IEC 61850 client to the PV inverter, resulting in a cascading failure. Therefore, the reward for the attacker is not only limited to his/her impact on the communication nod (as that happened at the previous two stages), but also the consequences of his/her actions on the physical power grid. For the defender, to ''break" the attack chain from causing disruptive events in the physical electric system (especially, the PV inverter in the use case), the optimal strategy is $\tilde{\mathbf{x}}^*_{s_3} = (0.63, 0.37, 0)$, which the (asymptotic) frequency for taking action "Email-filter configuration" in all repetitions in state s_3 of the game is 0.63 and the action "IDS deployment" should be taken in other game rounds in state s_3. From the attacker's perspective, although he/she will obtain a relatively high payoff when exploiting MMS communication vulnerabilities, his/her risk of being detected might is also rather high. As once the defender knows that the weakness of the IEC 61850 client lies in MMS communications, he/she will take defense countermeasures correspondingly. Thus, the attacker's optimal strategy at this stage for the IEC 61850 client is $\tilde{\mathbf{y}}^*_{s_3} = (0.039, 0.961)$ (i.e., exploiting MMS communication vulnerabilities with a frequency of 0.039 in all repetitions in

state s_3 of the game and doing nothing at other time instants) to avoid the breakdown of his/her attack chain.

One may argue that, from intuition, since the vulnerability in social engineering is identified for this multistage cyber attack scenario, the optimal strategy for the defender is the configuration of an email filter on Windows 7 PCs, such that, the attacker has no entry point for his/her attack chain. Nevertheless, an intelligent attacker will learn about this pure strategy (i.e., "Email-filter configuration") from the defender, and he/she will do nothing. Once the defender knows the likelihood that the attacker exploiting that specific vulnerability is quite low, he/she will also consider deploying an IDS which can to some extent, prevent the download of malicious software (a significant procedure in a spear phishing attack) by scanning for attack signatures, or not pursuing any defence mechanisms at all. It is here that payoffs, which are derived from rewards (or losses) and costs of taking actions, become most relevant. When a cost is greater than the reward of carrying out that action, the optimal strategy will always favour a strategy that maximize the payoff that a player (either the defender or the attacker) will receive. The goal of this work is to figure out the best security planning for the defender to protect his/her communication networks in smart grids. The optimal security planning, at any given time instant, depends on the state of the communication network, as was the case when this work assessed the multistage cyber attack scenario for the demonstrated smart grid use case.

6.4 Discussion

6.4.1 Framework Evaluation and Validation

Evaluating and validating the proposed cyber threat assessment framework in the environment of smart grids are not as straightforward as for physical attacks. The evaluation of a cyber threat assessment is a difficult task because of the lack of agreed benchmarks and metrics for reporting results and comparing the different approaches. A few statistical measures for evaluating a threat assessment for multistage cyber attacks are discussed in [171]. However, as showed in [171], commonly used false positives and false negatives are necessary, but not sufficient to evaluate cyber threat assessments. However, for the time being, there are not publicly available benchmarks for evaluating competitive multi-players (two or more than two) under uncertainties. Moreover, the cyber threat assessment framework is formally different to those presented in the previous work [86, 86, 106], which means that direct comparisons are

not possible. Nevertheless, this work has implemented the cyber threat assessment framework for assessing threats from a sample multistage cyber attack scenario in a smart grid, as well discussed the results in Section 6.3 of Chapter 6.

The lack of validation efforts is not uncommon in the context of conducting threat assessments [171]. Formally and theoretically, there are three different ways that can be broadly used to validate the proposed cyber threat assessment framework. One is face validation, where expert opinions are collected to reach a consensus on the appropriateness of the model. Experts involved in this work refer to those who are involved in the design, architecture, implementation, analysis or maintenance of a system. However, face validation does not generally include comparison of the results from the game theoretic model against measured security incident data. The second way involves real system measurements. However, due to liability, loss of reputation and other competition issues, data on cyber incidents and disruption in power grids do not seem to be available in the public domain for the time being. The first EU-wide rules on cybersecurity, the Directive on Security of Network and Information Systems, states that one of its objectives concerns risk management and incident reporting obligations among operators of essential services and digital service providers. However, although a representative database for system configurations and cyber attacks may be available, it needs to be frequently updated to account for constantly changing network vulnerabilities, legacy systems, and attack methods. Another problem facing threat assessment framework validation is the non-repeatability of threat situations: the system administrator is unable to compare outputs from two different actions under exactly the same conditions of a real system.

The third approach available for validating a threat assessment involves theoretical results/analysis. In this thesis, Section 6.2 has simulated the developed cyber threat assessment for a multistage cyber attack scenario, while Section 6.3 has analysed game (Nash) equilibria. Checking inequalities, as implied by the equilibria, could be a way to validate the designed attacker-defender game. More specifically, for example, simulation analysis may allow both players to know the optimal strategy profiles $(\tilde{\mathbf{x}}^*, \tilde{\mathbf{y}}^*)$ from the game model and their corresponding game values. If the defender (i.e., player 1) chooses another strategy $\mathbf{x}_s \neq \tilde{\mathbf{x}}_s^*$ ($s \in S$) at any stage N and obtains another game value, the game value obtained with strategy $\mathbf{x}_s$ is certainly less than that obtained with the optimal strategy $\tilde{\mathbf{x}}_s^*$. This process can be repeated for any stage and any game state. Eventually, the checking of inequalities implied by the equilibria can be taken as evidence that the model is behaving correctly.

6.4.2 Main Features of the Cyber Threat Assessment Framework

One of the main contribution of this work is the proposition of a stochastic game-theoretic model from a technical smart grid description, meanwhile, the developed stochastic game-theoretic cyber threat assessment framework has provided us with a detailed description of the ingredients of the game (e.g., actions of players, payoffs, state transition probabilities). This framework offers a quantitative and easy-to-follow method for practitioners wehn using the game-theoretic model to analyse cybersecurity in their smart grid communication networks. An illustrative example is presented to demonstrate the application of the developed cyber threat assessment framework for assessing a multistage cyber attack in a smart grid, where the game construction can be extended to large-scale smart grids of practitioners.

This cyber threat assessment framework has addressed a flexible and practical payoff formulation for the designed stochastic game theoretic model by considering the cascading effect of cyber attacks and the presumably goal diversity of interactions between the attacker and the defender in smart grid communication networks. The quantification of impact of cyber attacks on physical power grids in cyber threat assessment frameworks has not been comprehensively explored by the research community. This work has considered connectivities and vulnerabilities of network components, information asymmetry in cybersecurity scenarios (e.g., the attacker knows his/her own attack vectors, but the defender does not), and the dynamic nature of the underlying network environment in one stochastic game-theoretic model in order to predict the behaviours of players. The developed stochastic game-theoretic cyber threat assessment framework allows future instances of the game play to depend on previous rounds, as well as enables them to capture the probabilistic nature of play changes in a smart grid environment.

This work has developed a common belief-updating mechanism for both players to refresh their belief about the current system state. The common belief is strategy-dependent and allows both players to coordinate their decisions and efficiently control the dynamic networked systems. This work has also provided an explicit formulation for equilibrium calculation. By computing and analysing the optimal mixed strategies of the game, it has been shown the possibility of providing decision supports to the system administrator in order to determine the best defence strategies for responding to the potential threat, once it has been identified. This cyber threat assessment framework can serve as a basis for recommending appropriate optimal countermeasures to system administrators in order to better manage the network defence resources.

6.4.3 Modelling Issues

A Nash equilibrium gives the defender an idea of the attacker's strategy and a plan for what to do in each state of a multistage cyber attack. There are two main modelling issues to the developed stochastic game-theoretic cyber threat assessment framework in terms of Nash equilibria. Firstly, it is a non-zero-sum game for the interaction of the attacker and the defender, giving the costs of executing actions. Unlike zero-sum games, in which a single unique game value for Nash equilibrium (or equilibria) will always be found, there is no guarantee that a non-zero-sum game has a single game value for Nash equilibrium (or equilibria). Thus, it would be impractical to compute all possible Nash equilibrium strategies for a non-zero-sum game. The existence of multiple Nash equilibrium strategies in the proposed stochastic game-theoretic model may lead the attacker to believe that the defender is not playing an actual equilibrium strategy. However, owing to the different goals and action execution costs of the attacker and the defender, the model of a game with non-zero-sum appears more reasonable in order to capture the interplay between the attacker and the defender. Secondly, this framework assumes that both the attacker and the defender have perfect rationality. This assumption should be relaxed in future work to allow for more practical attack scenarios to be considered.

The full state space of the game theoretic model may be very large. For example, for a communication network with n_C nodes, the state space can have the size of $O(m_2^{n_C})$ (m_2 is the number of defence countermeasures available for one communication node). However, this thesis is only interested in a small subset of states that are involved in attack scenarios; thus, state explosion issues are avoided, as was the case in Section 6.2 with regard to a multistage cyber attack scenario. Another difficulty is in modelling players' actions, in particular, those of the attacker. This difficulty is shared with other formal modelling techniques. In the stochastic game-theoretic model, it is assumed that the action space for each player is the same for every stage, while "Exploit" has been used to represent all attacking actions. However, there are cases where the action space in any game stage is different from that in others. In realistic attack scenarios, an attacker may devise new actions to exploit the same vulnerability in order to attack the system. However, these new actions have not been taken into account in the game-theoretic model. Nevertheless, the expansion of action spaces for both players makes the Nash equilibrium computation more complicated; and, maybe, the first issue that arises in that situation is the reduction of computational complexity. The computational complexity of the

suggested stochastic game-theoretic cyber threat assessment framework will be a significant issue to address in the future.

In practice, it may be difficult to assign the costs/rewards to the actions and the state transition probabilities. This work shares this difficulty with those involved in other qualitative and quantitative approaches for cybersecurity where similar estimates are required. In the model, the impact of an attacker's actions on the CIA comes from the advice of experts. However, there may be biases and inconsistencies in expert opinions. Though the impact value assignment is beyond the scope of this thesis, this work will leave this matter to any future work involving a greater number of experts seeking to better understand their cyber environment needs and to normalize these biases. In the stochastic game-theoretic model, both players know their own payoffs when they make decisions about the actions they will take in the next game stage. But there are situations in realistic environments where one player has uncertainties about his/her own payoffs. This work has taken into account information asymmetry among players on game state, in the future, it intends to examine asymmetric information on payoffs for players.

6.5 Summary

This chapter applied the proposed stochastic game-theoretic cyber threat assessment framework to evaluate the multistage cyber attack scenario demonstrated in the SPARKS project. The demonstrated multistage cyber attack scenario in the smart grid was described from the reconnaissance step to the final compromise of the PV inverter. Further, it elaborated the transformation of a multistage attack scenario to a stochastic game, including game stages and states, payoff matrices for each game state, and state transition probabilities. The stochastic game was implemented and the practical meanings of the game equilibria for each type of assets in the smart grid were explained in detail. Additionally, it discussed the difficulties in evaluating and comparing cyber threat assessments, as well as presented challenging and possible approaches to validating the proposed cyber threat assessment framework. Next, it presented the main features of the developed cyber threat assessment framework. Finally, it investigated some further modelling issues, which may arise in extending the proposed cyber threat assessment framework.

