December 2021

An Insurance Framework for Cyber-Physical Power Systems Considering Integrated Cybersecurity-Reliability Assessment

Pikkin Lau
University of Wisconsin-Milwaukee

AN INSURANCE FRAMEWORK FOR CYBER-PHYSICAL POWER SYSTEMS CONSIDERING INTEGRATED CYBERSECURITY-RELIABILITY ASSESSMENT

by

Pikkin Lau

A Dissertation Submitted in

Partial Fulfillment of the

Requirements for the Degree of

Doctor of Philosophy

in Engineering

at

The University of Wisconsin-Milwaukee

December 2021

ABSTRACT

AN INSURANCE FRAMEWORK FOR CYBER-PHYSICAL
POWER SYSTEMS CONSIDERING INTEGRATED
CYBERSECURITY-RELIABILITY ASSESSMENT

by

Pikkin Lau

The University of Wisconsin-Milwaukee, 2021
Under the Supervision of Professor Lingfeng Wang

Due to the development of cyber-physical systems for modernizing power grids, vulnerability assessment has become an emerging focus in power system security studies. With the increasing application of cyber-enabled technologies in power systems, modern power system is prevalently exposed to a wide gamut of cybersecurity threats. In this dissertation, the power supply reliability is evaluated considering the strategic allocation of defense resources and smart technologies. The optimal mixed strategies are formulated by the Stackelberg Security Game to allocate the defense resources on multiple targets subject to cyberattacks. Smart monitoring with preventive and corrective measures is able to boost the substation availability against cyberattacks. A stochastic job-assignment strategy is also deployed to distribute the control and monitoring tasks to multiple threads to reduce the execution failures. In the case studies, it can be observed the intrusion tolerance capability of the Supervisory Control and Data Acquisition system provides buffered residence time before the substation failure to enhance the network robustness against cyberattacks.

Finally, this dissertation proposes novel actuarial insurance principle designs, for either a third-party insurer or a mutual insurance platform, as financial instruments to hedge against individual cyber risks of the transmission operators' via reliability implication anal-

ysis. The indemnity which covers the cyberattack-induced losses complies with the budget sufficiency. The proposed insurance premium principles tested via case studies demonstrate its mechanism for investments on enhancing the power grid cybersecurity.

To Prof. Lingfeng Wang

For offering me the life-changing opportunity to complete my Ph.D.

When I lost all hope in academic life

TABLE OF CONTENTS

LIST OF FIGURES

Figure Page

LIST OF TABLES

Table Page

LIST OF ABBREVIATIONS

ICTs	Information and Communication Technologies
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
ERO	Electric Reliability Organization
CPSs	Cyber-Physical Systems
SCADA	Supervisory Control And Data Acquisition
HMI	Human-Machine Interface
WAP	Wireless Access Point
RTU	Remote Terminal Units
EMU	Energy Management Units
WAN	Wide Area Network
LAN	Local Area Network
DMs	Defense Mechanisms
TTC	Time-To-Compromise
SCT	Substation Compromise Time
TG	Transmission Grid
LAN	Local Area Network

BN	Bayesian Network
SMP	Semi-Markov Process
SMC	Semi-Markov Chain
ENM	Epidemic Network Model
BTTC	Bayesian Time-To-Compromise
MTTC	Mean-Time-To-Compromise
MTTR	Mean-Time-To-Repair
CVSS	Common Vulnerability Scoring System
BCT	Beta Compromise Time
SSG	Stackelberg Security Game
SSE	Strong Stackelberg Equilibrium
ORIGAMI	Optimizing Resources In GAmes using Maximal Indifference
DRA	Defense Resource Allocation
MILP	Mixed Integer Linear Programming
(T)VaR	(Tail)Value-at-Risk
TCE	Tail Conditional Expectation
ERW	Expected Reliability Worth
DFS	Depth-First Search

SMC	Sequential Monte Carlo
ELC	Expected Load Curtailment
EFC	Expected Faulty-Bus Count
L/HDC	Low/High Defense Coverage
SDs	Standard Deviations
CoVs	Coefficients of Variation
RLC	Risk-Loading Coefficient
OPF	Optimal Power Flow
MCS	Monte Carlo Simulation

LIST OF NOTATIONS

V	Set of the vulnerabilities
T_b	Bayesian Time-To-Compromise
t_β	Beta Compromise Time
t^*	Compromise Time
$\{G, A, C, S\}$	Gate, Authentication, Countermeasure, Substation
$\{t_1, t_2, t_3\}$	Mean times of the BCT processes
$\{P_1, P_2, P_3\}$	Probabilities of the BCT processes
v_h	A known or zero-day vulnerability
c_h	Successful vulnerability exploitation of v_h
$p(v_h)$	Probability of exploiting v_h
$p(v_h \wedge c_h)$	Probability that v_h is exploited by c_h
$p(c_h \| v_h)$	Conditional probability of successfully exploiting v_h
$p(c_h)$	Total probability of successfully exploiting v_h
$\mathbf{1}_{\{\cdot\}}$	True/false binary indicator of a conditional statement
$U(\cdot)$	Uniform distribution
$N(\cdot)$	Normal distribution
$\Phi(\cdot)$	Cumulative Density Function of $N(\cdot)$

s	Skill factor of the intruder
$\|v\|$	Number of known vulnerabilities of the component
σ	Total number of vulnerabilities
$m(s)$	Number of available exploits
$f(s)$	Usable exploits
$E(s, \|v\|)$	Number of estimated tries
$p(DM_w)$	Strength of the DMs
L_j	An attack leaf
$p(L_j)$	Probability that L_j is active
$p(L_j \wedge e_{DM})$	Probability that a set of DMs are attacked by L_j
τ_x	Target substation x
γ_x	Substation impact index of τ_x
α, β	Intruder and Defender
$\begin{cases} U^c_{\alpha,\tau_x}, U^u_{\alpha,\tau_x} \\ U^c_{\beta,\tau_x}, U^u_{\beta,\tau_x} \end{cases}$	Covered/uncovered payoffs of α,β
$\mathcal{C}$	Defense coverage sequence
$p_{DC}(\tau_x)$	Defense coverage of τ_x

r	Correlation coefficient of the sampling copula
λ_x	Random sampling applied τ_x
$T_{b,x}$	BTTC of τ_x
$\boldsymbol{M} = \{M_q\}$	Defense resource budget vector
$\boldsymbol{\mathcal{L}}_q$	Monetary loss of TG q
$\pi(\boldsymbol{\mathcal{L}}_q)$	Premium of TG q
φ_q	Occurrence probability of the loss event
$\delta_{q,\varsigma}$	Probability TG q out of ς submits the claim
Π_q	Claim of TG q
Γ_q	Indemnity of TG q
$\mathbb{C}_q$	Commitment of TG q
$\rho(\boldsymbol{\mathcal{L}}_q)$	RLC of TG q
$\underline{\Omega} = \{\Omega\}$	Load loss event set
K_Ω	Probability density kernel of loss event Ω
D_Ω	Duration of loss event Ω
$W(D_\Omega)$	Cost mapping function of loss event Ω
$\boldsymbol{K_x}$	Load curtailment vector (MW)
ν	Time step of the reliability assessment

$\boldsymbol{B}$	Substation susceptance vector
$\boldsymbol{\theta}$	Vector of the substation voltage angles (rad)
$\boldsymbol{G}$	Vector of the available generation (MW)
$\boldsymbol{G_{cap}}$	Generation capacity vector (MW)
$\boldsymbol{D_{cap}}$	Load capacity vector (MW)
$\boldsymbol{F}$	Transmission power flow vector (MW)
$\boldsymbol{F_{cap}}$	Thermal limit vector of the transmission lines (MW)
$EN(\boldsymbol{\tau_x})$	Enabling function of the substations
$\mathbf{1}_{\{\cdot\}}$	True/false binary indicator of a conditional statement
$*$	Element-wise product operator
t_s	Vulnerability sojourn time
J_1, J_2, J_3	Number of assigned job threads
Y_1, Y_2	Duration of the task operation
$\mathbb{U}$	Residual time of the job thread executing the task
λ	Failure rate of the substation cyber-physical elements
μ	Repair rate of the substation cyber-physical elements
(λ_b, μ_b)	Baseline failure rate and repair rate of the CPS element
(λ_i, μ_i)	State failure rate and repair rate of smart monitoring

(λ_c, μ_c)	Composite failure rate and repair rate of smart monitoring
ζ	Set of adjacent nodes of a given graphical node
$\overrightarrow{T}_{rec}$	Epidemic recovery time vector
$\overrightarrow{T}_{epi}$	Epidemic infection time vector
T_{rec}	Epidemic recovery time of the substation
T_{epi}	Epidemic infection time of the substation
$\hat{T}_c$	Sampled substation compromise time
$\hat{T}_r$	Sampled substation repair time
$\mathbb{B}_\zeta$	Binomial variate of the adjacent node infectivity
ε	Basic reproduction number
c	Graphical edge coupling number
Z_{epi}	External epidemic infection time
R_{epi}	External epidemic recovery time
p_{atk}	Probability of cyberattack infection
$\mathbb{P}_v$	Partially correlated uniform variate of state sampling
$\mathbf{1}_{\{\cdot\}}$	Binary indicator function of whether the condition is met
S_x	Set of substations
$EN(\cdot)$	Enabling function of the substation state sequences

$\mathbf{U}$	Universal set including all participating TGs
S	Subset of the selected TGs
$\varepsilon_{q,k}$	Shapley cost of the TG q among k TGs in S
δ_q	Cumulative distribution of the loss smaller than $VaR_{\varpi}(\mathcal{L}_q)$
y	Number of TGs in the universal set
k	Number of TGs which submit their claims
$\Gamma^*_{q,k}$	Base indemnity of TG q among k TGs in S
$\psi(\cdot)$	Scaling function of Γ_q
$\Gamma^{\psi}_{q,k}$	Indemnity of TG q among k TGs in S

ACKNOWLEDGMENTS

My deepest appreciation goes to my academic advisor and committee chair Prof. Lingfeng Wang. He offered me the opportunity to continue my graduate studies at my most desperate moment. He is always responsive and willing to explain in details when I seek his guidance. He secured the necessary funding for me to concentrate on research. He identified my talent and has faith in me despite my repetitive failed attempts. Because of his great support which led to my solid academic outcomes, I consider the time I spent at University of Wisconsin-Milwaukee the most fruitful period in my academic career.

Prof. Wei Wei serves as my academic co-advisor in cyber-insurance designs. He went the extra mile to ensure cyber-insurance designs proposed in my publications make actuarial sense. His expertise in actuary was the key success factor of the grant which funded the most part of my PhD career. I thank Prof. Lingfeng Wang, Prof. Wei Wei, Prof. Zeyun Yu, Prof. Yi Hu, and Prof. Weizhong Wang for their time and valuable suggestions of this dissertation.

I thank all my mentor and colleagues who have been a great support through this work. Dr. Zhaoxi Liu provided essential instruction that led to my journal publications. Mr. Yitong Shen joined Prof. Lingfeng Wang's group at the same time as me. Mr. Shen and I took all of the classes, discussed research and had a good time traveling abroad together. Mr. Yunfan Zhang shared useful information allowing me to survive the qualifying exam. Mr. Youqi Guo's intelligence, and his profound knowledge in machine learning and game theory, are always my great inspiration.

My landlord Mr. Carl Van Hemelryk furnished a spacious attic unit right next to the

campus, while keeping the rent affordable for me. Since my residence is just two blocks away from my office, I saved tons of time in commuting and can travel back home frequently to relax. Mr. Van Hemelryk is an exceptionally hospitable landlord. Whenever a tenant reports any facility issue, he provides quick maintenance. I never feel bored of occasional conversations with him. I will miss the comfortable king size bed and the days renting with him.

Special thanks to U.S. National Science Foundation (Award 1739485) and State of Wisconsin for supporting my PhD studies.

Finally, I am extremely grateful to my dear father and hero Mr. Lau Iok who overcame all the financial stress to bring me up, my beloved late grandmother Ms. Ong Chhun who always prepared delicious food for me, and my mother Ms. Koeh Cheng-Miau who gave me a chance to experience this beautiful world.

CHAPTER 1. INTRODUCTION

1.1 Research Motivations

The looming cybersecurity issue on power grids due to the broad integration of ICTs has attracted extensive attention in recent years [1]. Threats of cyberattacks had come to the publics attention in the past decade. A ransomware incident occurred in 2018 at Atlanta, which affected the core city services and might cost $44.5 million for recovery [2]. A cyber event on the U.S. power grid was reported in 2019. A Denial-of-Service attack disabled the security devices in Utah, Wyoming and California without inducing actual power outage. As a result, Supervisory Control and Data Acquisition systems of electric utilities temporarily lost partial visibility [3]. Nevertheless, successful cyberattacks could lead to serious consequences. The first known cyber event anywhere in the world causing blackout can be traced back to the cyberattack on Ukrainian power grid in 2015. During the cyberattack, the hackers infiltrated through Virtual Private Network and successfully disabled the power supply to the customers of three distribution companies for several hours [4]. According to an annual report from North American Electric Reliability Corporation, the focus of financially motivated cyberattacks has been shifted to cryptojacking as of 2018. Prolonged cryptojacking may result in negative impacts that may trigger a Denial-of-Service condition on the system such as component burnout and exhaustion of the processing power [5].

In response to the increasing cyber vulnerability, NERC has stipulated a series of cyber-security standards [6], and NIST updated the framework for improving critical infrastructure cybersecurity in 2018 [7], respectively. Cybersecurity can be enhanced by more sophisticated defense systems to enable an improved resilience against potential cyberattacks. Attack-resilient Wide-Area Monitoring, Protection, And Control is a security framework constituted by an entire security life cycle from assessing risk to detecting and mitigating attacks to attack resilience [8]. Anomalies in power system applications such as Automatic Generation Control can be identified via the real-time load forecasts. In [9], an offline control is proposed as attack mitigation synthesized by the simulated real-time load and its forecast, successfully maintaining the system frequency during attack at around the nominal frequency. Different from the existing literature, our study reported in this paper focuses on the risk assessment on cybersecurity threats and system vulnerability for the actuarial study.

To de-risk the integration of innovative ICTs in CPSs including electric power grids, much research effort has been dedicated to efficient cyber-vulnerability assessment. Ten et al. [10] integrated the cyber-physical information of substations into evaluating vulnerability of the SCADA systems. DMs for the vulnerabilities have been proposed to reduce the potential losses. Based on the attack cost, the power system vulnerability can be quantified by the security mechanisms [11]. Probabilistic approaches can be applied in the security assessment of cyber-physical systems. For example, attack graph is used as a hierarchical graphic tool for vulnerability assessment combining intrusion scenarios and corresponding DMs. Various attack graphs are proposed to examine the network hardening options, the dependency, and the network security [12]-[14].

Meanwhile, quantitative security metrics have been proposed to measure the impact of

cyberthreats. McQueen et al. [15] proposed TTC modeling based on the data of vulnerability and exploits. Zieger et al. [16] eliminated arbitrary values by modeling the distribution of the attackers proficiency. Given the vulnerability and skill level of an attacker, TTC quantifies various defense mechanisms against the long-term impact of risks and cyberattacks by predicting the time required to compromise a system. Zhang et al. [17] addressed the attackers aspect in reliability evaluation by assessing the cybersecurity using TTC derived from attack graphs. The k-Zero Day Safety metric estimates the number of unknown vulnerabilities required to compromise the network system [18]. To gauge the capability of CPS to recover from multiple system contingencies, resilience metrics were developed to integrate graph theory with the vulnerability scoring system in power grids [19].

Various algorithms and tools have been developed to reduce the system vulnerability against cyberattacks. The impacts of cyberattacks can be evaluated by carrying out the transient vulnerability assessment on bulk power systems [20]. Risk management tools like insurance, by quantifying the possibility of loss or damage, are applicable to address the residual cyber risk. Insurance transfers the risk from a policyholder to an insurer. The cyber-insurance comes into play to protect and maintain financial health of the electric utilities suffering from cyberattacks. The insured utility regularly pays a cyber premium to the insurer to guarantee coverage on the losses induced by cyber risks. In the US alone, the size of the market for cyber-insurance in terms of premiums was 2.0 billion in 2014, with a yearly growth rate at $10 \sim 25\%$ [21]. Through client contract discrimination, a cyber-insurer may improve efficiency of a cyber-insurance market and security of the network [22]. In [23], a two-stage Stackelberg game model is developed to address the security pricing by allocating the equilibrium in cyber-insurance market.

In this dissertation, a Sequential Monte Carlo simulation is performed for the reliability analysis on the losses induced by potential cyberattack intrusions. The intrusion tolerant capability of the respective Transmission Grids is distributed by SSG based on the amount of available defense resources. A cyber-insurance principle is devised to estimate the individual premium of each TG based on the integrated reliability and cyber-vulnerability analysis [24]. In addition, a coalitional cyber-insurance framework is proposed for the modern cyber-physical power grids [25]. To the best knowledge of authors, it is the first time that a coalitional cyber-insurance premium design is tailor-made for the power system networks. In [26], stochastic cybersecurity insurance pricing models for graphical networks was proposed. The proposed cyber epidemic model inspired by [26] is conceived to further estimate the long-term infectious vulnerability risk on the graphical cyber epidemic network model coupled with power systems. Finally, a new mutual cyber insurance model based on the Shapley value is developed for power grids deploying smart technologies as a more economical option with relatively sufficient insolvency mitigation.

1.2 Dissertation Objectives

This dissertation intends to propose feasible cybersecurity insurance designs considering power system reliability and network vulnerabilities of Cyber-Physical Systems. Defense strategies to fortify the substation infrastructure against cyberattacks for the power system operators are explored. Stackelberg Security Game is implemented to enhance the intrusion tolerance capability of the SCADA servers in the substations. Depending on the available defense resources, in the Bayesian Network (BN), the server countermeasures against cy-

berattacks can be further strengthened. In addition, promising smart technologies such as smart monitoring and job assignment may be deployed to boost the substation availability under various epidemic attack scenarios.

The chief contributions of this dissertation are summarized as follows:

- A comprehensive quantitative risk assessment approach that integrates probabilistic and game-theoretic modeling to evaluate the cyberattack impact on the reliability is developed.

- An SSG model is proposed as the optimal stochastic distribution mechanism to allocate defense resources across the target substations in each TG. A Semi-Markov Process model is developed to model the intrusion tolerant capability of the SCADA system. The existent defense resource allocation strategies fall short in exploring the long-term impact of system compromise on the reliability due to cyberattacks. Thus, the proposed defensive strategy is devised to properly address the relationship between security investment and savings in insurance premium.

- A cyber-insurance framework is established for the TGs to estimate the cyber risk and the corresponding premiums for long-term planning. An actuarial insurance principle for a third-party insurer is proposed to estimate the actuarial implication of potential power supply interruptions caused by cybersecurity threats, integrating vulnerability metrics into long-term reliability assessment. The proposed insurance principle effectively addresses the dependence issue of the losses from different TGs by allocating premiums according to TGs individual responsibilities to the riskiness of the insurance portfolio.

- A novel coalitional cybersecurity-insurance framework for power systems is devised. The proposed framework performs reliability analysis accounting for the cyber vulnerability and estimates the premiums of TGs based on reliability worth analysis.

- A new graphic security assessment approach is developed where cyber-vulnerability is estimated by considering all feasible nodal routes from the intruders perspective. It is critical to distribute the security-enhancing budget in each TG judiciously through proper defense resource allocation scheme.

- A coalitional cyber-insurance design is proposed as an alternative or supplement to the conventional insurance administered by third-party insurers. In the proposed coalitional insurance model, TGs serve as both insurers and insureds.

- A novel mutual cyber-insurance framework based on the Shapley value of the cooperative game is devised. Load loss distributions are extracted from the mutual insurance participants to formulate cost values, ultimately obtaining reduced costs in the cooperative game.

- An integrated reliability evaluation model considering substations deploying smart monitoring and job thread assignment technologies is developed aiming to enhance the system robustness against cyberattacks.

- A state-sampling cyber epidemic model is integrated into the Bayesian Network cyber vulnerability model. This integrated model is devised considering the propagation of cyberattacks and network correlation.

1.3 Organization of Dissertation

The rest of this dissertation is organized as follows. In Chapter 2, an overview of the cyber-insurance is provided. Chapter 3 devises a cyber-insurance model considering optimal defense resource allocation. Chapter 4 proposes a coalitional cyber-insurance design considering cyber vulnerability. Chapter 5 introduces a mutual cyber-insurance model for power systems with deployment of smart technologies. Chapter 6 draws concluding remarks and discusses the future work.

CHAPTER 2. OVERVIEW OF CYBER-INSURANCE

2.1 History

With increasingly interconnected distributed systems, security assessment has become challenging due to high penetration of risks. Back in the 90s, cyber-insurance was proposed as a powerful financial instrument to hedge against the uncertainties of hazards. When damaging cyberattacks occur, cyberinsurance policies are in place to recover losses of the insured clients [27]. The early cyberinsurance policies typically covered the professional software and media risks.

The transition from physical space to cyber space took place in mid-2000s. Cyberinsurers providing protection expense coverage started to appear. The public sector's awareness was also growing during the same period. California enacted data breach notification law in 2003 mandating disclosure of system security breach to affected residents, which was later extended to medical and health insurance information in 2008 [28]. Widespread adaptions to similar laws passed in other states motivated cyberinsurers rolling out new policies extending the coverage to information security, public relations, credit monitoring, and customer notification. Until late-2000s, small sub-limits in coverage were imposed on most cyberinsurance policies since the cyberinsurers and reinsurers were hesitant to adopt higher sub-limits with excessive uncertainties involved in new exposures to a wider variety of cyber risks. The ever-evolving nature of the communication technologies created new cyber risks which forced the

cyberinsurers to adapt and devise insurance policies tailored to individual end-user CPSs [29].

2.2 Cyberattack Events

Cyberattacks over the past few years have been shifted from data breach to ransomeware attacks. The data breach is of higher risk to certain sectors holding more personal identifiable information, and vice versa. By contrast, the ransomware cyberattacks have been indiscriminate in the classes of businesses as long as the businesses are sensitive to short-term disruption. Ransomware demanding from six-figure to more than a million dollars could become the norm [30]. Baltimore city fell victim to a ransomware demanding payment to unlock encrypted city files in 2019, where the city refused to pay the ransom and ended up spending $6 million for cyberattack remediation and network hardening [31]. Cyberattacks had drawn increasing attention from the government sector. Ransomware attacks on critical infrastructure included in USA's agenda as a national security priority at the G7 in 2021 [32]. On July 2, 2021, Kaseya, a software provider headquartered in Miami, suffered from a cyberattack that encrypted and disrupted the operation of more than a million end-customer's systems. In response, Kaseya identified the source of outbreak and shut down its cloud-based product to patch the vulnerabilities. [33]. A Tenable's report revealed common vulnerabilities and exposures has risen 183% from 2015 to 2020. Healthcare and education were among the industries most struck by cybersecurity breaches. Ransomware was the most popular genre of cyberattack occured in 259 incidents in 2020 alone. Due to growing threats of cyberattacks, efforts of vulnerability management with constant cybersecurity patching

and updates are essential [34].

Between 2010 and 2014, 150 successful cyberattacks on information systems of electricity grids was recorded by the US Department of Energy. Korea Hydro and Nuclear Power, a South Korean power company, was hacked in 2014 with the manuals of two nuclear reactors and data of 10,000 employees posted online [35]. The widespread Ukrainian blackout that cut power to 225,000 households in 2015 was caused by a virus attached in the phishing emails targeting system administrators responsible for distributing electricity throughout Ukraine. Another cyberattack was launched on Ukrainian in 2016, resulting in loss of Kiev's one-fifth power consumption during that night [36]. A 2017 cyber assault that hit a plant of a petrochemical company in Saudi Arabia was meant to trigger an explosion but accidentally shut down the plant due to a bug in the aggressor's source code. Investigators believed the cyber assault was much more dangerous than erasing hard drives which would have killed or injured people if the mistake was fixed [37].

2.3 Market Prospect

In 2020, Visiongain estimated the global cyberinsurance market at a value of US$7.29 billion whose projected growth would be at a compound annual growth rate of 21.4% over the decade 2021–2031. The development of information technologies has introduced a new set of hazards to both tangible and intangible assets currently not covered by existing insurance designs. Specifically, cyberinsurance in the past predominantly concentrated on digital assets like customer data. Experts in the industry predicted the coverage of cyberinsurance will likely further comprise physical assets and other assets such as intellectual properties,

business disruption [38].

According to FBIs Criminal Crime Complaint Center, complaint count of cyber crimes increased from 1,495 to 19,369 during 2014–2019. Over the same period, the associated financial losses rocketed from $60.3 million to $1.8 billion. Since the insurance companies strove for meeting the growing demand for loss coverage, direct premiums also grew steadily [28].

Due to increasing adoption of digitalization, higher cyber risks could trigger a rise in the cyber re/insurance pricing. A report predicted cyberinsurance could be one of the fastest growing insurance markets in the next decade, with cyber re/insurance premiums potentially doubling over 2021–2023. On the flip side, the volatility of cyber risks has discouraged the cyberinsurers from rapidly expanding the investment on capacity despite the growing demand. Thus, reinsurance market is still a major instrument for the primary insurers to manage the risks in the cyberinsurance market [39].

From 2016 to 2019, the number of cyberinsurance policies increased by about 60%, and the number of cyberinsurers increased by about 35%. Meanwhile, cyberattack costs to insurers nearly doubled. The cyberinsurance cost to insurers, following a increasing trend, depends on factors such as frequency and severity/cost of cyberattacks. Since cyberinsurance is a relatively new field with constantly evolving cybersecurity threats, it would be challenging to garner data essential to accurately estimate the policy cost, inevitably resulting in insolvency. Claim data collected from the policyholders may be used to improve the accuracy of the policies and offer more comprehensive coverage. On the other hand, a way for the insurers to reduce the risk exposure is to tighten the terms and conditions. Recently, more insurers had removed the limited cyber coverage used to be included in the commercial

and casualty insurance policies [40]. Many institutions, including businesses and the public sector, may not have a profound knowledge in cybersecurity despite regularly getting struck by cyberattacks. The cyberinsurers are responsible for promoting and educating the general public about the applications and importance of cyberinsurance. In addition, the contemporary cyberinsurance practices leave some gray areas without clear definition as to what is included in or excluded from cyber coverage [41]. Reinsurers also play an important role in enhancing risk resilience of the cyberinsurance ecosystem by providing extended coverage as risk transfer, policy making, actuarial support, data analytics and pre-/post-incident cyber solutions [42].

CHAPTER 3. A RELIABILITY-BASED CYBER-INSURANCE MODEL CONSIDERING OPTIMAL DEFENSE RESOURCE ALLOCATION

3.1 Introduction

Fig. 3.1 illustrates the ICT network of the power systems. There are three major parts connected through the WAN: generation operation, control center, and substations, each of which uses a LAN to coordinate the intelligent electronic devices. The substations are installed with the SCADA systems for monitoring the substations subject to potential cyberattacks. The cyberattack mechanism is described as follows. In the attacks, the attacker aims to infiltrate the firewalls or bypass the VPN to obtain access to the SCADA servers of the substations. After gaining the root privilege of the SCADA servers, the attacker may maliciously manipulate the voltage and current measurements or send false commands to trip the breakers in the substations. As a result, cyberattacks could disconnect generation units and transmission lines from the grid, leading to significant load curtailment and monetary losses of the TGs.

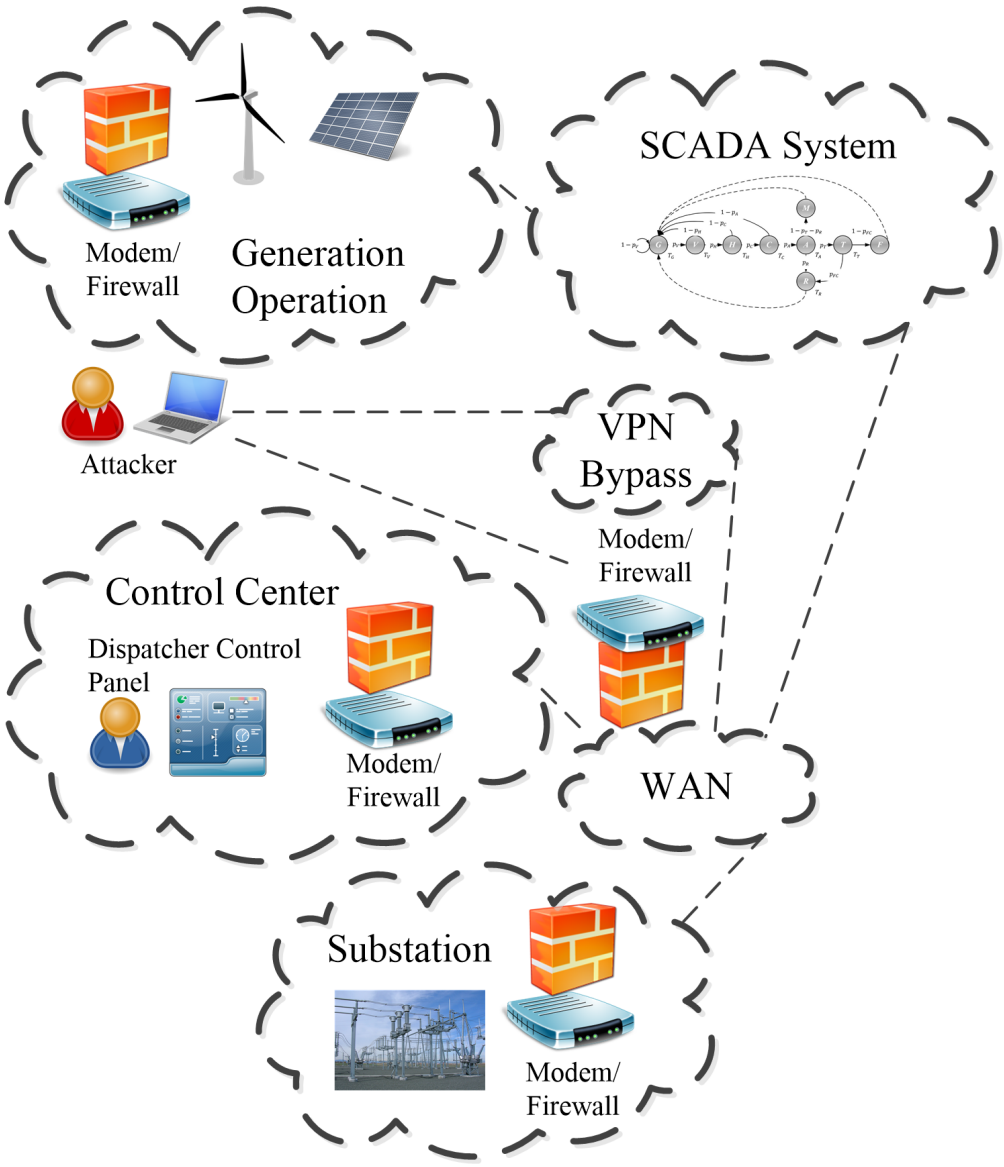


Figure 3.1: ICT Network including SCADA Infrastructure, Substations, Control Center, and Generation Operation System.

3.2 SMP Intrusion Tolerant Model

Widespread applications of the ICTs introduce higher risks on cybersecurity in the power systems. SMP model is applicable to evaluate the cyberattack on the SCADA system at each substation [17], [43]. An intrusion tolerant model of the SCADA system is formulated by SMP in this chapter. Referring to Fig. 3.2, the stochastic process of the cyberattack is composed of a set of states $S_n = \{G, V, H, C, A, T, R, M, F\}$, briefly described in Table 3.1. The states can be classified into two types: transient states and absorbing states. The transient states map the process of the attack on the SCADA system from the good state to the failure state. Restoration of the system to a good state takes place with a given probability determined by SSG. Absorbing states map the restoration process from the failure state to the good state except for state R which represents restoration. In brief, transient states $\{G, V, H, C, A, T, R\} \in S_t$ and absorbing states $\{M, F\} \in S_a$.

The details of the states in the proposed SMP are described as follows: Step 1) The SMP starts from the good state G where the system has no exposure to cybersecurity risks. Once the strategies for cybersecurity fail, the SCADA system is transitioned from the good state G to the vulnerability state V.

Step 2) When the attacker successfully gains the privilege of the targeted server, the SCADA system proceeds to the host state H.

Step 3) After the attacker infiltrates from the targeted server to obtain the privileges of the connection servers in the whole network, the network connection state C is reached.

Step 4) During state C, the attacker embeds backdoor programs in the servers to increase vulnerabilities of the SCADA system. The system enters the attack state A if an active attack

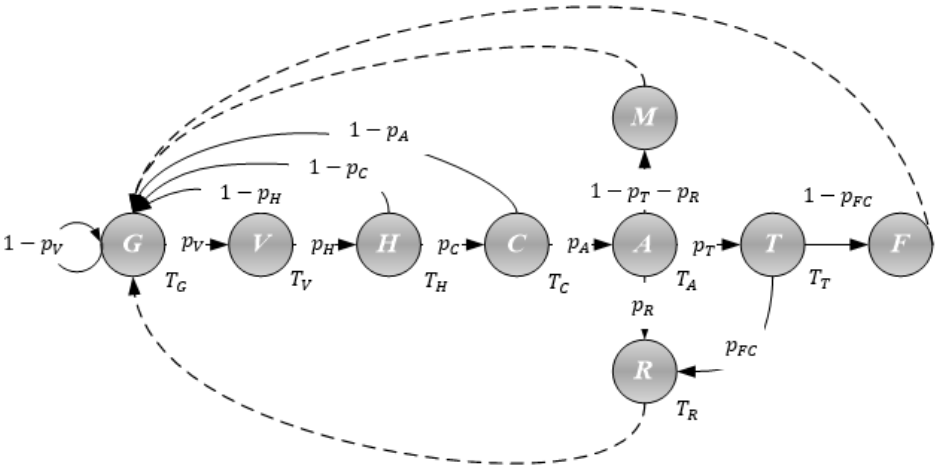


Figure 3.2: Semi-Markov process model of the intrusion tolerant SCADA system at power system substations.

Table 3.1: State Description in the SMP Model

State	Description
G	Good state. The system has no exposure to cybersecurity risks.
V	Vulnerability state. The cybersecurity countermeasure fails.
H	Host state. The attacker successfully gains the privilege of the targeted server.
C	Network connection state. The attacker obtains the privilege of the connection servers.
A	Attack state. The state where an active attack is successfully launched.
T	Triage state. The attack is identified during network exploitation.
R	Restoration state. Additional defense resources/security mechanisms are invested to the system to survive the attack.
M	Masked compromise state. The system has redundancy to offer normal services under the active attack.
F	Failure state. The state where damage occurs in the system.

is successfully launched.

Step 5) In the intrusion states $\{G, V, H, C, A\}$, if the attack process is exposed by the detection strategies of the SCADA system, the attack process is interrupted, and the system returns to the good state G.

Step 6) If the SCADA system has redundancy to offer normal services under the active attack, the masked compromise state M occurs.

Step 7) When the attack is detected during network exploitation, the triage state T is reached. In this state, various defense approaches are considered in response to the attack. If the defense resources are invested to sustain the attack, the restoration state R occurs. Otherwise, the system enters the failure state F and results in damage [44]. The cyberattack process is completed.

3.3 Cyberattack Modeling

The transient states of the SMP model capture the dynamics of the attack from the good state to the failure state, which is characterized by the MTTC. In practice, the MTTC is modeled based on the data of vulnerabilities and exploits. Herein, the SMP model is applied to evaluate the MTTC of target substations. In contrast, MTTR describes the mean time for the SCADA system to recover from the failure state to the good state. Denote the transition probability for the $(j, i)^{th}$-entry in the Markov kernel as p_{ji}, whose empirical values can be obtained by fitting the vulnerability occurrence data; and the Markov transition matrix

representing the SMP model of the cyberattack can be expressed as follows:

$$P_n = \begin{bmatrix} \tilde{p}_V & p_V & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \tilde{p}_H & \dots & p_H & \dots & \dots & \dots & \dots & \dots & \dots \\ \tilde{p}_C & \dots & \dots & p_C & \dots & \dots & \dots & \dots & \dots \\ \tilde{p}_A & \dots & \dots & \dots & p_A & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & p_T & p_R & \tilde{p}_{TR} & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & p_{DC} & \dots & \tilde{p}_{DC} \\ 1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{bmatrix} \tag{3.1}$$

subject to:

$$\sum_{i \in S_n} p_{ji} = 1, \forall j \in S_n \tag{3.2}$$

where $\tilde{p}_i = 1 - p_i$, $\tilde{p}_{TR} = 1 - p_T - p_R$ and $\tilde{p}_{DC} = 1 - p_{DC}$.