Chapter 7

Conclusions and Future Work

7.1 Main Contributions and Results

There has been increased concern that cyber-physical systems are targets of cyber attacks, which only affect the cyber network, but can also impact the physical network. The electric power grid is extremely dependent on ICT infrastructure to enable the integration of renewable energy resources/electric vehicles and perform automated monitoring and control functions. The exposure of new ICT assets and their increasing adoption in smart grid initiatives are making smart grids more vulnerable to cyber threats, while raising numerous concerns about the adequacy of current security approaches. Cyber attacks have the ability to compromise equipment in the physical power grid and render them unavailable at critical times of operations. Cyber threats are evolving over time and becoming highly complicated, resulting in the use of multistage attacks, which are composed of a number of interrelated attack steps, whereby the immediate attack is only one step in a more complex chain of related events.

Most of the standards and guidelines for smart grid cyber threat and risk assessments, such as NIST-IR 7628 [21] or the protection profiles published by BSI [22, 23], have been deemed to be too general and high-level to provide enough detail to conduct proper threat and risk assessments in smart grids. Although a wealth of research (even at the European project level) have been conducted to address cyber security paradigms, many threat and risk assessment solutions are mainly centred around assessing vulnerabilities and cyber threats, without adequately addressing the additional constraints (e.g., a mix of legacy and new systems) required to support threat and risk assessments in smart grids. Threat and risk assessments will become even worse when the roll-out of smart grids leads to a large complex combination of legacy

and new technologies. The application of game theory in smart grid communication networks for assessing threats from multistage cyber attacks and the prediction of an attacker's action at each step of a multistage cyber attack, are still in their infancy nowadays. Furthermore, the impact of cyber attacks on physical power grids has not been fully analysed.

This thesis investigates an application-oriented stochastic game-theoretic cyber threat assessment framework, which is strongly related to the risk management process given in the ISO/IEC 27005 standard. The cyber threat assessment framework is tailored to address the specific challenges of performing threat assessments for multistage cyber attacks in smart grid communication networks. A multistage cyber attack is composed of multiple steps, where the success of the previous step usually provides occurring conditions for the next step, with such situations covered by a stochastic game. Therefore, a stochastic game-theoretic model is designed as the proposed stochastic game-theoretic cyber threat assessment framework.

In the designed stochastic game-theoretic model, there are two players: the attacker, who represents a team of cooperating opponents, and the defender, who represents a whole team of system administrators and security operators. The designed stochastic game-theoretic model captures the presumed goal diversity and information asymmetry characteristics of adversarial interactions between the attacker and the defender in smart grid communication networks. This model takes into account the common knowledge about the system, which is available to both the attacker and the defender in terms of asset information, vulnerability databases, and network topology/connectivity. At every step of the multistage attack chain, both players have motivations and capabilities to launch further attacks or defend against attacks. Therefore, there is a probability that the game will end in any game state, with such a probability being positive. Hence, the designed stochastic game-theoretic model is established with positive stop probabilities in each game state in mind.

Due to the fact that no player knows the exact current game state (instead both players have a private local game state), this thesis proposes a belief (i.e., a probability distribution) updating mechanism for both players to form a common belief about the current game state. The formulated common belief is strategy-dependent and allows both players to coordinate their decisions and efficiently control the dynamic networked systems. This thesis provides an explicit formulation for equilibrium calculation. The ingredients of the designed stochastic game-theoretic model is elaborated in detail and provides a solid basis for the implementation of the proposed stochastic game-theoretic cyber threat assessment framework.

To provide a flexible and practical payoff formulation for the designed stochastic game-theoretic model, a mathematical analysis of the cascading failure propagation in an interdependent power and communication network model is presented in this thesis. The cascading failures considered in this thesis include both interdependency cascading failures and node overloading cascading failures. In the proposed interdependent power and communication network model, both power and communication networks are modelled as fully directed networks, while interdependence relations between the power network and the communication network are allocated according to physical features (e.g., geographic criteria) of smart grids in realistic cases. Additionally, a load redistribution rule is proposed to non-uniformly redistribute loads of a failed distribution node among its upstream functional distribution nodes in the physical power grid. Simulation results show the spatial characteristics of cascading failure propagation from the joint effect of interdependency and node overloading failures. The physical impact of cyber attacks is characterized by defining a cyber disruption metric, which quantifies the scope, magnitude, and the time distribution of disruptive events in power grids. As a cyber attack can also impact on the information security of nodes in communication networks, this thesis defines an information impact metric to measure the network information security (i.e., confidentiality, integrity, and availability) impairment of communication nodes. Consequently, a player's payoff when carrying out an action is formulated by combining the cyber disruption metric and the impact metric with the cost of taking that action.

The presented application-oriented stochastic game-theoretic cyber threat assessment framework elaborates detailed implementation steps for smart grid practitioners to follow when conducting the threat assessment process. The proposed cyber threat assessment framework is implemented, based on suitable software tools. Furthermore, the proposed stochastic game-theoretic cyber threat assessment framework is applied to evaluate a demonstrated multistage cyber attack scenario in a smart grid system, while the practical meaning of the output from the proposed stochastic game-theoretic cyber threat assessment framework is explained in detail. Finally, the difficulties in evaluating/comparing cyber threat assessment processes, challenges and possible approaches to validate the proposed cyber threat assessment framework, main features and modelling issues of the developed stochastic game-theoretic cyber threat assessment framework are discussed.

The proposed application-oriented stochastic game-theoretic cyber threat assessment framework can be integrated into existing risk management processes, which are running in smart grids, or applied as a standalone threat assessment process in architectural concepts of proposed

new smart grid use cases. The expected and appropriate optimal security countermeasures for defenders to defend against multistage cyber attacks can be estimated from the designed stochastic game-theoretic model presented in this thesis. As the stochastic game-theoretic cyber threat assessment framework is solely software based, it does not require costly and energy-consuming centralized server hardware. Moreover, this framework can be executed on an isolated machine, while the assessment implementation has no impact on the running of smart grid communication infrastructures.

7.2 Possible Extensions

As mentioned in Section 3.4.2, there are some assumptions behind the proposed stochastic game-theoretic cyber threat assessment framework. Meanwhile, Section 6.4.3 has suggested further research work on relaxing the rationale assumption, modelling players' action spaces, analysing computational complexity, and assigning costs/rewards for players' actions. This section discusses possible future directions that may deepen the understanding of threat assessment, intensify the exploration of cascading failure propagation, and enhance the ability to design a proper threat assessment process, which operates efficiently and is end-user friendly.

Important parts of the proposed stochastic game-theoretic cyber threat assessment framework have already been implemented (e.g., players' payoff formulation and control recommendation); however, other aspects of fully fledged implementation are still missing. This work has manually generated the adversarial graph from our use case attack scenario. Nevertheless, security argument graphs need to be integrated into the stochastic game-theoretic cyber threat assessment framework in order to provide a precise underpinning for threat modelling. A security argument graph is a graphical representation that integrates various kinds of security-related information (e.g., threat agents and system components) to determine about the security level of a system. Such graphs can be automatically constructed by the Cyber Security Argument Graph Evaluation (CyberSAGE) tool [172, 173], which deals with National Electric Sector Cybersecurity Organization Resource (NESCOR) failure scenarios as security argument graphs. While this thesis presents a smart grid network model, consisting of three kinds of nodes in the smart grid communication network, an advancement of this work would be to consider a larger network model with more node heterogeneity or to apply the threat assessment framework to the broader context of energy distribution networks. The designed stochastic game-theoretic model needs to be extended to allow for three or more players in

more smart grid-related network security scenarios. Furthermore, one important aim of future work would be to better understand the attack steps, in order to appreciate the different targets of the adversary and facilitate modelling stages in the stochastic game-theoretic model.

A promising approach for system reliability and robustness enhancement is to introduce redundant design, for example, redundancies of communication nodes/power equipments in the smart grid and redundancies of interdependencies of power grids and communication networks. However, there is still a lack of any general way to determine and analyse the optimal number of redundant nodes that the smart grid needs in order to reduce the risk of cascading failures and, at the same time, to balance the complexity of the system. Additionally, there is not any generic quantitative methodology to analyse the impact of redundant communication nodes/power equipments on the cascading failure propagation process. Therefore, further studies on these matters would be of great significance.

Another observation concerning cascading failure propagation is the potential single point of failures on control centres in smart grid communication networks. The main role of control centres is to collect information from adjacent information relays and make electricity controlling decisions. Once control centres experience failures, power nodes will lose their controls, resulting in energy instability. The combination of advances in network function virtualization could be an interesting approach to provide application-level high availability and resilience of control centres. Another critical issue that arises from cascading failure propagation is the real physical features of the power grids. This thesis has taken node capacity and network heterogeneity of the power grid into account when implementing the proposed cascading failure propagation approach. Further models that consider more physical features (e.g., power flow) when analysing cascading failures should offer more insightful results for cascading failure propagation in interdependent cyber-physical systems.

In the designed stochastic game-theoretic model, both players are Bayesian players, who have a prior probability distribution about which game state is being played. However, there are situations where both the attacker and the defender are non-Bayesian, that is, they do not have a prior probability distribution on the game states or their utility functions. Non-Bayesian players have been investigated in repeated games [174, 175]; however, including them in stochastic games is a promising future research direction. The visualization of the presented cyber threat assessment process with other solutions is a highly interesting research objective in order to enable a better understanding of the proposed stochastic game-theoretic cyber threat assessment

framework for practitioners. As an extension, this work will develop or integrate a suite of end-user friendly tools, which can be used to support the visualization of the implementation of the stochastic game-theoretic cyber threat assessment framework. As discussed in Section 6.4, there is a lack of agreed benchmarks and metrics for evaluating and comparing different cyber threat assessment methods and frameworks. Therefore, apart from the design and application of these methods and frameworks, the development of evaluation metrics for threat and risk assessment methods and frameworks should be of significant importance to future research. The proposed stochastic game-theoretic model imposes no restrictions whatsoever on the units in which the payoffs are defined. Hence, for a concrete instantiation of the models for an application, the most suitable security metric can be used to set the payoffs in the stochastic model.

The above-mentioned thoughts are intended to provide good starting points for future research, which could significantly extend the solution methods and results presented in this thesis.

Appendix A

Abbreviations, mathematical notations and symbols

A.1 List of Abbreviations

The number after each abbreviation indicates the page on which the abbreviation is defined.