The visit counter V_i is defined by the average number of visits on transient state i. Combining the transition probabilities and mean sojourn times, MTTC can be calculated analytically, with the visit counter as an intermediate step. Individual visit counter holds a relation as follows:

$$V_i = 1_{\{i=G\}} + \sum_j V_j p_{ji}, i, j \in S_t \tag{3.3}$$

By matrix partitioning, submatrix P_t consisting of the transient states S_t is extracted

from P_n. P_t includes the information needed to calculate V_i.

$$\begin{bmatrix} \tilde{p}_V & p_V & \dots & \dots & \dots & \dots & \dots \\ \tilde{p}_H & \dots & p_H & \dots & \dots & \dots & \dots \\ \tilde{p}_C & \dots & \dots & p_C & \dots & \dots & \dots \\ \tilde{p}_A & \dots & \dots & \dots & p_A & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & p_T & p_R \\ \dots & \dots & \dots & \dots & \dots & \dots & p_{DC} \\ 1 & \dots & \dots & \dots & \dots & \dots & \dots \end{bmatrix} \tag{3.4}$$

Substituting the elements in P_t into 3.3, a linear system is constructed, and a unique solution for V_i is guaranteed since the system determinant is always non-zero. The analytical form of V_i is listed as follows:

$$\begin{cases} V_G = 1 + \sum_{i \in G,V,H,C} (1 - p_i) V_i + V_R \\ V_V = p_V V_G \\ V_H = p_H V_V \\ V_C = p_C V_H \\ V_A = p_A V_C \\ V_T = p_T V_A \\ V_R = p_R V_A + p_{DC} V_T \end{cases} \tag{3.5}$$

$$\begin{cases} V_G = \frac{1}{p_V p_H p_C p_A (1-p_R-p_{DC}p_T)}, \\ V_C = \frac{1}{p_A (1-p_R-p_{DC}p_T)}, \\ V_V = \frac{1}{p_H p_C p_A (1-p_R-p_{DC}p_T)}, \qquad V_A = \frac{1}{1-p_R-p_{DC}p_T} \\ V_H = \frac{1}{p_C p_A (1-p_R-p_{DC}p_T)}, \qquad V_T = \frac{p_T}{1-p_R-p_{DC}p_T} \\ V_R = \frac{p_R+p_{DC}p_T}{1-p_R-p_{DC}p_T} \end{cases} \tag{3.6}$$

An alternative way to obtain the sequence $\{V_i\}$ numerically is to extract the first column of the transpose of the matrix inverse of $I_t - P_t$:

$$\{V_i\} = V_i'' \ s.t. \ V'' = (I_t - P_t)^{-1} = [V_1'' \dots V_j'']^T \tag{3.7}$$

where I_t is the identity matrix with the same size as P_t. The randomness of the cyberattack, on the other hand, is modeled by the transition probabilities and mean sojourn times estimated by the random variables:

$$\begin{cases} p_i^U = b_1 \hat{p}_i^T + b_2 \hat{p}_i^N, \quad i \in S_t \\ T_i^U = b_1 \hat{T}_i^T + b_2 \hat{T}_i^N, \quad i \in S_t \end{cases} \tag{3.8}$$

where $\hat{p}_i^T$ and $\hat{p}_i^N$ are the tangent and normal transition probabilities in the SMC model of the intrusion tolerant system, respectively; $\hat{T}_i^T$ and $\hat{T}_i^N$ are the tangent and normal mean sojourn times in the SMC model of the intrusion tolerant system, respectively; and b_1 and b_2 are the weighting coefficients. MTTC $\bar{\lambda}$is expressed as follows by definition:

$$MTTC = \bar{\lambda} = \sum_{i \in S_t} V_i T_i \tag{3.9}$$

The transition probabilities, $\hat{p}_i^T$ and $\hat{p}_i^N$, which follow a Gamma distribution, must lie in $[0, 1]$. The mean sojourn times, $\hat{T}_i^T$ and $\hat{T}_i^N$, follow an exponential distribution. The weighting

coefficients b_1 and b_2 follow a Bernoulli distribution, i.e., $b_1 = 1 - b_2$, $b_2 \sim Bern(\zeta)$, where ζ is the mean value of the Bernoulli distribution. A Bernoulli distribution is a single-trial special case of the Binomial distribution. For observing the correlation of the cyber risk across the TGs, the tangent components $\hat{p}_i^T$, $\hat{T}_i^T$ represent individual cyber risks, while the normal components $\hat{p}_i^N$, $\hat{T}_i^N$ represent common cyber risks. In this model, $\zeta \in [0, 1]$ is the strength of interdependence. $\zeta = 0$ indicates no interdependence of the cyber risks across the TGs. $\zeta = 1$ indicates complete interdependence of the cyber risks. Otherwise, it is a case with partial interdependence of the cyber risks.

The mathematical modeling of these variates is explained below. The exponential variate for each mean sojourn time component is generated through a simple logarithmic operation on the uniform variate. Given the specified mean value $T_j > 0$,$j \in S_t$, the random variable for the tangent mean sojourn time $\hat{T}_i^T$ that follows an exponential distribution is expressed as:

$$f(\hat{T}_i^T) = \frac{1}{T_j} \exp - \frac{x}{T_j} \tag{3.10}$$

By the inverse transform method, the sampled tangent mean sojourn time $\hat{T}_i^T$ is obtained:

$$\hat{T}_i^T = F^{-1}(U) = -T_j \ln(1 - U) \tag{3.11}$$

where U is a uniform variate between $(0, 1)$. The normal mean sojourn time $\hat{T}_i^N$ is computed in a similar manner.

The components of the transition probabilities $\hat{p}_i^T$ and $\hat{p}_i^N$ are Gamma variates. Set $\hat{p}_i = \{\hat{p}_i^T, \hat{p}_i^N\}$. Since the inverse transform of the Gamma distribution is quite complicated, the variates of $\hat{p}_i$ are instead obtained from summing i.i.d. exponential variates. Denote

each exponential variate as Z_i s.t. $E[Z_i] = \bar{z}_i$, then:

$$\hat{p}_i = Z_1 + Z_2 + \cdots + Z_n = \sum_{i=1}^{n} Z_i, E[\hat{p}_i] = n\bar{z}_i \tag{3.12}$$

Remark 1. Using the moment generating function method, it can be shown that if $Z_i \sim Exp(\bar{z}_i)$, $\hat{p}_i \sim Gamma(n, \bar{z}_i)$ [45].

The randomness of cyberattacks is modeled by a time sequence generated by a given variate. Weibull distribution, a distribution function typically used in failure analysis, is the selected type of variate. TTC λ following a Weibull distribution has the following probability density function:

$$g(\lambda) = \frac{k}{\breve{\lambda}}\lambda^{k-1} \exp -(\frac{\lambda}{\breve{\lambda}})^k \tag{3.13}$$

where $\lambda \geq 0$,$k > 0$, with the mean value $\breve{\lambda}\Gamma(1 + \frac{1}{k}) = \bar{\lambda}$. Take indefinite integral, the cumulative density function is obtained:

$$U = G(\lambda) = \int_0^{\lambda} g(\mathcal{T})d\mathcal{T} = 1 - \exp -(\frac{\lambda}{\breve{\lambda}})^k \tag{3.14}$$

The state duration sampling is implemented using the following relation:

$$\lambda = G^{-1}(U) = \breve{\lambda}[-\ln(1 - U)]^{1/k} \tag{3.15}$$

The power system reliability worth evaluated in this chapter is the monetary loss. Expected values of reliability worth are computed as:

$$ERW = E[X] = \sum_{\underline{\Omega}} K_\Omega W(D_\Omega) \tag{3.16}$$

where X is the potential loss, $\underline{\Omega}$ is the load loss event set, K_Ω is the probability density kernel of loss event Ω, D_Ω is the duration of loss event Ω, and $W(D_\Omega)$ is the cost mapping function of loss event Ω.

3.4 Insurance Premium Principle

The design goals of the cyber-insurance principle are as follows: (1) the premiums should sufficiently cover the claims of the potential losses; and (2) the premiums should be affordable for the TGs. In this section, the losses mentioned are referred to the reliability worth, i.e., the monetary losses induced by load interruption.

A fundamental and widely used insurance principle is the expected value premium. Given a potential loss X, the expected value premium is calculated as follows:

$$\pi(X) = (1 + \rho)E[X] \tag{3.17}$$

where ρ is the Risk Loading Coefficient (RLC). RLC is set positive to cushion against uncertainty, administration cost, as well as to provide some profit margin. On the other hand, RLC is usually relatively low to guarantee the affordability of the insurance product. Fortunately, even with a low RLC, the law of large number guarantees that the total premium collected by the insurer is sufficient to cover the total potential losses, as long as the insurance pool is large enough. It should be stressed that this law works well only in traditional insurance practice where individual risks are independent. However, due to the nature of cybersecurity threats, cyber-related losses from different TGs are likely to be dependent. Therefore, more advanced premium principles are needed to price and manage these potentially dependent risks.

Definition 1 (Total Premium via VaR): Denote the potential losses in different TGs as $X_1, X_2, ..., X_n$. Given the total loss $TL = \sum_{i=1}^{n} X_i$, a total premium via Value at Risk (VaR) is calculated as:

$$TP_1 = VaR_\alpha(TL) = VaR_\alpha(\sum_{i=1}^{n} X_i) \tag{3.18}$$

where $VaR_\alpha(Y) = \inf\{y : P(Y > y) \leq \alpha\}, \alpha \in (0,1)$. The premium is defined to control the confidence level α that the total loss TL exceeds the total premium TP_1, i.e., $P(TL > TP1) = \alpha$.

Definition 2 (Total Premium via TVaR): To ensure the premium better covers the potential loss, a more conservative option for the insurer is a total premium via Tail Value at Risk (TVaR):

$$TP_2 = TVaR_\alpha(TL) = \frac{1}{\alpha}\int_0^\alpha VaR_p(TL)dp \tag{3.19}$$

Mathematically, the probability that the total loss TL exceeds the total premium TP_2 is bounded by the confidence level α, i.e., $P(TL > TP2) < \alpha$. In this sense, the TVaR premium is more conservative than the VaR premium.

The determined total premium is then allocated to individual TGs. To do so, new premium designs are necessary. Denote the centralized version of the i^{th} potential loss X_i as $X_i' = X_i - E[X_i]$, and the centralized total loss as $TL' = \sum_{i=1}^{n} X_i E[X_i]$.

Definition 3 (VaR and TVaR-Derived Premiums): The individual premiums via VaR (π_1) and TVaR (π_2) can be respectively calculated by:

$$\pi_1(X_i) = E[X_i] + \frac{VaR_\alpha(X_i')}{\sum_{i=1}^{n} VaR_\alpha(X_i')} VaR_\alpha(TL') \tag{3.20}$$

$$\pi_2(X_i) = E[X_i] + \frac{TVaR_\alpha(X_i')}{\sum_{i=1}^{n} TVaR_\alpha(X_i')} TVaR_\alpha(TL') \tag{3.21}$$

The allocated individual premiums are straightforward for the total premiums TP_1 and TP_2 in the sense that:

$$\sum_{i=1}^{n} \pi_1(X_i) = VaR_\alpha(TL) = TP_1 \tag{3.22}$$

$$\sum_{i=1}^{n} \pi_2(X_i) = TVaR_\alpha(TL) = TP_2 \tag{3.23}$$

A simpler premium design (π_3) to allocate TP_2 based on individual contributions to the total TVaR is defined as below:

$$\pi_3(X_i) = E[X_i | TL > VaR_\alpha(TL)] \tag{3.24}$$

It can be easily shown that $\sum_{i=1}^{n} \pi_3(X_i) = TVaR_\alpha(TL) = TP_2$.

The premium allocation is analogous to the capital allocation problem, which has been well studied in the financial literature [46]. Therefore, the premium designs proposed above share certain commonalities with some capital allocation principles. However, a necessary emphasis is that the proposed insurance premium principle is an innovative attempt for insurance pricing application. The major difference between the proposed premium designs and traditional ones lies in the consideration of potential dependence among risks. Traditional premium designs price risks based on marginal characteristics without considering dependence. In the context of cyberinsurance, this could result in serious insolvency situation for the insurer. The proposed premium designs determine the premiums based on the total losses and thus substantially mitigate the insolvency risk.

3.5 Proposed Game-Theoretic Cyber-Insurance Framework

Game theory has been applied to decentralize the power system control to reduce the risk of failures in the communication infrastructures. By avoiding the need of a top-down design, decentralized multiplayer games can model the power system dynamics as component players in a game. In addition, the nature of the general-sum games also enables the

possibility of cooperation or bargaining [47], [48]. Stackelberg game is a class of hierarchical games. The leading agent commits to a strategy before the following agent in a typical Stackelberg game. The agent can be a player or a coordinated group. In a two-player SSG, the defender is the leader, and the attacker is the follower.Specifically, the attacker chooses its best strategy given the action of the defender. SSG is widely used in practical applications such as scheduling patrols, traffic checkpoints, airport transportation protection in areas of heavy terrorist activities [49]-[53]. Interested readers are referred to [54] for more details of the applications and corresponding challenges of the SSG. The compact-form algorithms for multi-target SSGs can significantly accelerate the computation compared to the normal-form approaches [55][57].

With the increasing penetration of Wide Area Network (WAN), protecting the CPSs from potential risks becomes of the utmost importance. Since the resources for defending the CPS are usually scarce, the strategy for effectively distributing the defense resources determines the strength of the targets to resist the adversaries. The defense resources are referred to a weight assignment system that quantifies the available security budget. The defense resources reflect the relative cost and effort required to construct the security countermeasure, including authentication, authorization, encryption, firewalls, antivirus software, intrusion detection systems, etc. To ensure the cybersecurity of substations, defense resources can be invested on necessary defense mechanisms against the cyberattacks. For example, the firewalls of SCADA servers can be equipped with advanced security tools such as network analyzers, scanners, and forensic software to monitor and control the incoming and outgoing network traffic.

ORIGAMI is an algorithm designed for a two-player general-sum game. Here ORIGAMI

is intended to identify the vulnerability of each target considering the security budget available for each TG in a twoplayer general-sum SSG [55]. The algorithm serves as a risk evaluation method on the defenders end, envisioning potential cybersecurity threats in the system. Distributed ORIGAMI is deployed by each TG to allocate the defense resources on the associated substations. In other words, the investment of defense resources protects the targets from potential cyberattacks. In this chapter, the ORIGAMI algorithm is integrated into power system reliability analysis subject to cybersecurity threats considering the optimal defense resource allocation scheme. ORIGAMI transforms the original NP-hard problem to a more efficient iteration form. The detailed procedure of ORIGAMI is depicted in Algorithm 3.1.

Remark 2: In ORIGAMI, the compact two-player SSG model is represented by the payoff functions of the attacker α and the defender β on the target set $\tau = \{\tau_1, \tau_2, ..., \tau_n\}$ given the defense coverage sequence $\mathcal{C} = \{p_{DC}(\tau_i)\}$. Each target τ_i is assumed to start from a good state. For both the attacker and defender, two scenarios are considered: a target is either covered c or uncovered u by the defender. The payoff functions are calculated as follows:

$$U_\alpha(\mathcal{C}, \tau_i) = p_{DC}(\tau_i)U^c_{\alpha,\tau_i} + (1 - p_{DC}(\tau_i))U^u_{\alpha,\tau_i} \tag{3.25}$$

$$U_\beta(\mathcal{C}, \tau_i) = p_{DC}(\tau_i)U^c_{\beta,\tau_i} + (1 - p_{DC}(\tau_i))U^u_{\beta,\tau_i} \tag{3.26}$$

where $p_{DC}(\tau_i) \in [0, 1]$; the attackers payoff for a covered attack is denoted by U^c_{α,τ_i} , and an uncovered attack is denoted by U^u_{α,τ_i}. Likewise, U^c_{β,τ_i} and U^u_{β,τ_i} for the defender. With the binary attack sequence $\mathcal{A} = \{a(\tau_i)\}$, the defenders payoff is:

Algorithm 3.1: Substation Protection Coverage Considering Optimal Defense Resource Allocation

Input: $target\ set\ \tau = \{\tau_1, \tau 2, \ldots, \tau_n\}, defense\ resources\ m$
Output: $\mathcal{C} = \{p_{DC}(\tau_i)\}$
function
  Generate $\{U^u_{\alpha,\tau_i}\}$, $\{U^c_{\alpha,\tau_i}\}$ by a set of random variables
  Sort the targets by uncovered attacker's payoff $\{U^u_{\alpha,\tau_i}\}$
  Initialize $left \leftarrow m$, $next \leftarrow 1$,$\mathcal{C} \leftarrow \mathbf{0}$, $\{\Delta p_{DC}(\tau_i)\} \leftarrow \mathbf{0}$,$Cvg_{Bnd} \leftarrow -\inf$
  repeat
    for $i = 1 : next$ **do**
      Compute $\Delta p_{DC}(\tau_i) \leftarrow \frac{U^u_\alpha(next) - U^u_\alpha(\tau_i)}{U^c_\alpha(\tau_i) - U^u_\alpha(\tau_i)}$
      if $p_{DC}(\tau_i) + \Delta p_{DC}(\tau_i) \geq 1$ **then**
        $Cvg_{Bnd} \leftarrow \max(Cvg_{Bnd}, U^c_\alpha(\tau_i))$
      end
    end
    Compute $sum(\Delta p_{DC}(\tau_i))$
    if $Cvg_{Bnd} \geq -\inf$ ***OR*** $\Delta p_{DC}(\tau_i) \leq left$ **then**
      BREAK
    end
    $\mathcal{C}(\tau) \leftarrow \mathcal{C}(\tau) + \Delta p_{DC}(\tau)$
    $left \leftarrow left - sum(\Delta p_{DC}(\tau_i)))$
    $next++$
  until $next == n$;
  Compute $ratio(i) \leftarrow \frac{1}{U^u_{\alpha,\tau_i} - U^c_{\alpha,\tau_i}}$, $i = 1 : next$
  Compute $sum(ratio(i))$
  for $i = 1 : next$ **do**
    $p_{DC}(\tau_i) \leftarrow p_{DC}(\tau_i) + ratio(\tau_i) * \frac{left}{sum(ratio(i))}$
    if $Cvg_{Bnd} \geq 1$ **then**
      $Cvg_{Bnd} \leftarrow \max(Cvg_{Bnd}, U^c_{\alpha,\tau_i})$
    end
  end
  if $Cvg_{Bnd} > -\inf$ **then**
    $p_{DC}(\tau_i) \leftarrow \frac{Cvg_{Bnd} - U^u_\alpha(\tau_i)}{U^c_\alpha(\tau_i) - U^u_\alpha(\tau_i)}$, $i = 1 : next$
  end
end

$$U_\beta(\mathcal{C}, \mathcal{A}) = \sum_\tau a_\tau U_\beta(C, \tau_i) \tag{3.27}$$

subject to $a(\tau_i) \in \{0, 1\}$.