ACTs attack countermeasure trees 27

ADTs attack-defense trees 27

AGs attack graphs 27

AMIs advanced metering infrastructures 6

ANSI American National Standards Institute 6

APT advanced persistent threat 3

ARP address resolution protocol 125

ATs attack trees 26

BNE Bayesian Nash Equilibrium 44

BSI Bundersamt für Sicherheit in der Informationstechnik 3

CAPEC common attack pattern enumeration and classification 25

CIA confidentiality, integrity, and availability 20

CPTs conditional probability tables 31

List of Abbreviations

CVE common vulnerability enumeration 25

CVSS common vulnerability scoring system 66

CWE common weakness enumeration 25

DC direct current 24

DDoS distributed denial of service 3

DERs distributed energy resources 6

DoS denial of service 3

DSOs distributed systems operators 6

EC European Commission 17

ENISA European Union Agency for Network and Information Security 6

FANs field area networks 6

HAG hybrid attack graph 28

HMI human-machine interface 3

HMMs hidden Markov models 31

ICMP Internet Control Message Protocol 59

ICS industrial control system 4

ICT information and communication technology 1

IDS Intrusion detection system 51

IEDs Intelligent electrical devices 21

LANs local area networks 6

MDP Markov decision process 28

MITM man-in-the-middle 57

MMS manufacturing message specification 123

MPE Markov perfect equilibria 82

NANs neighbourhood area networks 6

NERC North American Electric Reliability Corporation 17

NIST National Institute of Standards and Technology 6

NLP Nonlinear programming 54

PBE perfect Bayesian equilibria 82

PLC programmable logic controller 62

POMDP partially observable Markov decision process 82

PRISM Performance and Risk-based Integrated Security Methodology 17

PV photovoltaic 123

RAT remote administrator/access tool/trojan 125

RSMP Reference Security Management Plan for Energy Infrastructure 17

SAG sequential attack graph 28

SCADA supervisory control and data acquisition 1

SGAM smart grid architecture model 20

SGIS Smart Grid Information Security 17

SGLIOS stochastic game with lack of information on one side 68

SPBE structured Bayesian perfect equilibria 82

TARA threat assessment & remediation analysis 25

TTPs tactics, techniques, and procedures 25

UPS uninterruptible power supply 96

VPN virtual private network 5

WANs wide area networks 6

A.2 General Notations

In general, the following rules are applied (x and X are used as wildcards in this list):

- Random variables are denoted by upper case normal font letters, their realizations by the corresponding lower case letters
- Bold letters refer to row vectors (lowcase letters) or matrices (uppercase letters)

- All functions are denoted in uppercase calligraphic letters (such as $\mathcal{F}$)
- "Blackboard bold" capital letters refer to a set of numbers, like $\mathbb{N}$ refers to natural numbers, $\mathbb{R}$ refers real numbers, $\mathbb{E}(\cdot)$ refers to the expectation, and $\mathbb{P}$ refers to the probability of an event
- The conditional probability that a event A would happen given that event B happened is denoted as $\mathbb{P}(A|B)$
- The probability of two events A and B is interpreted as $\mathbb{P}(A,B) = \mathbb{P}(A \cap B)$
- The cardinality of the set x is denoted as $|x|$
- Approximations of a x (scalar, distribution, etc) are marked by a tilde — $\tilde{x}$
- Optimality of a x (scalar, distribution, etc) are marked by an asterisk — x^*
- Mean and average of a x are marked by a bar — $\bar{x}$
- The disjoint set union of set X_1 and X_2 is marked as $X_1 \uplus X_2$
- The transpose of a x (vector, matrix, etc) is denoted as $(x)^T$
- $\times$ The Cartesian product operation
- $\sum$ Sum of all values in range of series
- $\prod$ Product of all values in range of series

A.3 List of Symbols

The number after each symbol indicates the page on which the symbol is first occurred.

m_1	number of actions for player 1 and $m_1 = \|AS_1\|$ 40
AS_1	action space of player 1 51
AS_2	action space of player 2 51
$\mathbf{x}^*_{s_N}$	player 1's optimal strategy in state s_N 81
$\mathbf{y}^*_{s_N}$	player 2's optimal strategy in state s_N 81

$B_{P(0)}^{\{i\}}$	the betweenness of a power node $v_P^{\{i\}}$ 99
$C_P^{\{i\}}$	the load capacity of a power node $v_P^{\{i\}}$ 99
I_b	the impact of action b from the attacker on information security of nodes in the communication network 53
M_c	the cyber disruption metric 53
h_N	a common knowledge of the game up to (but exclude) stage N 69
G_C	a communication network 94
$v_C^{\{i\}}$	a communication node in the communication network 98
n_C	the number of nodes in the communication network 94
Ava_b	the relative impairment degree that action b ($b \in AS_2$) has made in availability 110
δ	communication nodes' assets in availability 110
Con_b	the relative impairment degree that action b ($b \in AS_2$) has made in confidentiality 110
α	communication nodes' assets in confidentiality 110
Int_b	the relative impairment degree that action b ($b \in AS_2$) has made in integrity 110
β	communication nodes' assets in integrity 110
C_a	the cost of the action a ($a \in AS_1$) 110
C_b	the cost of the action b ($b \in AS_2$) 110
$\theta_N(\ell)$	defense state of a node ℓ in the communication network at stage N 52
t_d	the time duration of the disruptive events 109
n_d	the number of distribution substations in the power network 95
Θ_r^{out}	the number of downstream nodes that the power node $v_P^{\{r\}}$ has 105
E	a random variable representing the stage the game ends 70
$\emptyset$	empty set 68

$\mathcal{H}(\cdot)$	the total expected payoff function. In the non-zero-sum game, an index i will be added 70
$\mathcal{A}_N(\cdot)$	the expected payoff function at stage N 70
$\mathcal{R}_N(\cdot)$	the expected immediate payoff function under the condition that the game does not end at N stage. In the non-zero-sum game, an index i will be added 70
j	number of incoming edges of an arbitrary node in any network 95
$\triangle_c L_{P(t)}^{\{r\}}$	the load incremental factor of the power node $v_P^{\{r\}}$ 104
$L_{P(0)}^{\{i\}}$	the initial load of the power node $v_P^{\{i\}}$ 98
$s_{\{1,N\}}$	the private local state observed by player 1 at stage N 72
$s_{\{2,N\}}$	the private local state observed by player 2 at stage N 72
$\mathbf{T}_1(s_N, \mathbf{v})$	a matrix to describe the long-term payoff of player 1 when player 1 is in state s_N 80
k	number of outcoming edges of an arbitrary node in any network 95
$O_P^{\{r\}}$	a random variable which denotes the power node $v_P^{\{r\}}$ is overloaded 105
$\mathbf{G}_{\{s_\ell\}}$	the matrix of immediate payoffs that a player receives at state s_ℓ 68
$\mathbf{G}_{\{1,s_\ell\}}$	the matrix of immediate payoffs that player 1 receives at state s_ℓ 71
$\mathbf{G}_{\{2,s_\ell\}}$	the immediate payoff matrix that player2 receives at state s_ℓ 71
ρ_N	the belief of game states at stage N and $\rho_N \in \Delta(S)$ 70
S	a finite set of states $S = \{s_1, s_2, \cdots, s_\ell, \cdots, s_{k_C}\}$, where $k_C = \|S\|$ is the number of states in S 52
i	the i-th player in the game and $i \in I$ 36
I	a set of players 36
G_P	a power network 94
$v_P^{\{i\}}$	a power node in the power network 98
$v_P^{\{r\}}$	one upstream distribution nodes of the node $v_P^{\{i\}}$ 104
n_P	the number of nodes in the power network 94

ρ_1	a prior information $\rho_1 \in \Delta(S)$ about the initial state 68
$\mathbf{J}_\ell$	the $1 \times \ell$ ($\ell \in \{m_1, m_2\}$) row vector with all 1s 83
Ω^{m_1}	the set of all probability vectors of length m_1 69
Ω^{m_2}	the set of all probability vectors of length m_2 70
s_N	the game state at stage N 65
k_C	$k_C = \|S\|$ is the total number of states 68
$p_{suc}(y_{s,b})$	the attacker's success probability of taking action $y_{s,b}$, $s \in S$, $b \in AS_2$ 66
$\mathbf{v}$	a value vector which is a sub-vector of the game value vector 80
$L_{P(t)}^{\{i\}}$	the load of a power node $v_P^{\{i\}}$ at time t 99
T_p	the tolerance parameter 99
$q(\cdot\|\cdot)$	state transition probability 67
u	the probability that there is no path from the giant cluster to the node from which a randomly chosen link originates 103
Θ_i^{in}	the set of functional upstream distribution nodes that the node $v_P^{\{i\}}$ has 104
v	the probability that a node to which a randomly chosen link leads has no path to the giant cluster 102
$\mathbf{v}_1$	the set of values for player 1 and $\mathbf{v}_1 = (v_{1,s_1}, v_{1,s_2}, \cdots, v_{1,s_{k_C}})$ 80
v_{1,s_ℓ}	player 1's value of the game in state s_ℓ 80
$\mathbf{v}_2$	the set of values for player 2 and $\mathbf{v}_2 = (v_{2,s_1}, v_{2,s_2}, \cdots, v_{2,s_{k_C}})$ 80
v_{2,s_ℓ}	player 2's value of the game in state s_ℓ 80
$w_P^{\{i\}}$	the weight of a power node $v_P^{\{i\}}$ 99
$\phi_N(\ell)$	working state of a node ℓ in the communication network at stage N 52
$\mathbf{x}$	a vector of mixed strategies of player 1 69
$\mathbf{x}_s$	the mixed strategy of player 1 in state s 69
$y_{s,b}$	the probability that b action of the attacker is taken 66
$\mathbf{y}$	a vector of mixed strategies of player 2 70

$\mathbf{y}_s$	the mixed strategy of player 2 in state s 69

Appendix B

Derivation of equations

From probability theory and statistics, it can be seen that $\mathbb{P}(A|BC) = \dfrac{\mathbb{P}(ABC)}{\mathbb{P}(BC)}$. Therefore,

$$\begin{aligned}&\mathbb{P}(s_{\{1,N-1\}}|h_{N-1},a_{N-1})\\&= \frac{\mathbb{P}(s_{\{1,N-1\}},h_{N-1})\cdot\mathbb{P}(a_{N-1}|s_{\{1,N-1\}},h_{N-1})}{\mathbb{P}(h_{N-1},a_{N-1})}\end{aligned} \tag{B1}$$

Now, let's analyse Equation (B1) term by term. The conditional probability of A given B is defined as $\mathbb{P}(A|B) = \dfrac{\mathbb{P}(AB)}{\mathbb{P}(B)}$. Therefore,

$$\mathbb{P}(s_{\{1,N-1\}},h_{N-1}) = \mathbb{P}(h_{N-1})\cdot\mathbb{P}(s_{\{1,N-1\}}|h_{N-1}) \tag{B2}$$

and the denominator of Equation (B1) can be further expressed as

$$\begin{aligned}&\mathbb{P}(h_{N-1},a_{N-1})\\&= \mathbb{P}(h_{N-1})\cdot\mathbb{P}(a_{N-1}|h_{N-1})\\&= \mathbb{P}(h_{N-1})\cdot\sum_{s'_{\{1,N-1\}}}\mathbb{P}(a_{N-1}|h_{N-1},s'_{\{1,N-1\}})\cdot\mathbb{P}(s'_{\{1,N-1\}}|h_{N-1})\end{aligned} \tag{B3}$$