Remark 3: A solution of SSE is always guaranteed in SSG, which occurs when the defender chooses an optimal mixed strategy to maximize the defenders payoff. In a typical two-player SSG, the SSE does not coincide with the Nash equilibrium unless the game is zero-sum.

ORIGAMI computes the attacker/defenders payoff with randomized covered/ uncovered initial payoffs on each target to accelerate the defense resource allocation. The optimal mixed strategy of the defender in this setting can be computed in polynomial time [58]. Randomly distributing the initial payoffs facilitates the encryption against the attack. ORIGAMI features iterative search for the attackers minimal payoff whose defense coverage roughly coincides with the defenders maximal payoff.

In this chapter, ORIGAMI allocates the defense resources based on the attack/defense payoff of each target according to the TG ownership of the load buses. In Algorithm 3.1, the defense resources m are either assigned to individual targets or not at all, generating the defense coverage sequence $\mathcal{C} = \{p_{DC}(\tau_i)\}$. The effect of the target correlation is mostly induced by the SMP model, with slight variation caused by the power system configuration and the defense resource allocation. In the next section, target correlation among TGs will be demonstrated in the case studies of reliability assessment.

The complete procedure of the proposed cyber-insurance framework is demonstrated by the flow chart in Fig. 3.3.

Cybersecurity reliability assessment: based on the ownership boundary indicated in

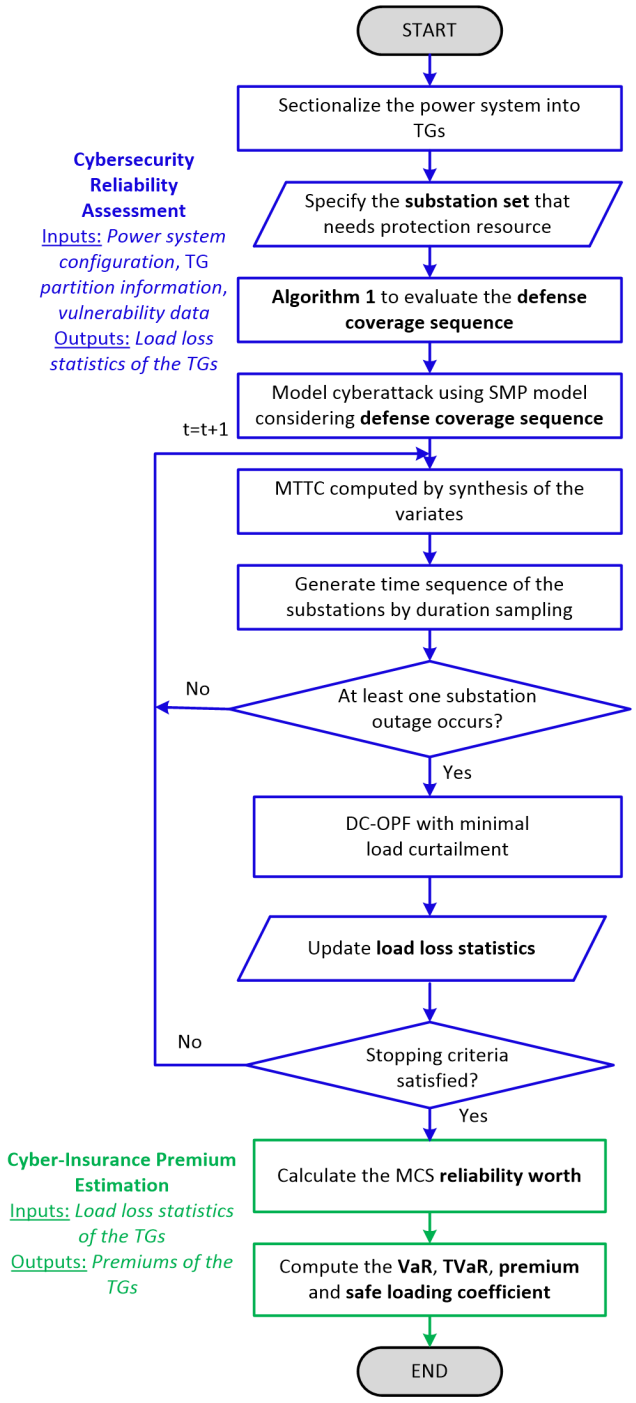


Figure 3.3: Procedure of the proposed cyber-insurance framework considering integrated cybersecurity-reliability assessment.

the TG partition information, the power system is sectionalized into individual TGs. The empirical mean values in the SMC model can be obtained by fitting the vulnerability data in practice. In the SMP model, defense resource allocation is achieved by plugging in $\{p_{DC}(\tau_i)\}$ obtained from Algorithm 3.1. Incorporating the randomness in the transition probabilities and mean sojourn times, the MTTC statistics is synthesized to generate the time sequence of the cyberattacks via the sampled TTC. If at least one substation outage exists, the optimal power flow analysis is performed to minimize the load curtailment. The total load curtailment and loss of load duration are then recorded. The process is repeated until the stopping criterion is reached.

Cyber-insurance premium estimation: based on the statistical records of the load loss in the MCS, the reliability worth based on the results of the MCS is calculated. The cyber-insurance premiums for the TGs are then determined. The premium principle was presented in detail in the previous section.

3.6 Numerical Evaluation and Analysis

3.6.1 Base Case Loss Evaluation

The single-line diagram of the IEEE Reliability Test System RTS-96 used for case studies of the proposed cyber-insurance framework is shown in Fig. 3.4. The IEEE RTS-96 is composed of 3 identical areas, 6 inter-area transmission lines, with details specified in [59]. The test system is assumed to be individually operated by 7 independent TGs. TG1-TG2 are located at Area 1, TG3-TG5 are located at Area 2, and TG6-TG7 are located at Area 3.

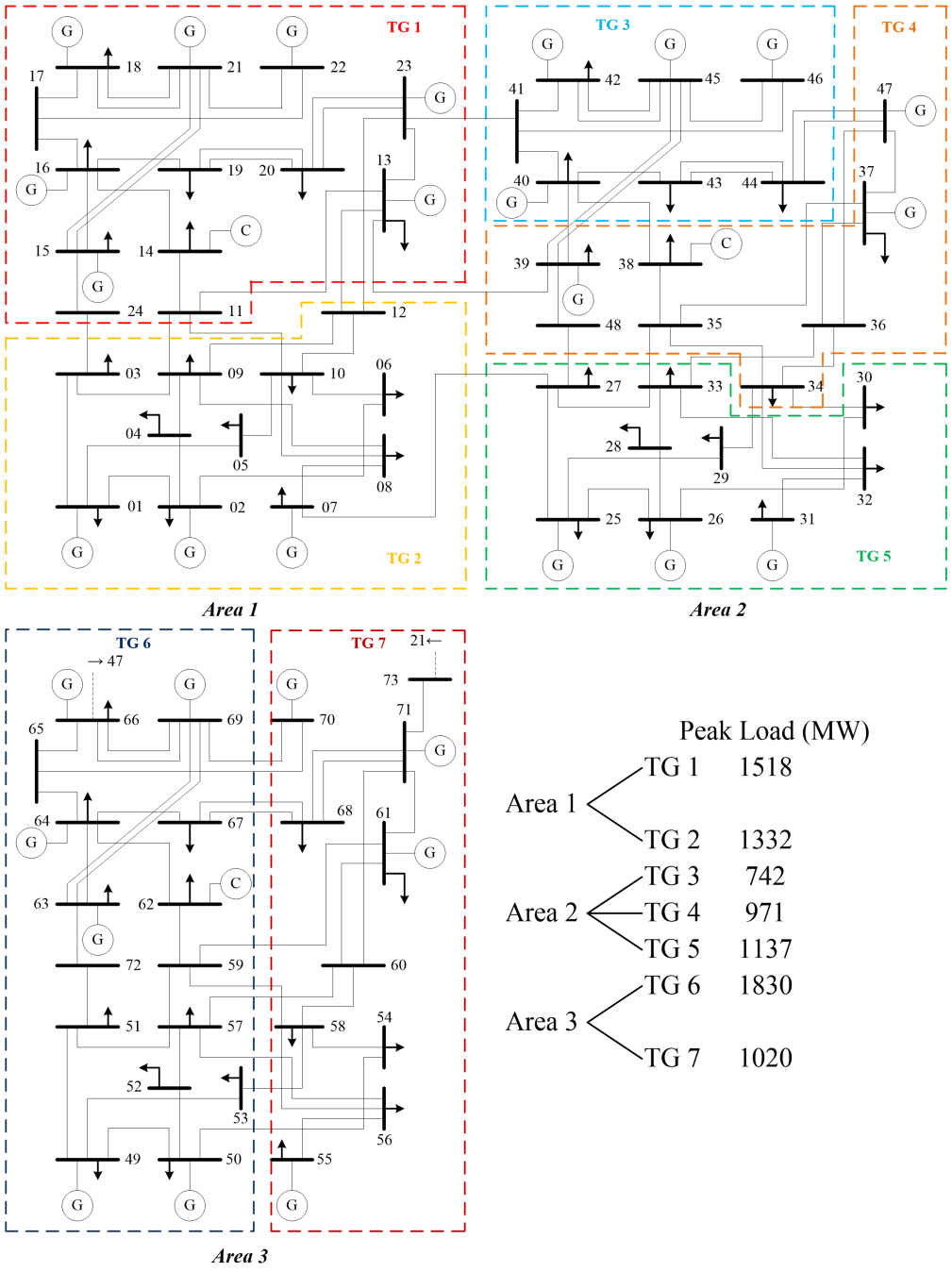


Figure 3.4: IEEE Reliability Test System RTS-96

In the case studies, sequential MCS is conducted using the SMP model to estimate TG adequacy subject to cyberattacks. For each TG, the defense resource coverage is allocated in the SMP model using SSG. The sequential MCS is conducted over a period of 2,000 years with hourly intervals.

The following parameters are the mean values of the SMP model in case studies:

$$\begin{cases} T_G = 5\ days, T_V = 2\ days, T_H = 1\ day, T_C = 0.5\ day \\ T_A = 0.5\ day, T_T = 0.5\ day, T_R = 1\ day \\ p_V = 1, p_H = 0.6, p_C = 0.5 \\ p_A = 0.4, p_T = 0.5, p_R = 0.3 \end{cases} \tag{3.28}$$

where $\{p_{DC}(\tau_i)\}$ is directly determined by Algorithm 3.1.

In addition to the parameters, the allocation of the defense resources determines the intrusion tolerant capability and thus the security level of each TG. Two case groups are set up to demonstrate the impact of the intrusion tolerant capability in the case studies. In the case group of LDC, the available defense resources only suffice for protecting 20% of the substations in each TG. This case group examines the effectiveness of the SSG with a tight budget of the defense resources. On the other hand, we would also like to know the loss distribution across the TGs when abundant defense resources are accessible. In the case group of HDC, the available defense resources are increased to cover 80% of the substations. The nominal MTTCs calculated based on the foregoing SMP mean values in 3.28 and $\{p_{DC}(\tau_i)\}$ are illustrated in Fig. 3.5, with the substations sorted in ascending order of the bus number in the individual TGs. TGs with high defense coverage are expected to

provide protection more robust against cyberattacks. For example, TG1 has 13 buses, with high defense coverage, the defense resources are set as $m_{TC_1} = 13 * 80\% \approx 10$ and allocated as follows:

$$\begin{aligned} &\{p_{DC}(\tau_i)\}_{TC_1} \\ &= \{0.5491, 0.5757, 0.3778, 0.8704, 0.5171, 0.6996, 1.0000, \\ &\quad 0.4610, 0.7340, 0.8944, 0.7562, 0.8893, 0.8987\} \end{aligned} \tag{3.29}$$

The defense coverage sequence has a sum limited by the defense resources. For verification, $sum(p_{DC}(\tau_i))_{TG_1} \leq m_{TG_1}$.

By substituting 3.28 and 3.29 into 3.6 and 3.9, the resulting nominal MTTC (days) are given as follows:

$$\begin{aligned} &\{MTTC\}_{TC_1} \\ &= \{154.91, 159.95, 128.79, 249.51, 149.27, 188.43, 330.67, \\ &\quad 140.29, 198.21, 261.38, 205.08, 258.77, 263.63\} \end{aligned} \tag{3.30}$$

Likewise, the nominal MTTC of other TGs can be computed.

In both case groups, various strengths of interdependence are considered: $\zeta = 0$, $\zeta = 0.7$, and $\zeta = 1$. Interdependence strength is a contributing factor for high vulnerabilities of the TGs. Cyberattacks are launched to the targets/substations. The time sequence of each substation is determined by random variables in the SMP model. Here we assume when a substation which enters the failure state is compromised by cyberattacks, the connected generators and transmission lines will be tripped.

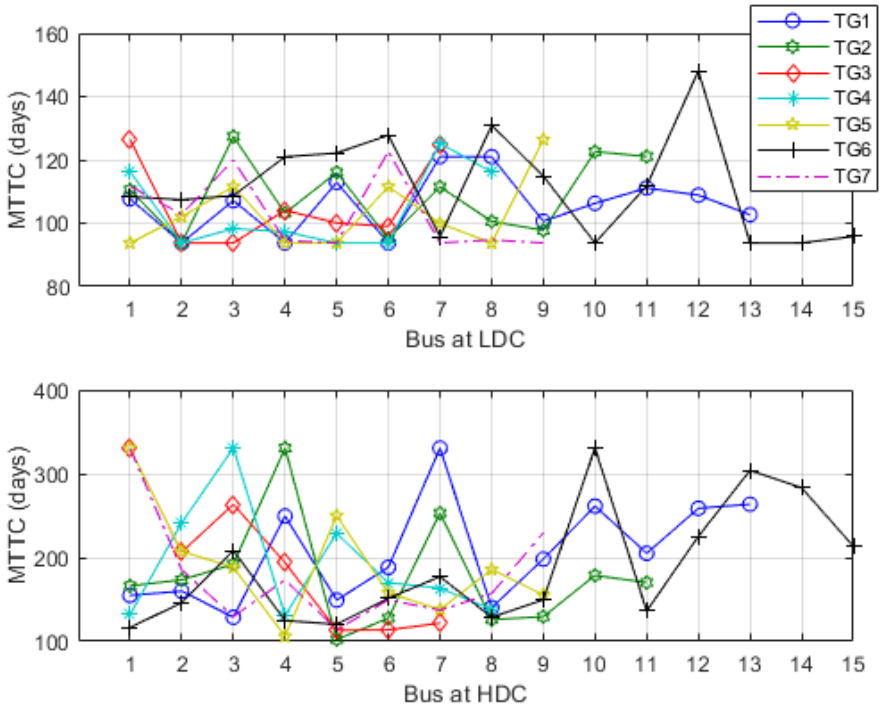


Figure 3.5: Substation nominal MTTCs of the TGs at various defense coverages.

The OPF is then performed in the TGs to minimize the load curtailment subject to the deficient generation capacity and network constraints. Reliability worth, i.e., the monetary losses, is calculated based on the OPF results. Finally, the actuarial insurance principle is applied to estimate the individual TG premiums based on the monetary loss distribution due to cyberattacks.

In the case group of low defense coverage, the expected values, SDs, and CoVs under various cases are listed in Table 3.2. The expected values and standard deviations only vary slightly with the increased strength of interdependence ζ . The CoV lies in a typical range $[0.64, 0.76]$. The loss distribution histogram illustrated as Fig. 3.6 agrees with the values in Table 3.2. For different levels of interdependence strength, the bins follow a heavy-tailed and roughly monotonic distribution. The correlation matrices visualized as Fig. 3.7 indicate the correlation between the TGs increases as the common cyber risk increases. Except the diagonal entries (which must be 1), the planes of the correlation remain quite flat. When $\zeta = 0$, any two of the TGs share no interdependence as indicated by the fact that the correlations are close to zero. The correlations range between $[0.20, 0.30]$ as ζ increases to 0.7. $\zeta = 1$ results in high correlations up to 0.69.

In the case group where high defense coverage is applied, disappearance of high losses is noticeable in Fig. 3.8. In the marginal distributions, it can be clearly observed that the probability mass shifts to the low loss area. Concentration of the loss distribution on the lower end also contributes to the increased CoVs lying in [0.730.92] as listed in Table 3.3. Substantial reduction on the losses can be clearly observed across the TGs. Fig. 3.9 shows the strength of interdependence is decreased with high defense coverage. The case of $\zeta = 0$ reflects exact uncorrelation. $\zeta = 0.7$ induces mild correlations bounded by $[0.15, 0.25]$. When

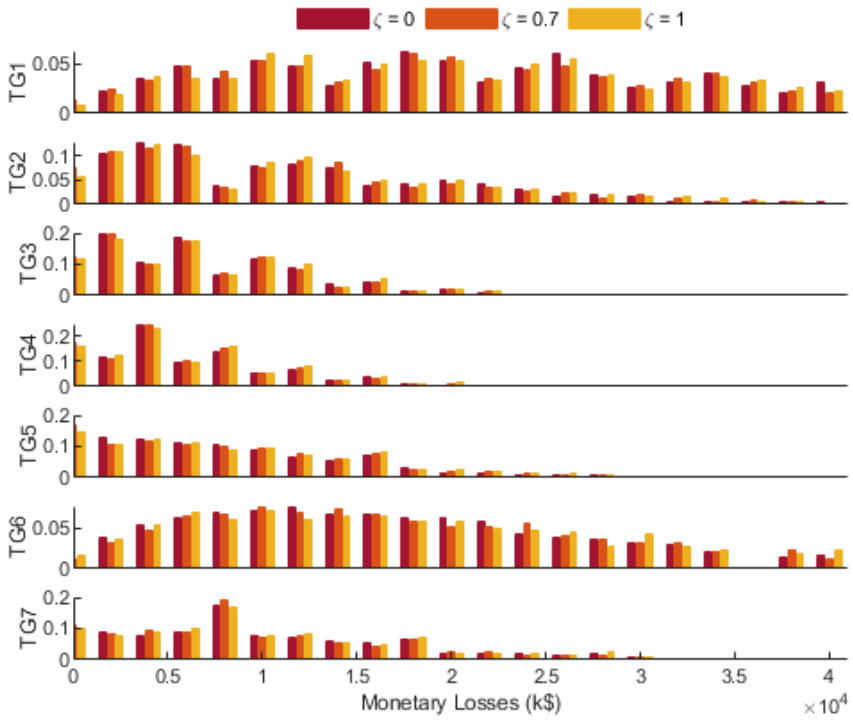


Figure 3.6: Histogram of the marginal distributions of the losses in the TGs at Low Defense Coverage.