Substituting Equation (B2) and Equation (B3) into (B1), we get

$$\begin{aligned}&\mathbb{P}(s_{\{1,N-1\}}|h_{N-1},a_{N-1})\\&= \frac{\mathbb{P}(h_{N-1})\cdot\mathbb{P}(s_{\{1,N-1\}}|h_{N-1})\cdot\mathbb{P}(a_{N-1}|s_{\{1,N-1\}},h_{N-1})}{\mathbb{P}(h_{N-1})\cdot\sum_{s'_{\{1,N-1\}}}\mathbb{P}(s'_{\{1,N-1\}}|h_{N-1})\cdot\mathbb{P}(a_{N-1}|h_{N-1},s'_{\{1,N-1\}})}\end{aligned} \tag{B4}$$

Since the visited game state s_{N-1} at $N-1$ stage is known by both players and the actions a_{N-1} and b_{N-1} are also components of history h_N for N stage, Equation (B4) can be further written as

$$
\begin{aligned}
&\mathbb{P}(s_{\{1,N-1\}}|h_{N-1},a_{N-1}) \\
&= \frac{\mathbb{P}(s_{\{1,N-1\}}|h_{N-1})\cdot\mathbb{P}(a_{N-1}|s_{\{1,N-1\}},h_{N-1})}{\sum_{s'_{\{1,N-1\}}}\mathbb{P}(s'_{\{1,N-1\}}|h_{N-1})\cdot\mathbb{P}(a_{N-1}|s'_{\{1,N-1\}},h_{N-1})} \\
&= \frac{\mathbb{P}(s_{\{1,N-1\}}|h_{N-1})\cdot x_{s_{\{1,N-1\}},a_{N-1}}}{\sum_{s'_{\{1,N-1\}}}\mathbb{P}(s'_{\{1,N-1\}}|h_{N-1})\cdot x_{s'_{\{1,N-1\}},a_{N-1}}}.
\end{aligned}
\tag{B5}
$$

Appendix C

Tables for smart grid use case

Machine Type	Action b	Con_b	Int_b	Ava_{ab}	Impact of action b I_b
Windows PC	Exploit	1	1	7	5
	Do Nothing	0	0	0	0
Data Historian	Exploit	3	1	1	2
	Do Nothing	0	0	0	0
IEC 61850 client	Exploit	2	10	4	8
	Do Nothing	0	0	0	0

Table C1: Impact of actions from the attacker on CIA of communication nodes.

C. TABLES FOR SMART GRID USE CASE

State name	Defender's equilibrium strategy	Defender's game value	Attacker's equilibrium strategy	Attacker's game value
s_1	(0.32,0.68,0)	-1.495	(0.1,0.9)	0
s_2	(1,0,0)	-2	(0,1)	0
s_3	(0.577,0.423,0)	-2.501	(0.039,0.961)	0

For the defender (player 1), $(\mathbb{P}(A), \mathbb{P}(B), \mathbb{P}(C))$ represents the probability to take action "Email-filter configuration" is $\mathbb{P}(A)$, the probability to take action "IDS deployment" is $\mathbb{P}(B)$, and the probability to take action "Patch" is $\mathbb{P}(C)$.

For the attacker (player 2), $(\mathbb{P}(A), \mathbb{P}(B))$ represents the probability to take action "Exploit" is $\mathbb{P}(A)$ and the probability to take action "Do nothing" is $\mathbb{P}(B)$.

Table C2: Nash equilibrium strategies and game values for some states of the game between the defender and the attacker.

Player	Action	Cost
Attacker	Exploit	2
	Do nothing	0
Defender	Email-filter configuration	2
	IDS deployment	3
	Patch	5

Table C3: Cost of actions from both players.

$\mathbf{G}_{\{1,s_1\}} = \begin{bmatrix} 3 & -2 \\ -6 & -1 \\ -10 & -5 \end{bmatrix}$	$\mathbf{G}_{\{2,s_1\}} = \begin{bmatrix} -7 & 0 \\ 3 & 0 \\ 3 & 0 \end{bmatrix}$
$\mathbf{G}_{\{1,s_2\}} = \begin{bmatrix} -4 & -2 \\ -1 & -3 \\ -3 & -3 \end{bmatrix}$	$\mathbf{G}_{\{2,s_2\}} = \begin{bmatrix} 0 & 0 \\ -4 & 0 \\ -4 & 0 \end{bmatrix}$
$\mathbf{G}_{\{1,s_3\}} = \begin{bmatrix} -15 & -2 \\ 10 & -3 \\ 8 & -5 \end{bmatrix}$	$\mathbf{G}_{\{2,s_3\}} = \begin{bmatrix} 11 & 0 \\ -15 & 0 \\ -15 & 0 \end{bmatrix}$
$\mathbf{G}_{\{1,s_4\}} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$	$\mathbf{G}_{\{2,s_4\}} = \mathbf{G}_{\{1,s_4\}}$
$\mathbf{G}_{\{1,s_5\}} = \mathbf{G}_{\{1,s_4\}} = \mathbf{G}_{\{1,s_6\}}$	$\mathbf{G}_{\{2,s_5\}} = \mathbf{G}_{\{1,s_5\}} = \mathbf{G}_{\{2,s_6\}}$
$\mathbf{G}_{\{1,s_7\}} = \mathbf{G}_{\{1,s_6\}} = \mathbf{G}_{\{1,s_8\}}$	$\mathbf{G}_{\{2,s_7\}} = \mathbf{G}_{\{1,s_7\}} = \mathbf{G}_{\{2,s_8\}}$
$\mathbf{G}_{\{1,s_9\}} = \mathbf{G}_{\{1,s_8\}} = \mathbf{G}_{\{1,s_{10}\}}$	$\mathbf{G}_{\{2,s_9\}} = \mathbf{G}_{\{1,s_9\}} = \mathbf{G}_{\{2,s_{10}\}}$
$\mathbf{G}_{\{1,s_{11}\}} = \mathbf{G}_{\{1,s_9\}} = \mathbf{G}_{\{1,s_{12}\}}$	$\mathbf{G}_{\{2,s_{11}\}} = \mathbf{G}_{\{1,s_{11}\}} = \mathbf{G}_{\{2,s_{12}\}}$
$\mathbf{G}_{\{1,s_{13}\}} = \mathbf{G}_{\{1,s_{11}\}}$	$\mathbf{G}_{\{2,s_{13}\}} = \mathbf{G}_{\{1,s_{13}\}}$

Table C4: Payoff matrices.

Appendix D

Summary of the ISO/IEC 27005 information security risk management standard

The ISO/IEC 27005 is based on the ISO/IEC 31000 standard and is developed for information security risk management. The ISO/IEC 27005 describes the steps (including risk assessment steps) that should be taken to implement an information security management system (ISMS) in an organisation. The ISO/IEC 27005 can be understood to as a canonical information security risk management standard, with a number of other standards being closely aligned. The ISO/IEC 27005 standard does not specify, recommend, or even name any specific risk management method. However, it implies a continual process consisting of a structured sequence of activities. Figure D.1 shows the activities in the defined risk management process of the ISO/IEC 27005 and those activities include [16]

1. Establishing the risk management context, which includes the scope, compliance obligations, approaches/methods to be used, and relevant policies and criteria for risk tolerance;
2. Quantitatively or qualitatively assessing relevant information risks, taking into account the information assets, threats, existing controls, and vulnerabilities to determine the likelihood of incidents or incident scenarios; and evaluating the predicted business consequences (to determine a "level of risk") if incidents or incident scenarios occurred,
3. Treating (i.e. modifying security controls, accept risks, and/or share risk information with third parties) the risks appropriately, using those "levels of risk" to prioritise them,

4. Keeping stakeholders informed throughout the process, and

5. Monitoring and reviewing risks, risk treatments, obligations and criteria on an ongoing basis; and identifying and responding appropriately to significant changes.

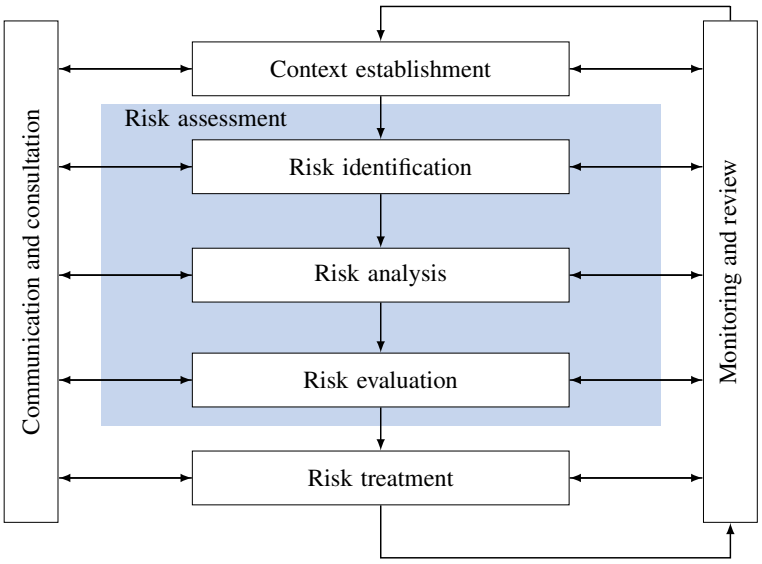


Figure D.1: Risk management process according to [1].

Publications by the author

[1] He, X., Sui, Z., de Meer, H.: Game-theoretic risk assessment in communication networks IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), IEEE, 2016. DOI 10.1016/j.jnca.2012.12.010 (Cited on page 30)

[2] He, X., Niedermeier, M., de Meer, H.: Dynamic key management in wireless sensor networks: A survey. Journal of Network and Computer Applications **36**(2), pp. 611-622 (2013). DOI https://doi.org/10.1016/j.jnca.2012.12.010

[3] He, X., Szalachowski, P., Kutulski, Z., Fotiou, N., Marias, G., Polyzos, C., de Meer, H.: Energy-aware key management in mobile wireless sensor networks. In: Annales UMCS Informatica Lubin-Polonia Sectio AI, pp. 83-96 (2012)

[4] Niedermeier, M., He, X., de Meer, H., Buschmann, C., Hartmann, K., Langmann, B., Koch, M., Fisher, S., Pfisterer, D.: Critical infrastructure surveillance using secure wireless sensor networks. Journal of Sensors and Actuator Networks **4**(4), pp. 336-370 (2015). DOI 10.3390/jsan4040336

[5] Fotiou, N., Marias, G., Polyzos, G., Szalachowsk, P., Kotulski, Z., Niedermeier, M., He, X., de Meer, H.: Towards adaptable security for energy efficiency in wireless sensor networks. In: 28th meeting of the Wireless World Research Forum (WWRF), Wireless World Research Forum (2012)

Bibliography

[1] International Organization for Standardization: BS ISO 31000:2009. Risk mamanagement. Principles and guidelines. Tech. rep., International Organization for Standardization (2009) (Cited on pages xiii, xiv, 16, and 161)

[2] McLaughlin, K., Kang, B.: SCADA intrusion detection system. http://pure.qub.ac.uk/portal/files/126667050/SCADA_IDS_Bilbao.pdf (2015). (Retrieved:04/06/2017) (Cited on page 124)

[3] Sridhar, S., Hahn, A., Govindarasu, M.: Cyber-physical system security for the electric power grid. Proceedings of the IEEE **100**(1), pp. 210–224 (2012). DOI 10.1109/JPROC.2011.2165269 (Cited on page 1)

[4] Liu, R., Vellaithurai, C., Biswas, S.S., Gamage, T., Srivastava, A.K.: Analyzing the cyber-physical impact of cyber events on the power grid. IEEE Transactions on Smart Grid **6**(5), pp. 2444–2453 (2015). DOI 10.1109/TSG.2015.2432013 (Cited on page 2)

[5] Symantec Corporation: Symantec Global Internet Security Threat Report Trends for 2009. Tech. rep., Symantec Corporation (2010) (Cited on page 3)

[6] Symantec Corporation: Internet Security Threat Report 2011 Trends. Tech. rep., Symantec Corporation (2012) (Cited on page 3)

[7] Khan, R., Maynard, P., McLaughlin, K., Laverty, D., Sezer, S.: Threat analysis of BlackEnergy malware for synchrophasor based real-time control and monitoring in smart grid. In: T. Brandstetter, H. Janicke, K. Jones (eds.) 4th International Symposium for ICS & SCADA Cyber Security Research 2016, pp. 53–63 (2016). DOI http://dx.doi.org/10.14236/ewic/ICS2016.7 (Cited on page 3)

[8] Hollis, D.: Cyberwar case study: Gerorgia 2008. Small Wars Journal (2011) (Cited on page 3)

[9] Damsky, I.: Black Energy security report. Tech. rep., ThreatSTOP, Inc. (2016). URL http://www.itbriefcase.net/black-energy-security-report. (Retrieved: 23/05/2017) (Cited on page 3)

[10] CBS Interactive Inc.: Iran confirms Stuxnet worm halted centrifuges. CBS News (2010). (Retrieved: 23/05/2017) (Cited on page 3)

[11] Falliere, N., Murchu, L., Chien, E.: W32.Stuxnet Dossier. Tech. rep., Symantec, Security Response (2011). URL https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. (Retrieved: 19/05/2017) (Cited on page 3)

[12] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2014. Tech. rep., Bundesamt für Sicherheit in der Informationstechnik (2014) (Cited on page 3)

[13] Lee, R., Assante, M., Conway, T.: German steel mill cyber attack. Tech. rep., SANS Industrial Control Systems (2014) (Cited on page 3)

[14] Hutchins, E., Cloppert, M., Amin, R.M.: Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In: 6th Annual International Conference on Information Warfare and Security (2011) (Cited on page 4)

[15] European Union Agency for Network and Information Security: Smart grid security. Annex I. General concepts and dependencies with ICT. Tech. rep., European Union Agency for Network and Information Security (2012) (Cited on pages 6 and 20)

[16] International Organization for Standardization: ISO/IEC27005:2011 Information technology – Security techniques – Information security risk management. Tech. rep., International Organization for Standardization (2011) (Cited on pages 6 and 160)

[17] Ross, R., Katzke, S., Johanson, L.: Minimum security requirements for federal information and information systems. Tech. rep., National Institute of Standards and Technology (2006) (Cited on page 6)

[18] European Union Agency for Network and Information Security: Glossary—ENISA. European Union Agency for Network and Information Security. URL https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary. (Retrieved: 23/05/2017) (Cited on page 6)

[19] International Society of Automation (ISA): ANSI/ISA–99.00.01–2007 Security for Industrial Automation and Control Systems. Part 1: Terminology, Concepts, and Models. Tech. rep., American National Standard (ANSI) (2007) (Cited on page 6)

[20] European Union Agency for Network and Information Security: Smart grid security. Annex II. Security aspects of the smart grid. Tech. rep., European Union Agency for Network and Information Security (2012) (Cited on page 7)

[21] The Smart Grid Interoperability Panel — Cyber Security Working Group (SGIP-CSWG): Guidelines for Smart Grid Cyber Security: Vol.1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements. Tech. rep., National Institute of Standards and Technology (2010) (Cited on pages 7, 17, and 141)

[22] Federal Office for Information Security: Protection profile for the gateway of a smart metering system (Gateway PP). Tech. rep., Federal Office for Information Security (2014) (Cited on pages 17 and 141)

[23] Federal Office for Information Security: Protection profile for the security module of a smart meter gateway (Security Module PP). Tech. rep., Federal Office for Information Security (2013) (Cited on pages 17 and 141)

[24] CEN-CENELEC-ETSI Smart Grid Coordination Group: SG-CG/M490/H_Smart Grid Information Security. Tech. rep., CEN-CENELEC-ETSI Smart Grid Coordination Group (2014) (Cited on page 17)

[25] CEN-CENELEC-ETSI Smart Grid Coordination Group: Report on response to Smart Grid Mandate M/490. Tech. rep., CEN-CENELEC-ETSI Smart Grid Coordination Group (2014) (Cited on page 17)

[26] National Technical Authority for Information Assurance: HMG IA Standard No. 1 Technical Risk Assessment. Tech. rep., National Technical Authority for Information Assurance (2009) (Cited on pages 17 and 55)

[27] The North American Electric Reliability Corporation (NERC): Security guidelines for the electricity sector: Vulnerability and risk assessment, version 1.0. Tech. rep., The North American Electric Reliability Corporation (NERC) (2012) (Cited on page 17)

[28] The Technical Department of ENISA, Section Risk Management: Risk management - Implementation principles and inventories for risk management/risk assessment methods and tools. Tech. rep., European Union Agency for Network and Information Security (ENISA) (2006) (Cited on page 18)

[29] Giannopoulos, G., Filippini, R., Schimmer, M.: Risk assessment methodologies for critical infrastructure protection. Part I: A state of the art. Tech. rep., European Commission, Institute for the Protection and Security of the Citizen (2012). DOI 10.2788/22260 (Cited on page 18)

[30] European Union Agency for Network and Information Security: Appropriate security measures for smart grids: Guidelines to assess the sophistication of security measures implementation. Tech. rep., European Union Agency for Network and Information Security (2012) (Cited on page 18)

[31] Kammerstetter, M., Langer, L., Skopik, F., Kupzog, F., Kastner, W.: Practical risk assessment using a cumulative smart grid model. In: 3rd International Conference on Smart Grids and Green IT Sytems (2014) (Cited on page 18)

[32] National Institute of Standards and Technology: NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments. Tech. rep., National Institute of Standards and Technology (2012). URL `http://dx.doi.org/10.6028/NIST.SP.800-30r1`. (Retrieved:04/06/2017) (Cited on page 20)

[33] König, S., Schauer, S., Rass, S.: A stochastic framework for prediction of malware spreading in heterogeneous networks. In: B. Brumley, J. Röning (eds.) Secure IT Systems. NordSec 2016. Lecture Notes in Computer Science, vol. 10014, pp. 67–81. Springer (2016). DOI 10.1007/978-3-319-47560-8_5 (Cited on page 20)

[34] Hecht, T., Langer, L., Smith, P.: Cybersecurity risk assessment in Smart Grids. In: ComForEN Workshop (2014) (Cited on page 20)

[35] Ruj, S., Pal, A.: Analyzing cascading failures in smart grids under random and targeted attacks. In: 28th International Conference on Advanced Information Networking and Applications. IEEE (2014). DOI 10.1109/AINA.2014.32 (Cited on pages 21, 22, 92, 93, 97, 98, and 103)

[36] Lu, X., Wang, W., Ma, J., Sun, L.: Domino of the smart grid: An empirical study of system behaviors in the interdependent network architecture. In: IEEE International Conference on Smart Grid Communications. IEEE (2013). DOI 10.1109/SmartGridComm.2013.6688026 (Cited on pages 21, 22, 93, and 96)

[37] Huang, Z., Wang, C., Ruj, S., Stojmenovic, M., Nayak, A.: Modeling cascading failures in smart power grid using interdependent complex networks and percolation theory. In: 8th IEEE Conference on Industrial Electronics and Applications, pp. 1023–1028. IEEE (2013). DOI 10.1109/ICIEA.2013.6566517 (Cited on pages 21, 22, 23, and 93)

[38] Huang, Z., Wang, C., Zhu, T., Nayak, A.: Cascading failures in smart grid: Joint effect of load propagation and interdependence. IEEE Access **3**, pp. 2520– 3536 (2015). DOI 10.1109/ACCESS.2015.2506503 (Cited on pages 22, 23, 93, 96, 97, 98, 105, and 115)

[39] Parandeheibi, M., Modiano, E., Hay, D.: Mitigating cascading failures in interdependent power grids and communication networks. In: IEEE International Conference on Smart Grid Communications (SmartGridComm). IEEE (2015). DOI 10.1109/SmartGridComm.2014.7007653 (Cited on pages 22, 23, 92, and 93)

[40] Rahnamay-Naeini, M., Hayat, M.: On the role of power-grid and communication-system interdependencies on cascading failures. In: IEEE Global Conference on Signal and Information Processing (GlobalSIP). IEEE (2014). DOI 10.1109/GlobalSIP.2013.6736931 (Cited on pages 22 and 23)

[41] Rahnamay-Naeini, M.: Designing cascade-resilient interdependent networks by optimum allocation of interdependencies. In: 2016 International Conference on Computing, Networking and Communications (ICNC). IEEE (2016). DOI 10.1109/ICCNC.2016.7440712 (Cited on pages 22 and 24)

[42] Falahati, B., Fu, Y.: A study on interdependenies of cyber-power networks in smart grid applications. In: IEEE PES Innovative Smart Grid Technologies. IEEE (2012). DOI 10.1109/ISGT.2012.6175593 (Cited on page 21)

[43] Shao, J., Buldrev, S., Havlin, S., Stanley, H.: Cascade of failures in coupled network systems with multiple support-dependence relations. Physical review E **83**(3), pp. 1–9 (2011). DOI https://doi.org/10.1103/PhysRevE.83.036116 (Cited on pages 21, 93, and 95)

[44] J. Gao S. V. Buldyrev, H.S., Havlin, S.: Networks formed from interdependent networks. Nature Physics **8**, pp. 40–48 (2012). DOI 10.1038/nphys2180 (Cited on page 21)

[45] Federal Office for Information Security: IT-Grundschutz-catalogues. Tech. rep., Federal Office for Information Security (2014) (Cited on page 25)

[46] International Organization for Standardization: ISO/IEC27002:2013 Information technology – Security techniques – Code of practice for information security controls. Tech. rep., International Organization for Standardization (2013) (Cited on page 25)

[47] Information Technology Laboratory: National Institute of Standards and Technology: NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems and Organizations. Tech. rep., National Institute of Standards and Technology (2009) (Cited on page 25)