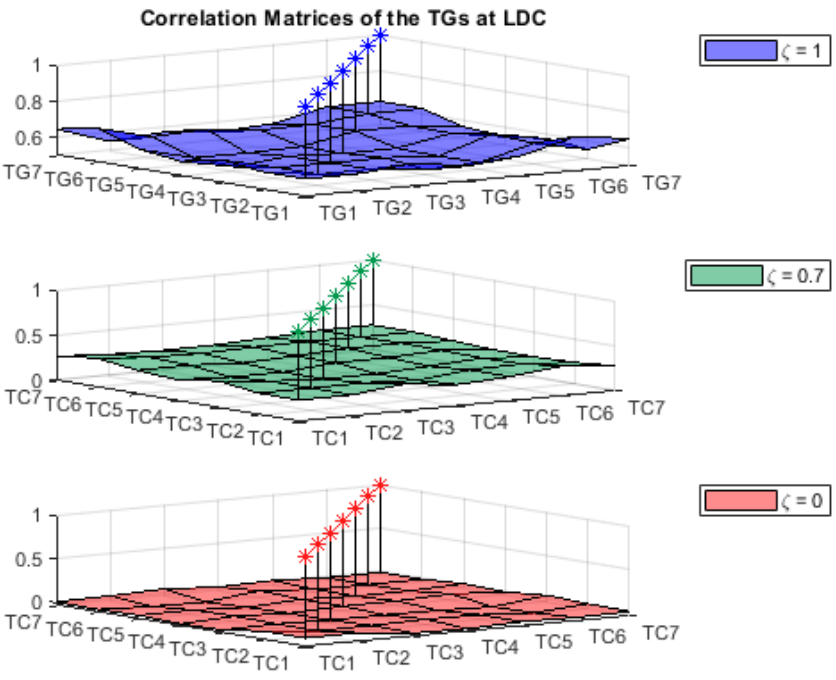


Figure 3.7: Correlation matrices with various strengths of interdependence at Low Defense Coverage.

Table 3.2: Expected Values (K$), Standard Deviations (K$) and Coefficients of Variation of Monetary Loss in the TGs at LDC

$\zeta = 0$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**	**TG6**	**TG7**
$E[X]$	27102	12138	7714	6252	8806	19440	10663
SD	17220	9031	5369	4704	6425	12746	7411
CoV	0.635	0.744	0.696	0.753	0.730	0.656	0.695
$\zeta = 0.5$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**	**TG6**	**TG7**
$E[X]$	27790	12585	7835	6685	9191	20214	10769
SD	17862	9548	5549	4910	6677	13102	7491
CoV	0.643	0.759	0.708	0.735	0.727	0.648	0.696
$\zeta = 1$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**	**TG6**	**TG7**
$E[X]$	28324	13215	8239	6815	9779	20465	11437
SD	18129	9852	5853	5072	7234	13522	8013
CoV	0.640	0.746	0.710	0.744	0.740	0.661	0.701

$\zeta = 1$, the correlations shift to $[0.45, 0.60]$. Both the relatively reduced losses and weaker interdependence as shown by the correlation matrices result from the high defense coverage. Correlation between any two TGs is varied by the TGs interconnection and security against cyberattacks.

Given the mean values of the parameters in the SMP model, the marginal statistics of the TGs are chiefly determined by the defense resource coverage and respective load distributions. Since the assumed cyberattacks are launched evenly to each substation, the TGs with more evenly distributed loads would preserve higher power security. For example, TG6 has a higher peak load but lower intrusion-induced loss than TG1.

Individual premiums of the TGs are designed to reflect the distribution of the losses

Table 3.3: Expected Values (K$), Standard Deviations (K$) and Coefficients of Variation of Monetary Loss in the TGs at HDC

$\zeta = 0$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**	**TG6**	**TG7**
$E[X]$	13845	6614	5035	4244	4472	11558	6169
SD	10109	5717	3788	3406	3947	8524	4845
CoV	0.730	0.864	0.752	0.802	0.883	0.738	0.785
$\zeta = 0.5$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**	**TG6**	**TG7**
$E[X]$	14052	6757	5052	4403	4562	12106	6424
SD	10879	6140	3937	3614	4127	9005	5065
CoV	0.774	0.909	0.779	0.821	0.905	0.744	0.789
$\zeta = 1$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**	**TG6**	**TG7**
$E[X]$	14745	7266	5304	4645	4865	12324	6712
SD	11394	6362	4268	3975	4452	9540	5633
CoV	0.773	0.876	0.805	0.856	0.915	0.774	0.839

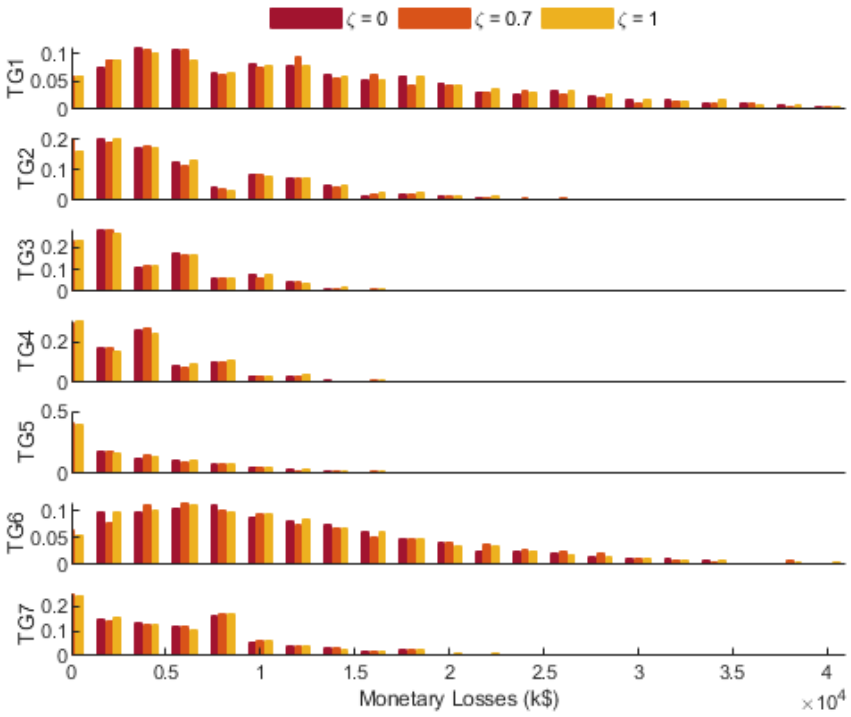


Figure 3.8: Histogram of the marginal distributions of the losses in the TGs at High Defense Coverage.

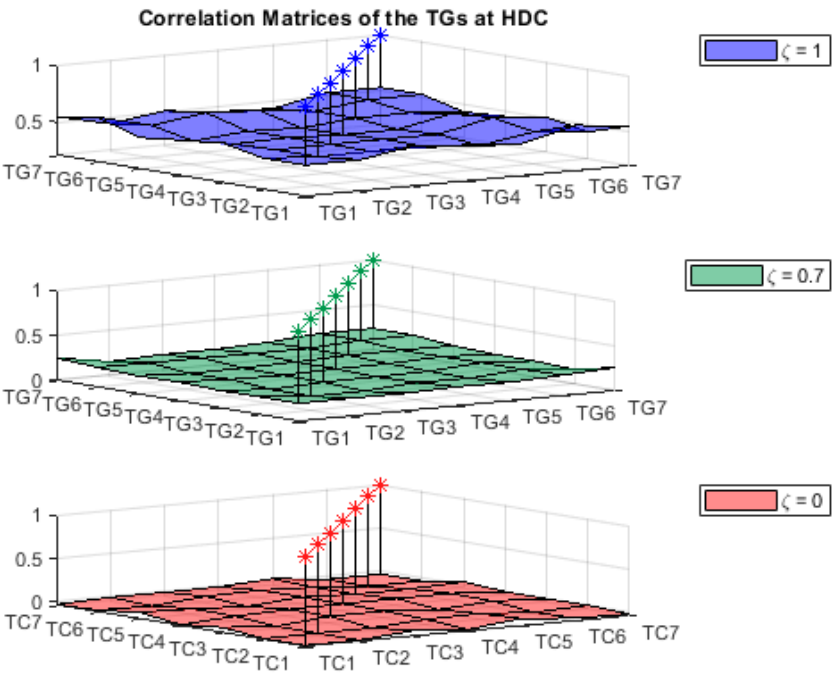


Figure 3.9: Correlation matrices with various strengths of interdependence at High Defense Coverage.

due to the cyberattacks. In the following subsection, the interdependence strength ζ which is varied in the SMC models across the TGs would exhibit its impacts on the premiums.

3.6.2 Actuarial Premium Calculation

Using the premium principle formulae 3.20, 3.21, 3.24, individual premiums of all the TGs are calculated. In this subsection, a confidence level of $\alpha = 5\%$ is set for all the premiums. From the insurers perspective, controlling the riskiness at a relatively low level is preferable. Specifically, π_1 (Premium via VaR) is designed to ensure the total premium is greater than the total loss with a probability of 1α.

π_2 (Premium via TVaR) guarantees the total premium exceeds the total loss with a probability greater than 1α. In this sense, π_2 can better cover the potential loss than π_1 premium although both exhibit the same trend in each TG. Unlike π_2, π_3 (Simplified Premium via TVaR) allocates the total premium TP_2 based on the individual contributions to the total TVaR instead of the ratios associated to marginal characteristics. In this way, π_3 better reflects individual responsibilities to the riskiness of the insurance portfolio. Individual premiums estimated using π_2 and π_3 turn out to be close. Under the proposed premium principle, the RLC is reintroduced as a measure of affordability of the insurance premiums. Specifically, it measures the proportion by which the premium exceeds the expected value of the risk:

$$\rho_i(X_i) = \pi(X_i)/E[X_i] - 1 \tag{3.31}$$

Due to the common cyber risks, individual RLCs would be substantially higher than those

Table 3.4: Actuarial Insurance Premiums (K$) of the TGs at LDC

$\zeta = 0$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**	**TG6**	**TG7**
π_1	40159	18684	11557	10068	13744	28306	16167
ρ_1	0.482	0.539	0.498	0.611	0.561	0.456	0.516
π_2	68020	33946	20999	18252	25404	52429	28880
ρ_2	1.51	1.80	1.72	1.92	1.88	1.70	1.71
π_3	68606	34258	20902	17767	24939	52795	28665
ρ_3	1.53	1.82	1.71	1.84	1.83	1.72	1.69
$\zeta = 0.5$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**	**TG6**	**TG7**
π_1	48088	23619	14430	12301	17633	34663	19177
ρ_1	0.730	0.877	0.842	0.840	0.919	0.715	0.781
π_2	70266	36165	22366	19289	26918	53872	29490
ρ_2	1.53	1.87	1.85	1.89	1.93	1.67	1.74
π_3	71255	36715	21827	19164	25895	53736	29774
ρ_3	1.56	1.92	1.79	1.87	1.82	1.66	1.76
$\zeta = 1$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**	**TG6**	**TG7**
π_1	57069	29479	17110	14548	21075	42191	24000
ρ_1	1.01	1.23	1.08	1.13	1.16	1.06	1.10
π_2	73704	37950	23549	19922	28585	55663	31876
ρ_2	1.60	1.87	1.86	1.92	1.92	1.72	1.79
π_3	74535	38403	23336	19919	28427	54552	32073
ρ_3	1.63	1.91	1.83	1.92	1.91	1.67	1.80

Table 3.5: Actuarial Insurance Premiums (K$) of the TGs at HDC

$\zeta = 0$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**	**TG6**	**TG7**
π_1	21271	10972	7926	6726	7569	17658	9515
ρ_1	0.536	0.659	0.574	0.585	0.692	0.528	0.542
π_2	38848	20469	14523	12953	14698	32307	17939
ρ_2	1.81	2.09	1.88	2.05	2.29	1.80	1.91
π_3	39286	20815	14082	12604	14111	32772	18066
ρ_3	1.84	2.15	1.80	1.97	2.16	1.84	1.93
$\zeta = 0.5$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**	**TG6**	**TG7**
π_1	25940	13156	9209	8632	8976	21763	12021
ρ_1	0.846	0.947	0.823	0.961	0.968	0.798	0.871
π_2	42524	22284	15010	14381	15582	34736	19827
ρ_2	2.03	2.30	1.97	2.27	2.42	1.87	2.09
π_3	43723	22938	15089	13766	15281	34415	19132
ρ_3	2.11	2.39	1.99	2.13	2.35	1.84	1.98
$\zeta = 1$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**	**TG6**	**TG7**
π_1	30710	16115	11908	10385	10817	25689	15613
ρ_1	1.08	1.22	1.25	1.24	1.22	1.08	1.33
π_2	44326	23709	16958	15181	16945	37800	23449
ρ_2	2.01	2.26	2.20	2.27	2.49	2.07	2.49
π_3	44881	24017	16678	15280	16941	38191	22381
ρ_3	2.04	2.31	2.14	2.29	2.48	2.10	2.33

in traditional insurance practice (usually less than 50%). As shown in Table 3.4, relative to $\zeta = 0$, the increment of the strength of interdependence, excluding proportionality to the increment of the premiums, results in high premiums. Besides, MCS with limited sampled years produces results which are susceptible to the risk uncertainty, reflected by the high RLCs of the individual TGs.

The actuarial principle is designed to incentivize high defense coverage with reduced individual premiums. In the case group of high defense coverage, a significant reduction on the premiums can be observed in Tables 3.5. In both Tables 3.4 and 3.5, the sum of individual premiums estimated using π_3 is equal to that using π_2 with minor redistributed allocation. The RLCs increase along with the increased defense coverage, indicating that the expected losses decrease more than the premiums. The analysis shows that the individual premium is negatively correlated with the defense resource coverage and positively correlated with the strength of interdependence.

CHAPTER 4. A RELIABILITY-BASED COALITIONAL CYBER-INSURANCE DESIGN CONSIDERING CYBER VULNERABILITY

4.1 Introduction

Referring to Fig. 4.1(a), the typical cyber-physical configuration in power systems includes a control center, generation, substations, and the SCADA system interconnected by LAN. Here is a probable attack scenario. The potential intruder initiates a security game with the power system operator/defender by infiltrating the firewall. In this game, the intruder may profit from the ransoms paid by the defender. When the defender fails to pay the demanded ransom, the intruder who obtained the root privilege of the application servers in the SCADA system sends false commands to the relay to trip the breakers of the substations. As a result, the generation units and transmission lines are disconnected, causing load interruption and corresponding monetary loss of the TG.

4.2 Graphic Model for Assessing Cybersecurity

The cyber model includes vulnerability nodes connected by the networking links. The cyber model of network vulnerability can be represented by an attack graph of BN. BN is

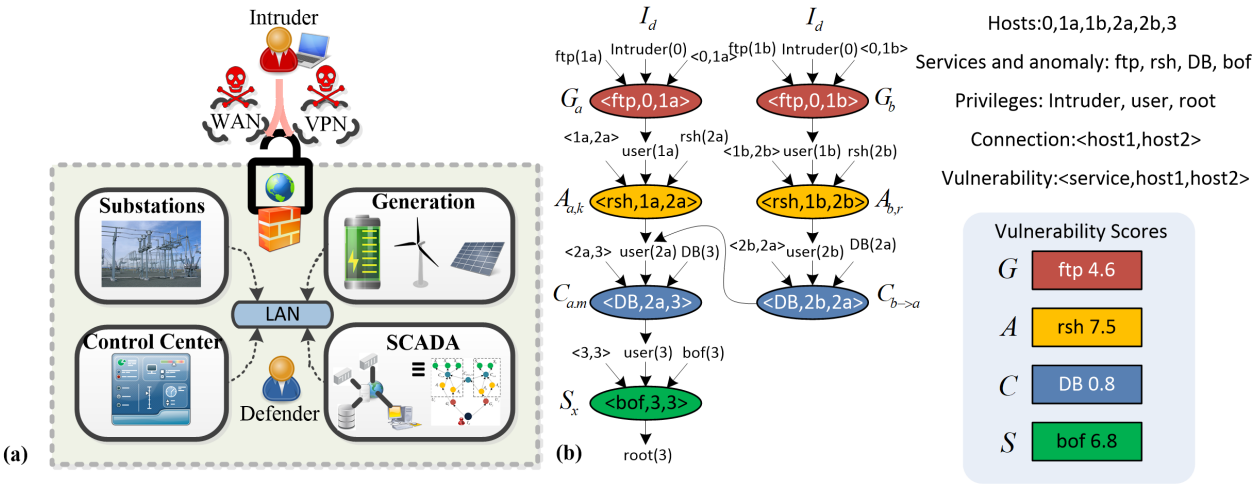


Figure 4.1: (a) Graph-based cyber-physical model considering network vulnerabilities. (b) Schematic BN-based attack graph for the cyber-vulnerability in the SCADA systems.

a probabilistic approach suited to estimate the combinational impact of the vulnerabilities and synthesize security metrics such as TTC [60], [61]. In cybersecurity assessment, attack graph is a stochastic modeling tool. The intruder targets on the root privilege to sabotage the server commanding a power system substation. To obtain the root privilege of the application server, the intruder needs to exploit n vulnerabilities. The vulnerability nodes are denoted by the ovals with colors corresponding to respective hierarchies. Connection provides a necessary link between two hosts through a vulnerability node. Privilege defines the allowable actions in the host. The intruder utilizes services to access the privilege via the connection. The intruder needs to meet three preconditions to complete a nodal vulnerability exploitation in the BN: Service ($\mathcal{S}_h$), Connection ($\mathcal{N}_h$), and Privilege ($\mathcal{P}_h$) assumed to be mutually independent.

As shown in *Definition 1*, the BTTC can be formulated using the BN-based attack

Definition 1: Bayesian Time-To-Compromise of the Substations

$$T_b = \frac{\Sigma_{v_h \in V} t_\beta(v_h) p(v_h \wedge c_h)}{p(c_h)} \tag{4.1}$$

Subject to:

$$t_\beta(v_h) = \begin{cases} t_\beta(|v|) & , v_h \in \{G, A, C\} \text{ (Definition 2)} \\ t_\beta(S) & , v_h \in S \text{ (Definition 3)} \end{cases} \tag{4.2}$$

$$p(v_h) = \frac{CVSS}{10} * U(0,1) \tag{4.3}$$

$$p(c_h|v_h) = \begin{cases} U(0.8,1) * 1_{\{c_h=T\}}, h = 1 \\ p(c_h|v_h \wedge (v_1 \vee ... \vee v_{h-1})), h \geq 2 \end{cases} \tag{4.4}$$

$$p(v_h \wedge c_h) = p(v_h) * p(c_h|v_h) \tag{4.5}$$

$$p(c_h) = \Sigma_{l=1}^{n} p(c_h|v_l) p(v_l) \tag{4.6}$$

graph and t_β of the respective vulnerability nodes. Denote $c_h = \mathcal{S}_h \wedge \mathcal{N}_h \wedge \mathcal{P}_h$ at each vulnerability v_h. The probability of exploiting the known or zero-day vulnerability v_h is $p(v_h)$. The conditional probability $p(c_h|v_h)$ is either determined by a random vulnerability that follows a uniform distribution or synthesized by a series of such vulnerabilities. The probability that the vulnerability v_h is exploited by the successful exploitation condition c_h is $p(v_h \wedge c_h)$, the product of $p(v_h)$ and $p(c_h|v_h)$. The BTTC is synthesized by further taking into account the BCT of all vulnerabilities from the intruder to the root privilege.

The BTTC evaluates the capability of respective substations to resist against the network adversary.

As shown in Fig. 4.1(b), to disrupt the substation operation, the intruder I_d Intruder(0) needs to compromise a series of vulnerability nodes $V = \{G, A, C, S\}$ to obtain the root privilege root(3): Gate node (G), Authentication node (A), Countermeasure node (C), Substation

node (S).

As shown in Fig. 4.1(b), to disrupt the substation operation, the intruder I_d Intruder(0) needs to compromise a series of vulnerability nodes $V = \{G, A, C, S\}$ to obtain the root privilege root(3): Gate node (G), Authentication node (A), Countermeasure node (C), Substation node (S). Feasible attack sequences are:

A1. Within a TG $I_d \rightarrow G_a \rightarrow A_{a,k} \rightarrow C_{a,m} \rightarrow S_x$

A2. Across different TGs $I_d \rightarrow G_b \rightarrow A_{b,r} \rightarrow C_{b \rightarrow a} \rightarrow C_{a,m} \rightarrow S_x$

CVSS comprises base score, temporal score, and environmental score that take a wide range of attack factors into account: confidentiality, integrity, availability, attack complexity, privileges required, exploit code maturity [62]. Services are designated with respective scores in CVSS, an open-access vulnerability evaluation system. For instance, file transfer protocol (ftp), remote shell service (rsh), and database server (DB), together with the anomaly of buffer overflow (bof), are implemented in the vulnerability nodes $V = \{G, A, C, S\}$. For the sake of brevity, interested readers are referred to [17], [19] for further descriptions.

4.2.1 Exploitation of Cyber-Vulnerability

Referring to Fig. 4.2, define t^* as the average time that the intruder spends in successfully exploiting the vulnerability. In [15], t^* was decomposed into three mutually exclusive stochastic processes whose mean times and probabilities are $\{t_1, t_2, t_3\}$ and $\{P_1, P_2, P_3\}$, respectively.

In Process 1, at least one exploit (readily exploitable vulnerability) is available to the intruder. Process 2 indicates at least one vulnerability is identified, while no exploit is

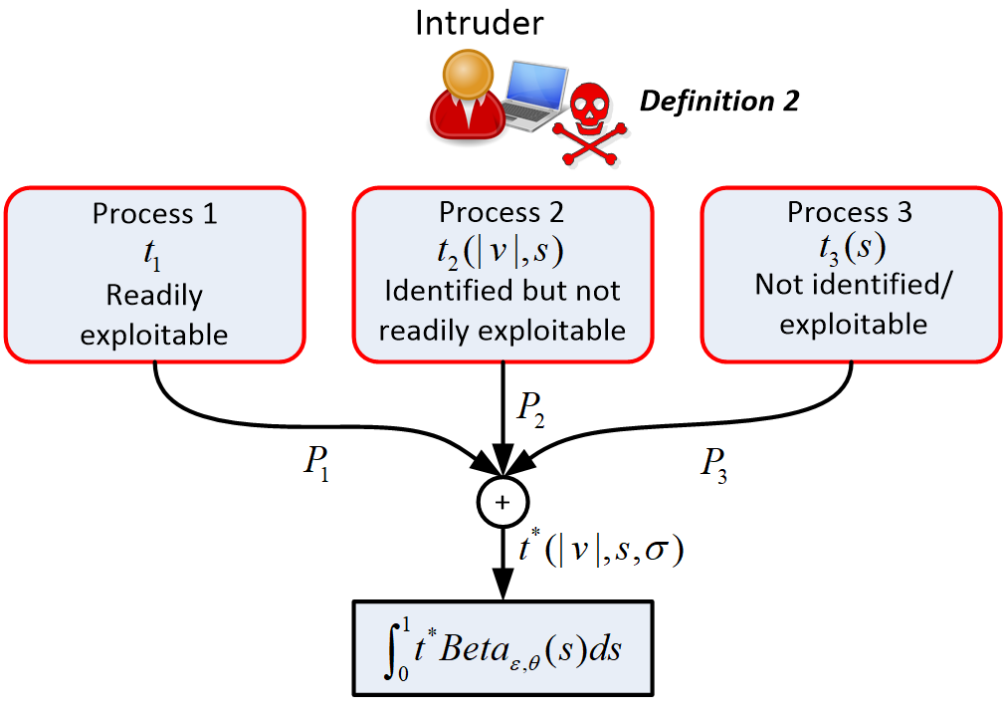


Figure 4.2: Block diagram of the processes estimating Beta Compromise Time (Definition 2).

available to the intruder. In Process 3, the intruder searches new vulnerability since no vulnerability can be exploited or identified by the intruder. One of the processes is active only when the other two are inactive. Note that the unidentified vulnerabilities may include, but not be limited to, eavesdropping a legitimate password through social engineering, obtaining a stolen password from an insider, and any coordination between the insider and the intruder.

In *Definition 2*, when calculating the stochastic metrics of these processes, a few variables should be taken into consideration: $|v|$ is the number of known vulnerabilities of the component; m is the number of available exploits; σ is the total number of vulnerabilities; $s \in [0, 1]$ is skill level factor; and E is the number of estimated tries, with auxiliary variables u and ξ. E is redefined in [16] to be a monotonically decreasing function with $|v|$. The

rationale for E is that less estimated tries are needed given more vulnerabilities.

Ultimately, various degrees of the skill level s curve-fitted by a Beta distribution are accounted for. The Beta Compromise Time (BCT) t_β over the distribution in exploiting the vulnerability is calculated with $\varepsilon = 1.5$ and $\theta = 2.0$ according to [16]. Interested readers are referred to [15],[16] regarding the selection of other constants. Since the cyber model preserves the flexibility for TGs to stipulate defense mechanisms, BCTs of the substation nodes are estimated in a different fashion, with details to be discussed in the next subsection.

4.2.2 Modeling of the Substation Attack Tree

The attack tree in Fig. 4.3 describes the attacks based on the combinational event sets that may result in substation failure [12], [17]. The defense mechanisms DM1-DM8 are the frontmost entries that safeguard the substations. In *Definition 3*, the defense coverage $p_{DC}(S)$ is the manageable resilience at each substation S. The relative strength of the DM is $p(DM_w)$, where η is the defense level, χ is the normalizing constant, and p_u is the randomness adjustment following a uniform distribution. Following this design, $p(DM_w)$ would lie in $[0, 1]$ and manifests η discrete levels of defense strengths against the cyber adversary.

Define e_{DM} as the exploits of the DMs. Since DMs are mutually independent, the probability that all/one of a set of DMs are attacked by the attack leaf L_j which is a logic gate. The logical AND L_j is conservatively triggered by the most robust DM. The logical OR L_j is aggressively triggered by the most vulnerable DM. The substation S is compromised if either of the failure goals (F_1, F_2) is activated by all the preceding attack leaves $\{L_j\}$.

In the next subsection, an algorithm for allocating the defense resources on the substa-

Definition 2: BCT Estimation (except Substation Nodes)

$$t_\beta(|v|) = \int_0^1 t^*(|v|, s, \sigma) * Beta_{\varepsilon,\theta}(s)ds \tag{4.7}$$

Subject to:

$$t^* = t_1P_1 + t_2P_2 + t_3P_3 \tag{4.8}$$

$$\begin{cases} P_1 &= 1 - e^{-|v|*\frac{m(s)}{\sigma}} \\ P_2 &= (1 - P_1)(1 - u) \\ P_3 &= 1 - P_1 - P_2 \end{cases} \tag{4.9}$$

$$\begin{cases} t_1 &= 1 \\ t_2 &= 5.8 * E(s, |v|) \\ t_3 &= (\frac{1}{f(s)} - 0.5) * 30.42 + 5.8 \end{cases} \tag{4.10}$$

$$\begin{cases} m(s) &= 83 * 3.5^{4s/2.7} - 82 \\ f(s) &= 0.145 * 2.6^{2s+0.07} - 0.1 \\ u &= (1 - f(s))^{|v|} \\ \bar{f} &= f(s) * |v| \end{cases} \tag{4.11}$$

$$\begin{cases} E(s, |v|) = E_1(s, |v|) + E_2(s, |v|) \\ E_1(s, |v|) = \xi(\lfloor \bar{f} \rfloor, |v|) * (\lceil \bar{f} \rceil - \bar{f}) \\ E_2(s, |v|) = \xi(\lceil \bar{f} \rceil, |v|) * (1 - \lceil \bar{f} \rceil + \bar{f}) \\ \xi(b, |v|) = \dfrac{b}{|v|} + \dfrac{b(|v| - b)!}{|v|!} * \bar{\xi} \\ \bar{\xi} = \Sigma_{t=2}^{|v|-b+1}[\dfrac{t(|v| - t + 1)!}{(|v| - b - t + 1)!(|v| - t + 1)}] \end{cases} \tag{4.12}$$

(a) Defense Mechanism (DM), Attack leaves(L), and Failure goals(F)

DM1	Configure LAN firewall
DM2	IP policy, filter rules and address rearrangment
DM3	Install intrusion tolerant system with backup capacity
DM4	Audit the user privileges to application server
DM5	Network analyzer, forensic tool, and traffic scanner
DM6	Digital token, certificate, and biometric verification
DM7	Data integrity check, security patch and anomaly record
DM8	Enact password policy: age, length, and character types
L1	Intercept TG command
L2	Duplicate substation information
L3	Gain the privilege of the targeted server
L4	Launch the active attack
L5	Exhaust the communication bandwidth
F1	Island the substation
F2	Trigger unexpected generation offline

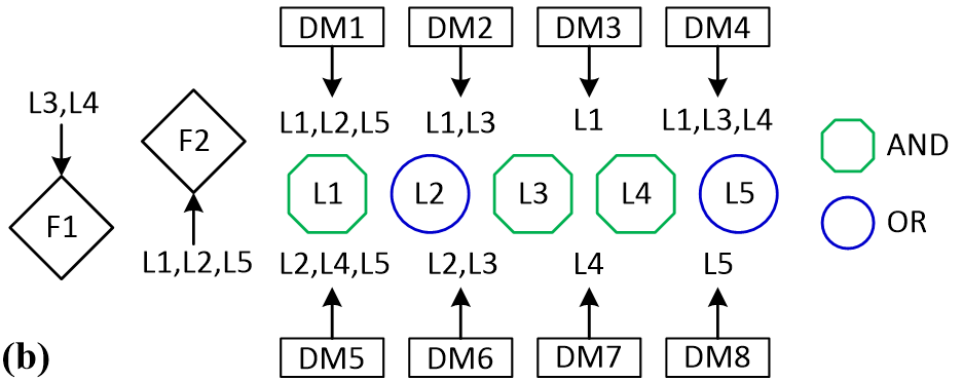


Figure 4.3: (a) Description of the (b) substation attack tree including defense mechanisms against attack leaves resulting in failure goal (Definition 3).

Definition 3: BCT Estimation of Substation Nodes

$$t_\beta(S) = \min(t_{\beta,F1}, t_{\beta,F2}) \tag{4.13}$$

Subject to:

$$\begin{cases} t_{\beta,F1} & = t_{\beta,L3} + t_{\beta,L4} \\ t_{\beta,F2} & = t_{\beta,L1} + t_{\beta,L2} + t_{\beta,L5} \end{cases} \tag{4.14}$$

$$t_{\beta,L_j} = \frac{t_\beta(v_j) p(L_j \wedge e_{DM})}{p(L_j)} \tag{4.15}$$

$$p(DM_w) = \chi * [\eta * p_{DC}(S)] + p_u \tag{4.16}$$

$$\begin{cases} p_{AND}(L_j \wedge e_{DM}) & = \Pi_w p(DM_w) \\ p_{OR}(L_j \wedge e_{DM}) & = 1 - \Pi_w [1 - p(DM_w)] \end{cases} \tag{4.17}$$

$$\begin{cases} p_{AND}(L_j) & = \max_w \{p(DM_w)\} \\ p_{OR}(L_j) & = \min_w \{p(DM_w)\} \end{cases} \tag{4.18}$$

tion nodes will be introduced.

4.2.3 Physical Model and Defense Resource Allocation

Applications of the game theory vary from reducing the variation of the local network load profile [63], managing the inter-grid energy exchange [64] to bargaining energy prices [65], among many others. Game-theoretic algorithms have been applied to distribute the security resources or alleviate possible load curtailments based on the cyber-physical network connection subject to cyberattack intrusion [66]. SSG is a hierarchical approach to arrange the security resources. Marginal strategy representation of the SSG can relieve the computational burden for the defense resource allocation [67].

Compact-form SSG algorithms have been developed to facilitate protection of the tar-

gets subject to attacks. Each TG conducts its own DRA optimization. In a two-player compact SSG, rival agents carry out strategies sequentially. The defender specifies its strategy preceding the best strategy selected by the intruder. Either player in the game can be an exact one entity or a group of entities. In the target set $\{\tau_x\}$, a target substation τ_x in service is either covered or uncovered by the defender. The respective payoff values are the expected values calculated based on the payoffs of covered and uncovered attacks, $\{U^c_{\alpha,\tau_x}, U^u_{\alpha,\tau_x}\}$ for the intruder α, and $\{U^c_{\beta,\tau_x}, U^u_{\beta,\tau_x}\}$ for the defender β. The payoffs can be assigned according to the criticality of the substation or the substation load. The defense coverage investment on the respective substation nodes corresponding to the target substations can be allocated up to the defense resource budget $\mathbf{M}$ that quantifies the security sparsity against the potential cybersecurity hazards experienced by the respective TGs.

Optimization 1 achieves optimal DRA by maximizing the defenders payoff [55] in each of the TGs. Benefitting from MILP formulation, DRA via *Optimization 1* can be completed in polynomial time. The TG operators can invest defense resource coverage $\mathcal{C} = \{p_{DC}(\tau_x)\}$ to individual substations based on the available security budget and the rank of criticality.

4.2.4 State Duration Sampling

The BTTC T_b quantifies the duration in which individual substations would be compromised. To emulate the randomness of the cyberattacks, the exponential variate for each substation τ_x is generated through a simple logarithmic operation. $T_{b,x}$ has exponential sample $\hat{T}_{b,x}$. Substituting into cumulative distribution function of the standard normal distribution Φ, a set of uniform variates can be obtained. In this chapter, λ sampled from

Algorithm 4.1: BTTC State Duration Sampling

Input: $P_{L,x}, P_{L,total}, \mu_\nu, U^c_{\beta,\tau_x}, U^u_{\beta,\tau_x}, U^c_{\alpha,\tau_x}, U^u_{\alpha,\tau_x}, \boldsymbol{M}, r$

Output: $\hat{T}_{b,x}$

function

  `/* Assign the defense coverage */`

  for *Each TG* q **do**

    for *Each target substation* x **do**

      Compute γ_x using (4.26)

      Compute the defender's payoff $U_\beta(\mathcal{C}, \tau_x)$:

      $\gamma_x\{p_{DC}(\tau_x)U^c_{\beta,\tau_x} + (1 - p_{DC}(\tau_x))U^u_{\beta,\tau_x}\}$

      Compute the intruder's payoff $U_\alpha(\mathcal{C}, \tau_x)$:

      $\gamma_x\{p_{DC}(\tau_x)U^c_{\alpha,\tau_x} + (1 - p_{DC}(\tau_x))U^u_{\alpha,\tau_x}\}$

    end

    Designate $\mathcal{C} = \{p_{DC}(\tau_x)\}$ using *Optimization 1*

  end

  `/* Estimate Beta Compromise Time */`

  Evaluate $t_\beta(|v|)$ using *Definition 2*

  Evaluate $t_\beta(C_S)$ using *Definition 3*

  `/* Sample substation state duration */`

  for *Each TG* q **do**

    $N_{cq} \leftarrow rN_t + \sqrt{1 - r^2}N_{nq}$

    `/*` $N_t, N_{n1}, ..., N_{ny} \sim N(0, 1), r \in [0, 1]$ `*/`

  end

  `/* Generate correlated set` $\{\lambda_x\} \sim U(\cdot)$ `*/`

  `/* Generate state duration sampling` $\hat{T}_{b,x}$ `*/`

  for *Each target substation* x **do**

    $\lambda_x \leftarrow \Phi(N_x)$

    Calculate $T_{b,x}$ using *Definition 1*

    $\hat{T}_{b,x} \leftarrow -T_{b,x} \ln \lambda_x$

  end

  return $\hat{T}_{b,x}$

end

Optimization 1: DRA via Maximal Defender Payoff
Input: $U^c_{\beta,\tau_x}, U^u_{\beta,\tau_x}, U^c_{\alpha,\tau_x}, U^u_{\alpha,\tau_x}, \boldsymbol{M}$
Output: $\{p_{DC}(\tau_x)\}$
$/^*\boldsymbol{M} = \{M_q\}^*/$

$$\max\ d \tag{4.19}$$

Subject to:

$$a_{\tau_x} \in \{0, 1\} \tag{4.20}$$

$$\Sigma_{\tau_x} a_{\tau_x} = 1 \tag{4.21}$$

$$p_{DC} \in [0, 1] \tag{4.22}$$

$$\Sigma_{\tau_x} p_{DC}(\tau_x) \leq M_q \tag{4.23}$$

$$d - U_\beta(\mathcal{C}, \tau_x) \leq (1 - a_{\tau_x})Z \tag{4.24}$$

$$0 \leq k - U_\alpha(\mathcal{C}, \tau_x) \leq (1 - a_{\tau_x})Z \tag{4.25}$$

where $d \geq U_\beta(\mathcal{C}, \tau_x), \forall \tau_x$ and Z is an arbitrarily large number.

the uniform distribution is replaced by a sample extracted from a correlated set $\{\lambda_x\}$, with correlation coefficient r. The same set produces the correlated loss pattern in the respective TGs.