[48] Wynn, J., Whitmore, J., Upton, G., Sprigges, L., Mckinnon, D., McInnes, R., Graubart, R., Clausen, L.: Threat assessment and remediation analysis methedology description. Tech. rep., The MITRE Corporation (2011) (Cited on page 25)

[49] Daley, K., Larson, R., Dawkins, J.: A structural framework for modeling multi-stage network attacks. In: International Conference on Parallel Processing Workshops (ICPP). IEEE (2002). DOI 10.1109/ICPPW.2002.1039705 (Cited on page 26)

[50] Karabey, B., Baykal, N.: Attack tree based information security risk assessment method integrating enterprise objectives with vulnerabilities. The International Arab Journal of Information Technology **10**(3), pp. 297–304 (2013) (Cited on page 26)

[51] Kammüller, F., Nurse, J.R.C., Probst, C.: Attack tree analysis for insider threats on the IoT using Isabelle. In: T. Tryfonas (ed.) Human Aspects of Information Security, Privacy, and Trust. HAS 2016. Lecture Notes in Computer Science, vol. 9750, pp. 234–246. Springer, Cham (2016). DOI 10.1007/978-3-319-39381-0_21 (Cited on page 26)

[52] Ma, Z., Smith, P.: Determining risk from advanced multi-step attacks to critical information infrastructures. In: E. Luiijf, P. Hartel (eds.) Critical Information Infrastructures Security. CRITIS 2013. Lecture Notes in Computer Science, vol. 8328. Springer, Cham (2013). DOI 10.1007/978-3-319-03964-0_13 (Cited on pages 27 and 31)

[53] Kordy, B., Mauw, S., Radomirović, S., Schweitzer, P.: Foundations of attack-defense trees. In: P. Degano, S. Etalle, J. Guttman (eds.) Formal Aspects of Security and Trust. FAST 2010. Lecture Notes in Computer Science, vol. 6561. Springer, Berlin, Heidelberg (2010). DOI 10.1007/978-3-642-19751-2_6 (Cited on page 27)

[54] Roy, A., Kim, D., Trivedi, K.: Cyber security analysis using attack countermeasure trees. In: the Sixth Annual Workshop on Cyber Security and Information Intelligence Research. ACM, New York, USA (2010). DOI 10.1145/1852666.1852698 (Cited on page 27)

[55] Qin, X., Lee, W.: Attack plan recognition and prediction using causal networks. In: 20th Annual Computer Security Applications Conference (2005). DOI 10.1109/CSAC.2004.7 (Cited on page 27)

[56] Dalton II, G., Mills, R., Colombi, J., R. A, R.: Analyzing attack trees using generalized stochastic Petri Nets. In: the 2006 IEEE Workshop on Information Assurance (2006). DOI 10.1109/IAW.2006.1652085 (Cited on page 27)

[57] Khaitan, S., Raheja, S.: Finding optimal attack path using attack graphs: A survey. International Journal of Soft Computing and Engineering **1**(3), pp. 2231–2307 (2011) (Cited on page 27)

[58] Viduto, V., Huang, W., Maple, C.: Toward optimal multi-objective models of network security: Survey. In: 17th International Conference on Automation and Computing. IEEE, Huddersfield, UK (2011) (Cited on page 27)

[59] Shandilya, V., Simmons, C., Shiva, S.: Use of attack graphs in security systems. Journal of Computer Networks and Communications **2014**(2014), pp. 1–13 (2014). DOI http://dx.doi.org/10.1155/2014/818957 (Cited on page 27)

[60] Lever, K., MacDermott, A., Kifayat, K.: Evaluating interdependencies and cascading failures using distributed attack graph generation methods for critical infrastructure defense. In: International Confernece on Developments of E-Systems Engineering. IEEE (2016). DOI 10.1109/DeSE.2015.34 (Cited on pages 27 and 28)

[61] Wang, L., Liu, A., Jajodia, S.: Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts. Computer Communications **29**(2006), pp. 2917–2933 (2006) (Cited on page 27)

[62] Zhu, Y., Yan, J., Sun, Y., He, H.: Resilience analysis of power grids under the sequential attack. IEEE Transactions on Information Forensics and Security **9**(12), pp. 2340–2354 (2014). DOI 10.1109/TIFS.2014.2363786 (Cited on pages 27 and 28)

[63] Hawrylak, P., Haney, M., Papa, M., Hale, J.: Using hybrid attack graphs to model cyber-physical attacks in the Smart Grid. In: 5th International Symposium on Resilient Control Systems (ISRCS). IEEE (2012). DOI 10.1109/ISRCS.2012.6309311 (Cited on page 28)

[64] Beckers, K., Heisel, M., Krautsevich, L., Martinelli, F., Meis, R., Yautsiukhin, A.: Determining the probability of smart grid attacks by combining attack tree and attack graph analysis. In: J. Cuellar (ed.) Smart Grid Security. SmartGridSec 2014. Lecture Notes in Computer Science, vol. 8448 (2014). DOI 10.1007/978-3-319-10329-7_3 (Cited on page 28)

[65] Ou, X., Govindavajhala, S., Appel, A.: MulVAL: a logic-based network security analyzer. In: 14th Conference on USENIX Security Symposium, vol. 14, pp. 8–8 (2005) (Cited on page 28)

[66] Greiner, R., Hayward, R., Jankowska, M., Molloy, M.: Finding optimal satisficing strategies for and-or trees. Artificial Intelligence **170**(1), pp. 19–58 (2006). DOI 10.1016/j.artint.2005.09.002 (Cited on page 28)

[67] Sarraute, C., Richarte, G., Obes, J.: An algorithm to find optimal attack paths in non-deterministic scenarios. In: 4th ACM Workshop on Security and Artificial Intelligence, pp. 71–80 (2011). DOI 10.1145/2046684.2046695 (Cited on page 28)

[68] Krautsevich, L., Martinelli, F., Yautsiukhin, A.: Towards modelling adaptive attack's behaviour. In: J. Garcia-Alfaro, F. Cuppens, N. Cuppens-Boulahia, A. Miri, N. Tawbi (eds.) Foundations and Practice of Security. FPS 2012. Lecture Notes in Computer Science, vol. 7743, pp. 357–364. Springer, Berlin, Heidelberg (2013). DOI 10.1007/978-3-642-37119-6_23 (Cited on page 28)

[69] Durkota, K., Lisý, V., Bošamský, B., Kiekintveld, C.: Optimal network security hardening using attack graph games. In: 24th International Joint Conference on Artificial Intelligence, pp. 526–532 (2015) (Cited on page 28)

[70] Ismail, Z., Leneutre, J., Bateman, D., Chen, L.: A methodology to apply a game theoretic model of security risks interdependencies between ICT and electric infrastructures. In: Q. Zhu, T. Alpcan, E. Panaousis, M. Tambe, W. Casey (eds.) Decision and Game Theory for Security. GameSec 2016. Lecture Notes in Computer Science, vol. 9996, pp. 159–171. Springer,Cham (2016). DOI 10.1007/978-3-319-47413-7_10 (Cited on pages 28 and 29)

[71] Osborne, M., Rubinstein, A.: A course in game theory. MIT Press (1994) (Cited on pages 28, 35, 39, and 82)

[72] W. Jiang. Z. Tian, H.Z., Song, X.: A stochastic game theoretic approach to attack prediction and optimal active defense strategy decision. In: International Conference on Networking, Sensing and Control (ICNSC), pp. 648–653. IEEE (2008). DOI doi:10.1109/icnsc.2008.4525297 (Cited on pages 29 and 56)

[73] He, W., Xia, C., Wang, H., Zhang, C., Ji, Y.: A game theoretical attack-defense model oriented to network security risk assessment. In: 2008 International Conference on Computer Science and Software Engineering. IEEE (2008). DOI 10.1109/CSSE.2008.1651 (Cited on pages 29, 34, and 110)

[74] Guillarme, N.L., Mouaddib, A.I., Gatepaille, S., Bellenger, A.: Adversarial intention recognition as inverse game-theoretic plan for threat assessment. In: IEEE 28th International Conference on Tools with Artificial Intelligence (2017). DOI 10.1109/ICTAI.2016.0111 (Cited on page 29)

[75] Nguyen, K., Alpcan, T., Başar, T.: Stochastic games for security in networks with interdependent nodes. In: International Conference on Game Theory for Networks. IEEE (2009). DOI 10.1109/GAMENETS.2009.5137463 (Cited on page 30)

[76] Miura-Ko, R.A., Yolken, B., Bambos, N., Mitchell, J.: Security investment games of interdependent organizations. In: 46th Annual Allerton Conference on Communication, Control, and Computing. IEEE (2009). DOI 10.1109/ALLERTON.2008.4797564 (Cited on page 30)

[77] Rass, S., Zhu, Q.: GADAPT: a sequential game-theoretic framework for designing defense-in-depth strategies against advanced persistent threats. In: Q. Zhu, T. Alpcan, E. Panaousis, M. Tambe, W. Casey (eds.) Decision and Game Theory for Security. GameSec 2016. Lecture Notes in Computer Science, vol. 9996, pp. 314–326. Springer, Cham (2016). DOI 10.1007/978-3-319-47413-7_18 (Cited on pages 30 and 33)

[78] Rass, S., König, S., Schauer, S.: Defending against advanced persistent threats using game-theory. PLoS ONE **12**(1), 1–43 (2017). DOI https://doi.org/10.1371/journal.pone.0168675 (Cited on pages 30 and 33)

[79] Kordy, B., Pouly, M., Schweitzer, P.: A probabilistic framework for security scenarios with dependent actions. In: A. Sekerinski (ed.) Integrated Formal Methods. IFM 2014. Lecture Notes in Computer Science, vol. 8739, pp. 256–271 (2014). DOI 10.1007/978-3-319-10181-1_16 (Cited on page 31)

[80] Fielder, A., Li, T., Hankin, C.: Defense-in-depth vs. critical components defense for industrial control systems. In: T. Brandstetter, H. Janicke, K. Jones (eds.) 4th Internation Symposium for ICS & SCADA Cyber Securtiy Research 2016, pp. 1–10 (2016). DOI 10.14236/ewic/ICS2016.1 (Cited on page 31)

[81] Haslum, K., Årnes, A.: Multisensor real-time risk assessment using continuous-time hidden Markov models. In: Y. Wang, Y. Cheung, H. Liu (eds.) Computational Intelligence and Security. CIS 2006. Lecture Notes in Computer Science, vol. 4456, pp. 694–703. Springer, Berlin, Heidelberg (2007). DOI 10.1007/978-3-540-74377-4_72 (Cited on page 31)

[82] Liao, N., Li, F., Song, Y.: Research on real-time network security risk assessment and forecast. In: International Conference on Intelligent Computation Technology and Automation (ICICTA). IEEE (2010). DOI 10.1109/ICICTA.2010.273 (Cited on page 31)

[83] Rass, S., Alshawish, A., Abid, M., Schauer, S., Zhu, Q., de Meer, H.: Physical intrusion games – optimizing surveillance by simulation and game theory. IIEEE Access **5**, pp. 8394–8407 (2017). DOI 10.1109/ACCESS.2017.2693425 (Cited on page 33)

[84] Manshaei, M.H., Zhu, Q., Alpcan, T., Başar, T., Hubaux, J.P.: Game theory meets network security and privacy. Journal of ACM Computing Surveys (CSUR) **45**(3), pp. 25:1–25:39 (2013). DOI 10.1145/2480741.2480742 (Cited on pages 34 and 56)

[85] Kodialam, M., Lakshman, T.: Detecting network intrusions via sampling: A game theoretic approach. In: Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies, pp. 1880–1889 (2003) (Cited on page 34)

[86] Lye, K.W., Wing, J.: Game strategies in network security. International Journal of Information Security **4**(1-2), pp. 71–86 (2005). DOI 10.1007/s10207-004-0060-x (Cited on pages 34, 55, 56, and 136)

[87] Hewett, R., Rudrapattana, S., Kijsanayothin, P.: Cyber-security analysis of smart grid SCADA systems with game models. In: 9th Annual Cyber and Information Security Research Conference, pp. 109–112. ACM (2014). DOI 10.1145/2602087.2602089 (Cited on page 34)

[88] Ryutov, T., Orosz, M., Blythe, J., von Winterfeldt, D.: A game theoretic framework for modeling adversarial cyber security game among attackers, defenders, and users. In: S. Foresti (ed.) Security and Trust Management. Lecture Notes in Computer Science, vol. 9331, pp. 274–282. Springer, Cham (2015). DOI 10.1007/978-3-319-24858-5_18 (Cited on page 35)

[89] Hamilton, S., Miller, W., Ott, A., Saydjari, O.: Challenges in applying game theory to the domain of information warfare. In: 4th Information Survivability Workshop (2002) (Cited on page 35)

[90] Hamilton, S., Miller, W., Ott, A., Saydjari, O.: The role of game theory in information warfare. In: 4th Information Survivability Workshop (2002) (Cited on page 35)

[91] Matsumoto, A., Szidarovszky, F.: Game theory and its applications. Springer (2016) (Cited on page 35)

[92] Fudenberg, D., Tirole, J.: Game Theory, 1st edn. The MIT Press (1991) (Cited on pages 37, 39, 82, and 135)

[93] Owen, G.: Game Theory, 3 edn. Emerald Group Publishing Limited (2001) (Cited on pages 37, 39, and 43)

[94] Veeravalli, V., Başar, T., Poor, H.: Minimax robust decentralized detection. IEEE Transactions on Information Theory **40**(1), pp. 35–40 (1994). DOI 10.1109/18.272453 (Cited on page 37)

[95] Mckelvey, R., McLennan, A., Turocy, T.: Gambit: software tools for game theory, Version 14.1.0. http://www.gambit-project.org (2014). (Retrieved:04/06/2017) (Cited on pages 38, 39, 41, and 85)

[96] Nash, J.: Non-cooperative games. Ph.D. thesis, Princeton University (1950) (Cited on pages 39 and 80)

[97] Shapley, S.: Stochastic games. Proceedings of the National Academy of Sciences of the United States of America **39**(10), pp. 1095–1100 (1953). DOI 10.1073/pnas.39.10.1095 (Cited on pages 41, 46, and 70)

[98] Filar, J., Vrieze, K.: Competitive Markov Decision Processes. Springer New York (1997). DOI 10.1007/978-1-4612-4054-9 (Cited on pages 41 and 81)

[99] Harsanyi, J.: Games with incomplete information played by "Bayesian" players, I-III. part II. Bayesian Equilibrium Points. Management Science **14**(5), pp. 320–334 (1968). DOI https://doi.org/10.1287/mnsc.14.5.320. URL `http://www.jstor.org/stable/2628673`. (Retrieved:23/05/2017) (Cited on page 44)

[100] Rajbhandari, L., Snekkennes, E.: Mapping between classical risk management and game theoretical approaches. In: Communications and Multimedia Security. CMS 2011. Lecture Notes in Computer Science, vol. 7025, pp. 147–154 (2011). DOI 10.1007/978-3-642-24712-5_12 (Cited on page 50)

[101] Mattioli, R., Levy-Bencheton, C.: Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks. Tech. rep., European Union Agency for Network and Information Security (2015) (Cited on pages 53 and 108)

[102] European Union Agency for Network and Information Security: ENISA smart grid security recommendations. Tech. rep., European Union Agency for Network and Information Security (2012) (Cited on page 55)

[103] Liang, X., Xiao, Y.: Game theory for network security. IEEE Communications Survey & Tutorials **15**(1), pp. 472–486 (2013). DOI 10.1109/SURV.2012.062612.00056 (Cited on page 56)

[104] Chen, L., Leneutre, J.: Fight jamming with jamming — a game theoretic analysis of jamming attack in wireless networks and defense strategy. Journal Computer Networks: The International Journal of Computer and Telecommunications Networking **55**(9), pp. 2259–2270 (2011). DOI https://doi.org/10.1016/j.comnet.2011.03.006 (Cited on page 56)

[105] Hamman, S., Hopkinson, K.M., McCarty, L.: Cyber-Physcial Systems: Foundations, Principles and Applications, chap. Applying Behavioral game theory to cyber-physical systems protection planning, pp. 251–264. Elservier (2017). DOI 10.1016/B978-0-12-803801-7.00017-1 (Cited on page 56)

[106] Ouyang, Y.: On the interaction of information and decision in dynamic network systems. Ph.D. thesis, University of Michigan (2016) (Cited on pages 56, 74, 76, and 136)

[107] Jones, M.: Asymmetric information games and cyber security. Ph.D. thesis, Georgia Institute of Technology (2013) (Cited on page 56)

[108] Vasal, D.: Dynamic decision problems with cooperative and strategic agents and asymmetric information. Ph.D. thesis, University of Michigan (2016) (Cited on pages 56, 74, and 82)

[109] National Cybersecurity and Communications Integration Center: ICS-CERT Year in Review: Industrial control systems cyber emergency response team. https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2014_Final.pdf (2014). (Retrieved:23/05/2017) (Cited on pages 57 and 59)

[110] McLaughlin, K., Friedberg, I., Kang, B., Maynard, P., Sezer, S., McWilliams, G.: Smart Grid Security: Innovative solutions for a modernized grid, chap. Secure communications in smart grid: networking and protocols, pp. 113–148. Elsevier Inc. (2015). DOI https://doi.org/10.1016/B978-0-12-802122-4.00005-5 (Cited on pages 57 and 59)

[111] Mission Support Center: Cyber threat and vulnerability analysis of the U.S. electric sector. Tech. rep., Idaho National Laboratory (2016) (Cited on page 58)

[112] Assante, M., Lee, R.: The industrial Control System Cyber Kill Chain. Tech. rep., SANS Institute InfoSec Reading Room (2015) (Cited on page 58)

[113] Higgins, K.: Researchers out default passwords packaged with ICS/SCADA wares. www.darkreading.com (2016). URL `http://www.darkreading.com/endpoint/researchers-out-default-passwords-packaged-with-ics-scada-wares/d/d-id/1323755`. (Retrieved:23/05/2017) (Cited on page 58)

[114] Harp, D., Gregory-Brown, B.: SANS 2016 State of ICS Security Survey. Tech. rep., SANS Institute InforSec Reading Room (2016) (Cited on page 59)

[115] Deighton, D.: Information security glossary. Tech. rep., Univerisity of Birmingham (2012) (Cited on page 61)

[116] Ritchey, R., Ammann, P.: Using model checking to analyze network vulnerabilities. In: IEEE Symposium on Security and Privacy. IEEE (2002). DOI 10.1109/SECPRI.2000.848453 (Cited on page 61)

[117] Balzarotti, D., Monga, M., Sicari, S.: Assessing the risk of using vulnerable components. In: D. Gollmann, F. Massacci, A. Yautsiukhin (eds.) Quality of Protection. Advances in Information Security, vol. 23. Springer (2006). DOI 10.1007/978-0-387-36584-8_6 (Cited on page 61)

[118] Pauna, A., Moulinos, K.: Window of exposure ⋯ a real problem for SCADA systems? Tech. rep., European Union Agency for Network and Information Security (2013) (Cited on page 64)

[119] Sallhammar, K., Knapskog, S.: Using game theory in stochastic models for quantifying security. In: the 9th Nordic Workshop on Secure IT-systems (2004) (Cited on page 66)

[120] Melolidakis, C.: Stochastic games and related topics, chap. Stochastic games with lack of information on one side and positive stop probabilities, pp. 113–126. Springer Netherlands (1991) (Cited on pages 68, 70, 71, 72, 74, 77, and 80)

[121] Kuhn, H.: Extensive games and the problem of information. Annals of Mathematics Studies **28**(28), pp. 193–216 (1953) (Cited on page 69)

[122] Melolidakis, C.: On stochastic games with lack of information on one side. International Journal of Game Theory **18**(1), pp. 1–29 (1989). DOI 10.1007/BF01248492 (Cited on pages 71, 76, 79, and 80)

[123] Feinberg, E.A., Shwartz, A. (eds.): Handbook of Markov Decision Processes: Methods and Applications. Springer US (2002) (Cited on page 80)

[124] Basu, S.: Incomplete information and asymmetric information. Zagreb International Review of Economics & Business **4**(2), pp. 23–48 (2001) (Cited on page 82)

[125] Nayyar, A., Gupta, A., Langbort, C., Baar, T.: Common information based Markov perfect equilibria for stochastic games with asymmetric information: finite games. IEEE Transactions on Automatic Control **59**(3), pp. 555–570 (2014). DOI 10.1109/TAC.2013.2283743 (Cited on page 82)

[126] Vasal, D., Anastopoulos, A.: A systematic process for evaluating structured perfect Bayesian equilibria in dynamic games with asymmetric information. In: American Control Conference (ACC). Boston, MA, USA (2016). DOI 10.1109/ACC.2016.7525439 (Cited on page 82)

[127] Ouyang, Y., Tavafoghi, H., Teneketzis, D.: Dynamic games with asymmetric information: common information based perfect Bayesian equilibria and sequential decomposition. IEEE Transactions on Automatic Control **62**(1), pp. 222–237 (2017). DOI 10.1109/TAC.2016.2544936 (Cited on page 82)

[128] Ouyang, Y., Tavafoghi, H., Teneketzis, D.: Dynamic oligopoly games with private Markovian dynamics. In: 54th Annual Conference on Decision and Control (CDC). IEEE (2016). DOI 10.1109/CDC.2015.7403139 (Cited on page 82)

[129] Rothblum, U.: Game Theory and Related Topics, chap. Solving stopping stochastic games by maximizing a linear function subject to quadratic constraints, pp. 103–105. North-Holland, Amsterdam (1979) (Cited on page 82)

[130] Filar, J., Schultz, T., Thuijsman, F., Vrieze, O.: Nonlinear programming and stationary equilibria in stochastic games. Mathematical Programming **50**(1), pp. 227 – 237 (1991). DOI 10.1007/BF01594936 (Cited on page 82)