Algorithm 4.1 summarizes the procedure of state duration sampling by evaluating the BTTC over cyber vulnerabilities. To indicate the load criticality of the substation τ_x, a substation impact index is in place as a weight coefficient:

$$\gamma_x = (1 + \frac{P_{L,x}}{P_{L,total}})^{\mu_\nu} \tag{4.26}$$

where

$P_{L,x}$	Load at the substation τ_x
$P_{L,total}$	Total load in the system
μ_ν	Number of adjacent substations

Following *Optimization 1*, BCT of the vulnerability nodes can be synthesized into BTTCs according to *Definitions 2,3*. BTTCs serve as mean values in state duration sampling.

4.2.5 Reliability Assessment

Based on the respective strengths against cyberattacks, a stochastic $\hat{T}_{b,x}$ sampled in **Algorithm 1** is assigned to individual substations, determining the online generation capacity. Specifically, if the intruder compromises the root privilege of the substation server, a false tripping command is assumed to be sent to the substation relays, leading to generation offline. For further clarification, *Optimization 2* is used to explain the minimization of aggregate substation load loss $\Sigma_x \boldsymbol{K_x}$ subject to cybersecurity threats in each observed time step ν. In each substation server, an enabling function $EN(\cdot)$ is implemented to set the upper bound $EN(\boldsymbol{\tau_x}) * \boldsymbol{G_{cap}}$ of the generation $\boldsymbol{G}$ by checking whether the time step ν lies in the interval defined by $\hat{T}_{b,x}$, returning 1 if true and 0 otherwise. In addition, the feasible load curtailment $\boldsymbol{K_x}$ and the power flow must never exceed the load capacity $\boldsymbol{D_{cap}}$ and the transmission thermal limit $\boldsymbol{F_{cap}}$, respectively.

Finally, the equality constraint of energy conservation between generation supply and load demand should be met at all times. In the following section, the cyber-insurance premium devised for different TGs and the indemnity mechanism will be presented.

Optimization 2: Reliability-based Load Curtailment Estimation

$$\min\{\Sigma_x \boldsymbol{K}_x\}_\nu \tag{4.27}$$

Subject to:

$$\boldsymbol{B\theta} + \boldsymbol{G} + \boldsymbol{K_x} = \boldsymbol{D_{cap}} \tag{4.28}$$

$$|\boldsymbol{F}| \leq \boldsymbol{F_{cap}} \tag{4.29}$$

$$\boldsymbol{0} \leq \boldsymbol{K_x} \leq \boldsymbol{D_{cap}} \tag{4.30}$$

$$\boldsymbol{0} \leq \boldsymbol{G} \leq EN(\boldsymbol{\tau_x}) * \boldsymbol{F_{cap}} \tag{4.31}$$

$$EN(\boldsymbol{\tau_x}) = \mathbf{1}_{\{\nu \in \bar{T}_{b,x}\}} \tag{4.32}$$

4.3 Design of Cyber-Insurance Premium

Cyber-insurance is envisioned as a promising financial instrument for the TGs against unpredictable losses. The cyber insurance is in place as a safety net for the power system operators who could otherwise suffer unpredictable monetary losses due to blackouts or load interruption induced by consequential cyberattacks. To incorporate the financial impact of cyberattacks on the economically related entities, it is essential for the premium package to encompass the statistics across the insured entities. However, implementing cyber insurance is difficult in practice due to a relatively small insured pool with large indemnities. Thus, novel insurance principles customized for the cyber-insurance are proposed to resolve the dilemma. A desirable cyber insurance design should allow sufficient total premiums to substantially, if not completely, cover all claims and fairly distribute premiums among the insureds.

To this end, two risk measures, VaR and TVaR, are introduced below. Specifically, VaR

measures the riskiness of a portfolio through percentile, which is defined as follows:

$$VaR_{\varpi}(\mathcal{L}) = \inf\{l : P(\mathcal{L} > l) \leq \varpi\}, \varpi \in (0,1) \tag{4.33}$$

TVaR measures the riskiness of a portfolio through the average of the worst $100\varpi\%$ scenarios. It is defined as follows:

$$TVaR_{\varpi}(\mathcal{L}) = \frac{1}{\varpi}\int_0^{\varpi} VaR_p(\mathcal{L})dp \tag{4.34}$$

Intuitively, TVaR is the average of all the possible values of L that are greater than VaR, so it is greater than VaR. In other words,$TVaR_{\varpi}(\mathcal{L}) = VaR_{\varpi}(\mathcal{L})$, TVaR is a more conservative risk measure than VaR.

Denote the total losses by $\mathcal{L}^* = \Sigma_q \mathcal{L}_q$. Using the risk measure TVaR, the total premium can be evaluated as:

$$TVaR_{\varpi}(\mathcal{L}^*) = \frac{1}{\varpi}\int_0^{\varpi} VaR_p(\mathcal{L}^*)dp, \forall p \leq \varpi \tag{4.35}$$

After the total premium is determined, individual premiums can be allocated to the individual TGs. With the total premium $TVaR_{\varpi}(\mathcal{L}^*)$, the insolvency which is the probability that the total losses exceed the total premium, is controlled at the level lower than ϖ.

A TCE premium design π_1 [24] to allocate $TVaR_{\varpi}(\mathcal{L}^*)$ based on individual contributions to the total TVaR, is defined as:

$$\pi_1(\mathcal{L}_q) = E[\mathcal{L}_q | \mathcal{L}^* > VaR_{\varpi}(\mathcal{L}^*)] \tag{4.36}$$

when $\mathcal{L}^*$ is continuous, it can be easily shown that $\Sigma_q \pi_1(\mathcal{L}_q) = TVaR(\mathcal{L}^*)$. Although π_1 is advantageous in controlling insolvency risk, it results in a high premium to indemnity ratio which thus jeopardizes its practicability. The coalitional platform among the TGs can

be introduced as a probable alternative to resolve the dilemma. No third-party insurer is involved in the coalition, as each TG who opts to participate in the coalition is both the insurer and the insured [68].

A coalitional premium π_2 can be defined as follows:

$$\pi_2(\mathcal{L}_q) = \varphi_q \Sigma_{k=1}^{y-1} \delta_{q,k} \psi(\Pi_q + (k-1)\bar{\Pi}_{-q}) \tag{4.37}$$

where y is the number of TGs in the coalition; φ_q is the occurrence probability of the loss event which is a ratio of the number of time steps with loss occurrence to the total sampled time duration in the reliability assessment; $\delta_{q,\varsigma}$ is the probability that the TG q among ς TGs submits the claim; Π_q is the claim of TG q; and $\bar{\Pi}_{-q} = \frac{(\Sigma_{k=1}^{y}\Pi_k)-\Pi_q}{y-1}$ is the average of all the claims except for that of TG q.The coalitional premium differs in each claim scenario. ς is the number of TGs which submit their claims. When ς is larger, payments toward claims from other TGs weigh more in the individual premiums.

Define the indemnity as $\Gamma_q = \Pi_q + (\varsigma - 1)\bar{\Pi}_{-q}$ and commitment as $\mathbb{C}_q$ of the TG q, respectively. The scaling function $\psi(*)$ in $\Pi_2(\mathcal{L}_q)$ ensures the indemnity sum $\Sigma_{q\in\sigma}\Gamma_q$ never exceeds the commitment sum $\Sigma_{q\in(y-\sigma)}\mathbb{C}_q$:

$$\Gamma_q^{\psi} = \psi(\Gamma_q) = \begin{cases} \Gamma_q, when\ \Sigma_{q\in\sigma}\Gamma_q \leq \Sigma_{q\in(y-\sigma)}\mathbb{C}_q \\ \\ \frac{\Sigma_{q\in(y-\sigma)}\mathbb{C}_q}{\Sigma_{q\in\sigma}\Gamma_q}, else \end{cases} \tag{4.38}$$

where $\Sigma_{q\in\sigma}\Gamma_q \leq \Sigma_{q\in(y-\sigma)}\mathbb{C}_q$ ensures the budget sufficiency.

Taking advantage of the abundant loss reimbursement to the potential claims in the TCE premium, the coalitional premium estimates the respective commitment values of TGs by the TCE premiums, and the claims are set to be the respective expected losses in the

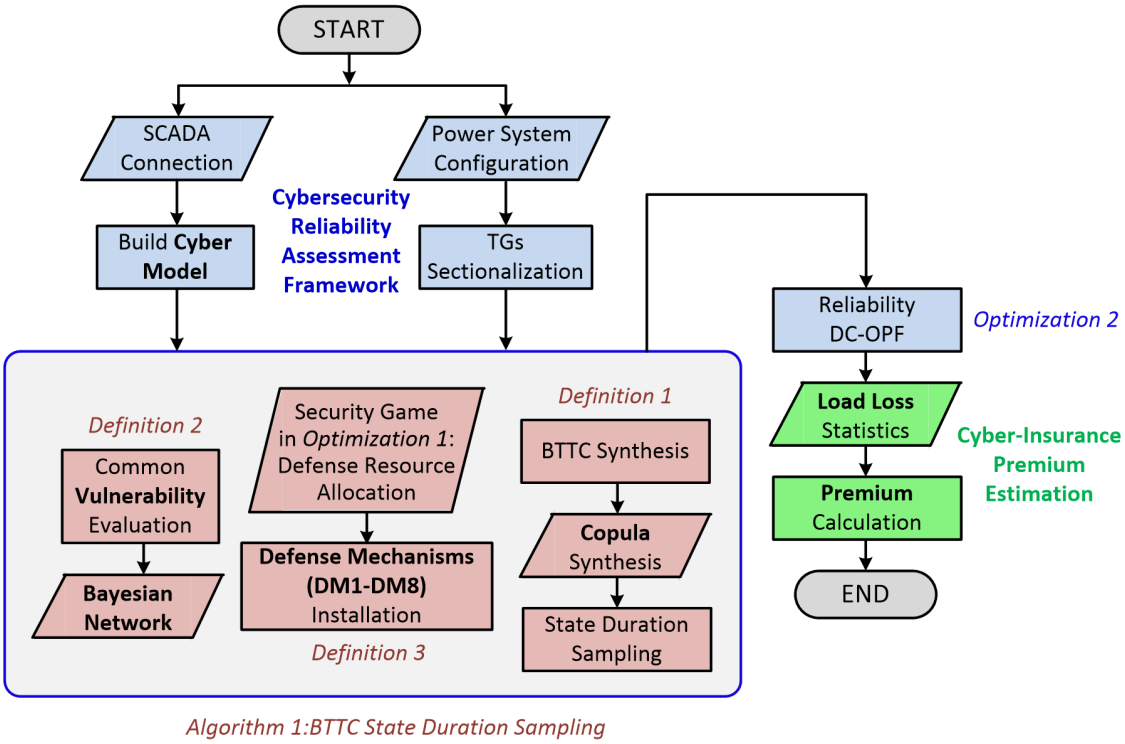


Figure 4.4: Flowchart of the proposed reliability-based cyber-insurance model considering cyber vulnerability, comprising (I) Cybersecurity-reliability assessment framework, and (II) Cyber-insurance premium estimation.

TGs:

$$\mathbb{C}_q = \pi_1(\mathcal{L}_q), \Pi_q = E[\mathcal{L}_q] \tag{4.39}$$

The notion of using π_1 as the commitments of π_2 is that π_2 based on a crowdfunding model serves as a remedy of π_1 which deeply penalizes the TGs with heavy-tailed loss distributions. π_2 allows respective TGs to submit the commitments and claims to the coalition. The very motivation of the coalitional premium application is to encourage the risk aversion by reduced premiums for all. The fairness of π_2 is justified by the even distribution of the premiums. In some cases, the indemnities of some TGs may even be allowed to exceed the

premiums without violating the budget sufficiency practice, which will be discussed in the case studies. Despite offering reduced premiums, π_2 is cautiously tailored so that the indemnity sum can never exceed the commitment sum, in which the individual indemnities would simply be scaled down by the ratio of the foregoing sums.

To achieve budget sufficiency, the indemnity formed by the claims filed by a group of TGs should never exceed the total commitment of other TGs in the coalition. Note that multiple sets of coalition which satisfy the budget sufficiency may exist. Selection of the coalition is on the discretion of participating TGs. As a rule of thumb, more affordable premiums are desirable so long as it can still cover the claims from the TGs. In other words, the coalition with the lowest total premium is selected.

Fig. 4.4 depicts the proposed coalitional cyber-insurance model. Stochastic evaluation of the BTTC, state duration sampling, and reliability assessment are shown. Application of the load loss statistics from reliability assessment to cyber-insurance premium computation is introduced. Further details are given in the following.

(I) cybersecurity-reliability assessment framework introduced in Section II. The CPS under study is constructed based on the graph-based cyber model of the SCADA system and the sectionalized physical power system configuration. BTTCs of the substations are composed of BCTs of the cyber nodes synthesized by the Bayesian Network of the vulnerability analysis (*Definition 2*) and BCTs of the game-inspired DRA optimization (*Definition 3, Optimization 1*). With a novel state duration sampling method considering the correlated copula of TGs generated using **Algorithm 1**, reliability-assessment-oriented DC-OPF is conducted to obtain temporal load curtailment statistics of the TGs.

(II) cyber-insurance premium estimation presented in Section III. Developed

to handle the load loss statistics of TGs, cyber-insurance premiums are computed by a novel coalitional premium design which takes the interdependence of TGs and the fairness and affordability of the premiums into account. The effectiveness of the proposed cybersecurity assessment framework and the merit of the proposed premium settings in various degrees of TGs' interdependence will be validated in the following section.

4.4 Case Studies and Discussion

4.4.1 Settings of the simulation

In case studies, the physical impact of cyberattacks is reflected by the load losses in reliability assessment. The crucial interdependence of cyber and physical aspects lies in the server of the SCADA system. If the root privilege of this server is obtained by the intruder, then malicious commands may be sent to trip protection relays and cause generation off-line, resulting in physical load losses.

The effectiveness of defense resource allocation is examined by case studies subject to tight and abundant budgets. The security budget m only suffices to partially cover substations. For example, 20% security budget is sufficient to cover one-fifth of the substations. In the scenarios of LDC and HDC, the corresponding available security budgets are set to be 20% and 80%, respectively.