[131] Barron, E.: Game Theory: An Introduction. John Wiley & Sons, Inc. (2007). DOI 10.1002/9781118032398 (Cited on page 82)

[132] Buldrev, S., Parshani, R., Paul, G., Stanley, H., Havlin, S.: Catastrophic cascade of failures in interdependent networks. Nature **464**(7291), pp. 1025–1028 (2010). DOI 10.1038/nature08932 (Cited on pages 92, 93, and 96)

[133] Rinaldi, S., Peerenboom, J., Kelly, T.: Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems **21**(6), pp. 11–25 (2001). DOI 10.1109/37.969131 (Cited on page 92)

[134] Motter, A., Lai, Y.C.: Cascade-based attacks on complex networks. Physical Review E **66**, pp. 1– 4 (2002) (Cited on pages 92, 93, and 98)

[135] Crucitti, P., Latora, V., Marchiori, M.: Model for cascading failures in complex networks. Physical review E **69**, pp. 1–4 (2004). DOI 10.1103/PhysRevE.69.045104 (Cited on page 92)

[136] Bourne, V.: Critical infrastructure readiness report: Holding the line against cyberthreats. Tech. rep., Intel Security ,The Aspen Institute (2015) (Cited on page 92)

[137] Yu, X., Singh, C.: Power system reliability analysis considering protection failures. In: IEEE Power Engineering Society Summer Meeting. IEEE, Chicago, IL, USA, USA (2002). DOI 10.1109/PESS.2002.1043514 (Cited on page 92)

[138] Kjølle, G., Utne, I., Gjerde, O.: Risk analysis of critical infractructures emphasizing electricity supply and interdependencies. Reliability Engineering & System Safety **105**, pp. 80–89 (2012). DOI https://doi.org/10.1016/j.ress.2012.02.006 (Cited on page 92)

[139] Ouyang, M.: Review on modeling and simulation of interdependent critical infrastructure systems. Reliability Engineeing & System Security **121**, pp. 43–60 (2014). DOI https://doi.org/10.1016/j.ress.2013.06.040 (Cited on page 92)

[140] Newman, M.E.J.: Assortative mixing in networks. Physical Review Letters **89**(20), pp. 1–4 (2002) (Cited on pages 92, 93, 96, 97, and 101)

[141] Zio, E., Sansavini, G.: Modeling interdependent network systems for identifying cascade-safe operating margins. IEEE Transactions on Reliability **60**(1), pp. 94–101 (2011). DOI 10.1109/TR.2010.2104211 (Cited on page 93)

[142] Huang, X., Gao, J., Buldrev, S., Havlin, S., Stanley, H.: Robustness of interdependent networks under targeted attack. Physical Review E **83**, pp. 1–4 (2011). DOI :10.1103/PhysRevE.83.065101 (Cited on page 93)

[143] Moreno, Y., Gómez, J., Pacheco, A.: Instability of scale-free networks under node-breaking avalanches. Europhysics Letters **58**(4), pp. 630–636 (2002) (Cited on pages 93 and 104)

[144] Jin, W., Song, P., Liu, G., Stanley, H.: The cascading vulnerability of the directed and weighted network. Physica A: Statistical Mechanics and its Applications **427**, pp. 302–325 (2015). URL `https://doi.org/10.1016/j.physa.2015.02.035` (Cited on pages 95 and 104)

[145] Yağan, Q., Qian, D., Zhang, J., Cochran, D.: Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness. IEEE Transactions on Parallel and Distributed Systems **23**(9), pp. 1708–1721 (2012). DOI 10.1109/TPDS.2012.62 (Cited on page 96)

[146] Albert, R., Barabási, A.L.: Statistical mechanics of complex networks. Reviews of modern physics **74**(1), 47–97 (2002). DOI https://doi.org/10.1103/RevModPhys.74.47 (Cited on page 97)

[147] Pagani, G., Aiello, M.: The power grid as a complex network: A survey. Physica A: Statistical Mechanics and its Applications **392**(11), pp. 2688–2700 (2013). DOI https://doi.org/10.1016/j.physa.2013.01.023 (Cited on pages 97 and 98)

[148] Yang, N., Liu, W., Guo, W.: Study on scale-free characteristic on propagation of cascading failures in power grid. In: IEEE Energytech. Cleveland, OH, USA (2011). DOI 10.1109/EnergyTech.2011.5948519 (Cited on page 97)

[149] Sturaro, A., S.Silvestri, Conti, M., Das, S.: Towards a realistic model for failure propagation in interdependent networks. In: IEEE International Conference on Computing, Networking and Communications (ICNC). IEEE, Kauai, HI, USA (2016). DOI 10.1109/ICCNC.2016.7440711 (Cited on pages 97 and 111)

[150] Newman, M.E.J.: Scientific collaboration networks. II. Shortest paths, weighted networks, and centrality. Physical Review E **64**(1) (2001). DOI https://doi.org/10.1103/PhysRevE.64.016132 (Cited on page 98)

[151] Holme, P., Kim, H., Yoon, C.N., Han, S.K.: Attack vulnerability of complex networks. Physical Review E **65** (2002). DOI https://doi.org/10.1103/PhysRevE.65.056109. Holme2002 (Cited on page 98)

[152] Newman, M.: Networks: An introduction. Oxford University Press (2010) (Cited on pages 98 and 101)

[153] Ercsey-Ravasz, M., Toroczkai, Z.: Centrality scaling in large networks. Physical Review Letters **105**(3), 1–4 (2010). DOI https://doi.org/10.1103/PhysRevLett.105.038701 (Cited on page 99)

[154] Brandes, U.: A faster algorithm for betweenness centrality. The Journal of Mathematical Sociology **25**(2), pp. 163–177 (2001) (Cited on page 99)

[155] Piraveenan, M., Prokopenko, M., Hossain, L.: Percolation centrality: Quantifying graph-theoretic impact of nodes during percolation in networks. PLoS ONE **8**(1), 1–14 (2013). DOI 10.1371/journal.pone.0053095 (Cited on page 99)

[156] Wilf, H.: Generatingfunctionology, 3 edn. A K Peters/CRC Press (2005) (Cited on page 100)

[157] Havlin, S., Stanley, H.E., Bashan, A., Gao, J., Kenett, D.: Percolation of interdependent network of networks. Chaos, Solitons & Fractals **72**, pp. 4–19 (2015). DOI https://doi.org/10.1016/j.chaos.2014.09.006 (Cited on page 103)

[158] Shao, J., Buldyrev, S., Braunstein, L., Havlin, S., Stanley, H.E.: Structure of shells in complex networks. Physical Review E **80**(3), pp. 1–13 (2009). DOI 10.1103/PhysRevE.80.036105 (Cited on page 103)

[159] Watts, D.: A simple model of global ccascades on random networks. Proceedings of the National Academy of Sciences of the United States of America **99**(9), pp. 5766– 5771 (2002). DOI 10.1073/pnas.082090499 (Cited on page 104)

[160] Venkatasubramanian, M.V.: Analyzing blackout events: Experience from the major western blackouts in 1996. Tech. rep., Power Systems Engineering Research Center (PSERC) (2003). (Retrieved:04/06/2017) (Cited on page 104)

[161] Lee, R., Assante, M., Conway, T.: Analysis of the cyber aattack on the Ukrainian power grid. Tech. rep., Electricity Information Sharing and Analysis Center (2016) (Cited on page 108)

[162] Rudrapattana, S.: Cyber-security analysis in smart grid SCADA systems: a game theoretic approach. Master's thesis, Texas Tech University (2013) (Cited on page 110)

[163] Hagberg, A.A., Schult, D.A., Swart, P.: Exploring network structure, dynamics, and function using NetworkX. In: G. Varoquaux, T. Vaught, J. Millman (eds.) the 7th Python in Science Conference, pp. 11–15 (2008) (Cited on page 111)

[164] Barabási, A., Albert, R.: Emergence of scaling in random networrks. Science **286**(5439), pp. 509–512 (1999). DOI 10.1126/science.286.5439.509 (Cited on page 111)

[165] Wang, Z., Scaglione, A., Thomas, R.J.: Generating statistically correct random topologies for testing smart grid communication and control networks. IEEE Transactions of Smart Grid **1**(1), pp. 28–39 (2010) (Cited on page 111)

[166] Eslami, A., Huang, C., Zhang, J., Cui, S.: Cascading failures in load-dependent finite-size random geometric networks. IEEE Transactions on Network Science and Engineering **3**(4), pp. 183–196 (2016). DOI 10.1109/TNSE.2016.2608341 (Cited on page 115)

[167] Kang, B., Maynard, P., McLaughlin, K., Sezer, S., Seittl, C., Kupzog, F., Strasser, T.: Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations.

In: IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA). IEEE (2015). DOI 10.1109/ETFA.2015.7301457 (Cited on pages 123 and 125)

[168] Budka, K.C., Deshpande, J., Thottan, M.: Communication networks for smart grids: Making smart grid real. Springer (2014). DOI 10.1007/978-1-4471-6302-2 (Cited on page 123)

[169] Brundlinger, R., Strasser, T., Lauss, G., Hoke, A., Charkraborty, S., Martin, G., Kroposki, B., Johnson, J., de Jong, E.: Lab tests: verifying that smart grid power converters are truly smart. IEEE Power and Energy Magazine **13**(2), pp. 30–42 (2015). DOI 10.1109/MPE.2014.2379935 (Cited on page 123)

[170] Bernardin, L., Chin, P., DeMarco, P., Geddes, K., Hare, D., Heal, K., Labahn, G., May, J., McCarron, J., Monagan, M., Vorkoetter, S.: Maple Programming Guide. Maplesoft, Waterloo, ON Canada (2005) (Cited on page 132)

[171] Yang, S., Holsopple, J., Sudit, M.: Evaluating threat assessment for multi-stage cyber attacks. In: IEEE Military Communications Conference. IEEE, Washington, DC, USA (2006). DOI 10.1109/MILCOM.2006.302216 (Cited on pages 136 and 137)

[172] Tippenhauser, N., Temple, W., Vu, A., Chen, B., Nicol, D., Kalbarczyk, Z., Sanders, W.: Automatic generation of security argument graphs. In: 20th Pacific Rim International Symposium on Dependable Computing (PRDC). IEEE (2014). DOI 10.1109/PRDC.2014.13 (Cited on page 144)

[173] Jauhar, S., Chen, B., Temple, W., Dong, X., Kalbarczyk, Z., Sanders, W., Nicol, D.: Model-based cybersecurity assessment with NESCOR smart grid failure scenarios. In: IEEE 21st Pacific Rim International Symposium on Dependable Computing, pp. 319–324 (2015). DOI 10.1109/PRDC.2015.37 (Cited on page 144)

[174] Megiddo, N.: On repeated games with incomplete information played by non-Bayesian players. International Journal of Game Theory **9**(3), pp. 157–167 (1980). DOI 10.1007/BF01781370 (Cited on page 145)

[175] Monderer, D., Tennenholtz, M.: Dynamic non-Bayesian decision making. Journal of Artificial Intelligence Research **7**(1997), pp. 231–248 (1997) (Cited on page 145)