The environment to validate the proposed coalitional cyber-insurance framework is the IEEE Reliability Test System (RTS-96). One-line diagram of the sectionalized RTS-96 is illustrated in Fig. 4.5, with details listed in [59]. The test system is divided into 3 areas

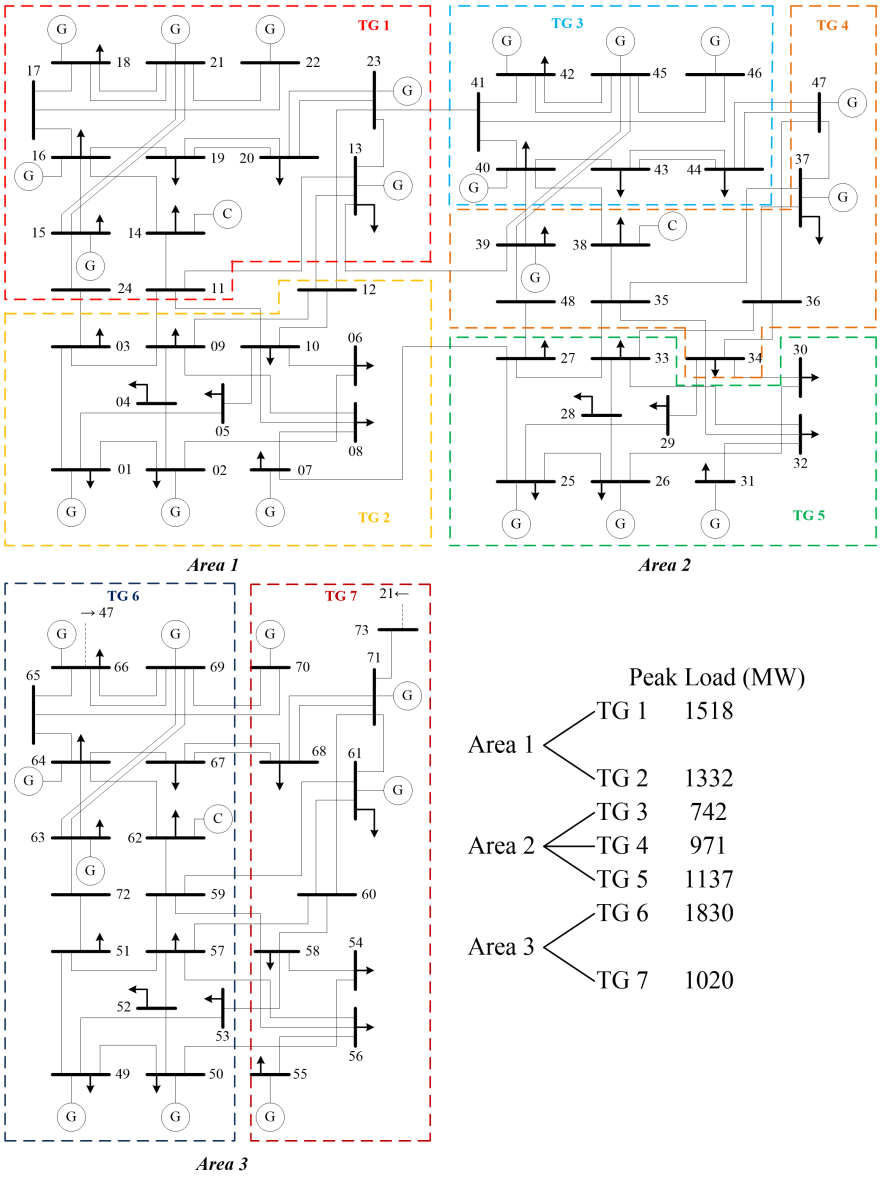
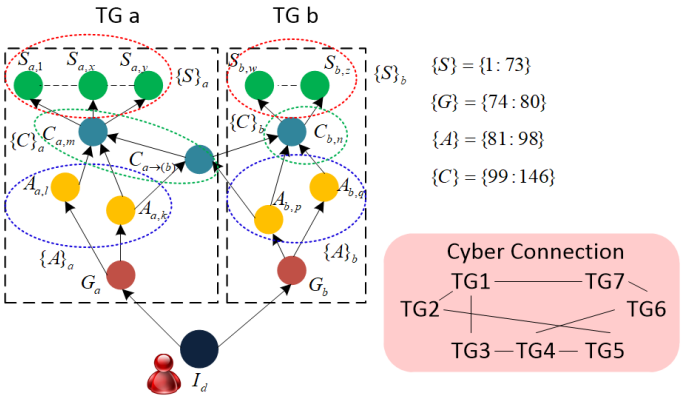


Figure 4.5: IEEE Reliability Test system 96 (RTS-96) and associated TGs.



Node(s)	TG1	TG2	TG3	TG4	TG5	TG6	TG7
$\{S\}$	$\{S\}_1$	$\{S\}_2$	$\{S\}_3$	$\{S\}_4$	$\{S\}_5$	$\{S\}_6$	$\{S\}_7$
G	74	75	76	77	78	79	80
$\{A\}$	81-83	84-86	87,88	89,90	91-93	94-96	97,98
$\{C\}$	99-107	108-113	114-117	118-122	123-129	130-139	140-146

Figure 4.6: Hierarchical vulnerability nodes of the cyber model in IEEE RTS-96.

including 7 TGs connected by 6 inter-area lines. No TG operates across the areas. In Area 1, TGs 1-2 are located. TGs 3-5 are situated in Area 2, and TGs 6-7 are located at Area 3. Peak load capacities are also shown in Fig. 4.5.

The proposed cyber model can be viewed as an attack net whose branches can be extracted as respective attack graphs of the substations. The cyber model of the SCADA system developed for the IEEE RTS-96 is shown in Fig. 4.6, with all feasible routes identified by a DFS algorithm [69]. Case studies are conducted using the SMC method sampling over 500 years with hourly time steps, where expected values of reliability worth are:

$$ERW = E[\mathcal{L}] = \Sigma_{\underline{\Omega}} K_{\Omega} W(D_{\Omega}) \quad (\$/yr) \tag{4.40}$$

The load loss correlation matrices are demonstrated in Fig. 4.7. We would like to observe the Pearson correlation between each of the two TGs. Note that the diagonal entries

are always 1's, which do not carry information. When $r = 0$, the correlation entries are mostly close to 0 with those belonging to TGs in the same area having slightly higher values, representing the impact induced by physical connection. As r increases to 0.5, the correlations range around 0.35. At LDC, the correlations can go as high as 0.78. In general, each TG at LDC has slightly higher correlation values than the same TG at HDC. The effectiveness of the copula is thus validated.

Figs. 4.8 and 4.9 illustrate the expected reliability worth, Standard Deviations SDs, and CoVs subject to LDC and HDC. CoV is a dimensionless ratio of the SD to the expected value. The effectiveness of DMs is validated by the fact that the expected losses of TGs monotonically decrease as the available security budget increases.

The trend that the expected losses increase with the correlation can also be observed. Since SDs are close to the expected losses, CoVs remain flat across the TGs within the range of [0.86 1.18]. With the obtained monetary loss statistics, the insurance premium can be calculated accordingly. In the next subsection, premium estimation according to the insurance principle will be demonstrated and discussed. We would like to find if the premiums which sample the tail risks capture the same trend as demonstrated by the loss expectation.

4.4.2 Estimation of the Premium Design

In the cyber-insurance framework, respective premiums of TGs estimated by marginal statistics of the loss distribution. Due to the interconnection of power grids across the TGs,

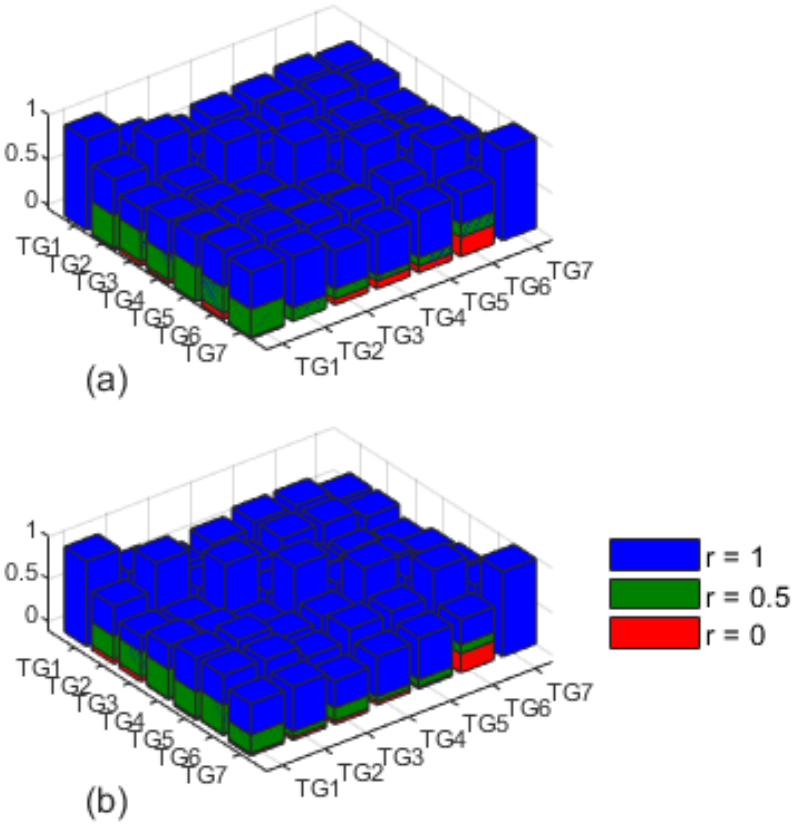


Figure 4.7: Load Loss correlation matrices of the TGs (a) at LDC (b) at HDC varied with correlated copulas.

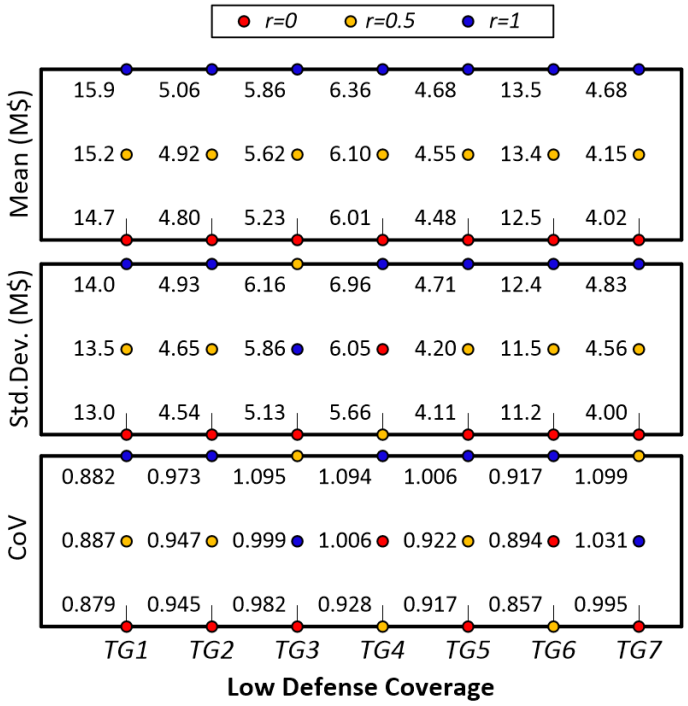


Figure 4.8: Expected Values (M$), Standard Deviations (M$) and Coefficients of Variation of Monetary Loss in the TGs at LDC.

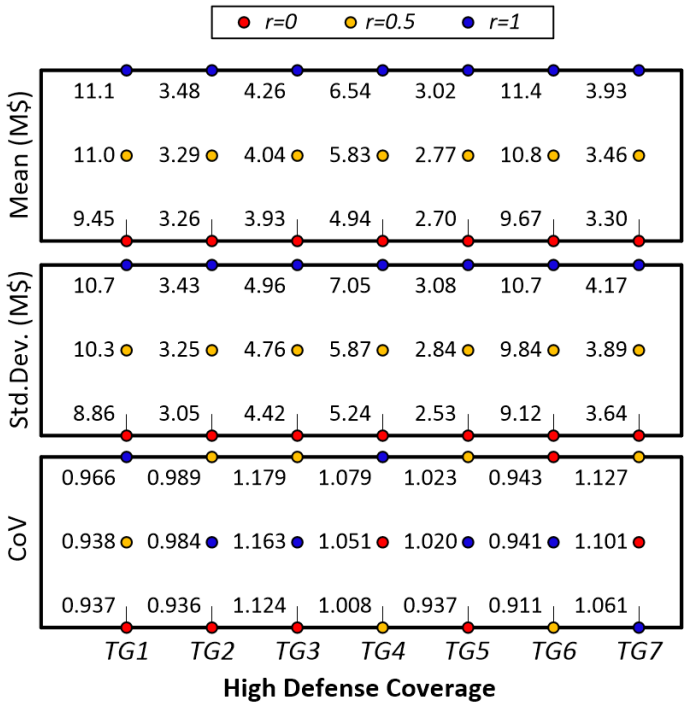


Figure 4.9: Expected Values (M$), Standard Deviations (M$) and Coefficients of Variation of Monetary Loss in the TGs at HDC.

Table 4.1: Actuarial Insurance Premiums (M$) of the TGs at LDC

$r = 0$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**	**TG6**	**TG7**
π_1	45.4	16.1	18.5	22.8	14.8	41.8	14.7
ρ_1	2.09	2.35	2.54	2.79	2.29	2.35	2.65
π_2	13.1	9.51	9.55	9.66	9.43	12.2	9.07
ρ_2	-0.11	0.98	0.83	0.61	1.10	-0.03	1.26
$r = 0.5$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**	**TG6**	**TG7**
π_1	49.5	17.1	22.5	20.4	15.1	41.6	17.2
ρ_1	2.26	2.47	3.01	2.35	2.31	2.10	3.14
π_2	14.3	10.5	10.4	11.0	10.5	13.8	9.79
ρ_2	-0.06	1.13	0.85	0.80	1.30	0.03	1.36
$r = 1$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**	**TG6**	**TG7**
π_1	50.0	17.4	21.1	26.4	16.8	44.9	17.4
ρ_1	2.14	2.43	2.60	3.15	2.59	2.33	2.72
π_2	14.7	10.7	10.8	10.6	10.4	13.7	10.3
ρ_2	-0.07	1.11	0.85	0.67	1.23	0.02	1.21

Table 4.2: Actuarial Insurance Premiums (M$) of the TGs at HDC

$r = 0$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**	**TG6**	**TG7**
π_1	32.7	10.9	16.4	18.7	8.43	35.1	13.5
ρ_1	2.46	2.35	3.18	2.75	2.12	2.63	3.08
π_2	9.37	7.22	7.09	7.65	7.12	9.36	6.92
ρ_2	-0.01	1.21	0.80	0.53	1.64	-0.03	1.09
$r = 0.5$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**	**TG6**	**TG7**
π_1	37.1	11.2	17.8	21.3	10.5	35.2	14.5
ρ_1	2.37	2.41	3.42	2.66	2.79	2.26	3.20
π_2	10.6	7.82	7.59	8.58	7.45	10.6	7.49
ρ_2	-0.04	1.37	0.88	0.47	1.69	-0.02	1.17
$r = 1$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**	**TG6**	**TG7**
π_1	38.9	12.4	18.9	26.1	11.1	37.9	15.1
ρ_1	2.50	2.55	3.44	3.00	2.68	2.34	2.84
π_2	11.0	8.23	8.04	9.06	8.01	11.1	8.24
ρ_2	-0.01	1.36	0.89	0.38	1.65	-0.02	1.09

the premiums should be allocated by synthesizing loss distribution across the TGs. A major motivation for the TGs to engage in the cyber-insurance is to alleviate the unexpected losses resulting from the cybersecurity threats.

The premiums are designed to account for the strength and peak load capacity varied by TGs. Although the premium design π_1 (TCE Premium) guarantees the loss coverage, the estimated premiums are remarkably higher than the expected losses. The low cost-effectiveness may discourage the TGs from participation.

To alleviate the financial burden of TGs, a novel premium package π_2 (termed Coalitional Premium) is designed using the crowdfunding concept. In this subsection, π_1 and π_2 are estimated according to the same set of loss distributions of TGs. Given a potential loss $\mathcal{L}_q$, RLC ρ that further highlights the affordability of the premium relative to the risk expectation is defined as follows:

$$\rho(\mathcal{L}_q) = \pi(\mathcal{L}_q)/E[\mathcal{L}] - 1 \tag{4.41}$$

where $\rho(\mathcal{L}_q) > 0, \forall q$ guarantees budget sufficiency. While positive RLC provides some margin to cushion against uncertainty, we will show majority of the participating entities provide safety-net margins to cover outliers with negative RLC according to the proposed insurance principle. To provide a viable insurance product, the RLC in the market is usually set relatively low.

The premiums collected from TGs is used as the budget for indemnities. In Table 4.1, ρ_1 ranges from 2.09 to 3.15. Higher ρ_1 is caused by heavy tails of the loss distribution. On the contrary, ρ_2 is dispersed in $[-0.11\ 1.36]$, mostly without exceeding 1. Note that a few TGs with slightly negative RLCs (TG1 and TG6) are tolerable for the coalition which gains

remarkably wider positive margins from the premiums of other TGs. In other words, the total coalitional premium still suffices to cover the claimed total potential losses given the insurance pool. In addition, π_2 also distributes the risks more uniformly than π_1, making the coalition a compelling insurance model. In Table 4.2, premiums are reduced at HDC, and π_2 still serves as a more affordable option, with ρ_2 being lower than 1.70.

The commitment term $\mathbb{C}_q$ can be flexibly replaced so long as the budget sufficiency still holds. The pattern of ρ_2 agrees with the more uniformly distributed π_2 across the TGs. While π_1 guarantees the monetary coverage of the losses by substantial margins at the cost of affordability, π_2 proposed in this chapter imposes lower financial threshold and fair premium distribution for the TGs. π_1 is more advantageous for thin tail distributions, while π_2 is more cost-effective in high risk uncertainty. The tradeoff between the two premium designs can be made based on the preference of individual practitioners.

CHAPTER 5. A NOVEL MUTUAL INSURANCE MODEL AGAINST CYBER RISKS IN POWER SYSTEMS DEPLOYING SMART TECHNOLOGIES

5.1 Introduction

A goal of this chapter is to gauge the risk of cyberattacks on the individual TGs to determine economical insurance pricing strategies. Fig. 5.1 conveys the proposed mutual insurance framework as multiple steps: (a) The power system configuration under study should be segmented according to the TGs ownership. (b) Within respective TG substations, smart monitoring and server job assignment are enforced to enhance the substation reliability subject to cyberattacks. (c) Accounting for the cyber connection across the TGs, an ENM is established to stochastically evaluate the long-term impact of cyberattacks. (d) Reliability-based optimal power flow is conducted to estimate the load loss profiles of respective TGs. (e) The insurance premium of each TG is computed based on the corresponding marginal distribution of the loss.

5.2 Proposed Epidemic Cyber-physical System Model

Fig. 5.2 illustrates the attack graph of the proposed ENM. The vulnerability v_h is denoted as a colored oval VUL. In the proposed ENM, two types of anomalies, ROB and

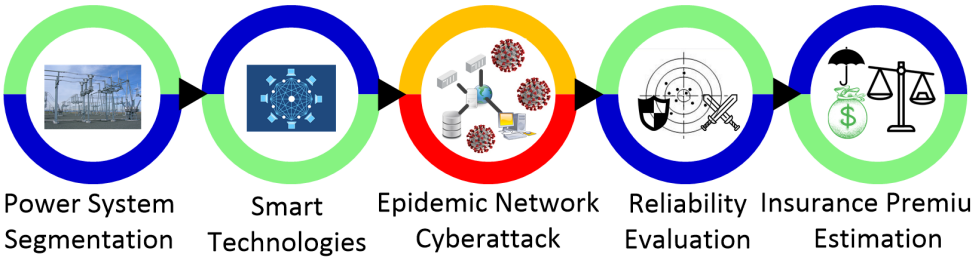


Figure 5.1: The steps in developing the proposed cybersecurity mutual insurance model.

DoS, are considered. ROB attack decrypts the control centers server privilege by iterating queries to a control server. DoS attack on the substation server is triggered by unauthenticated clients issuing specially crafted messages. The successful exploitation condition of vulnerability v_h occurs when the server privilege is obtained by the attacker, denoted as c_h.

Vulnerability scores are determined by CVSS comprising the base score, temporal score, and environmental score that take a wide range of attack-related factors into account, including confidentiality, integrity, availability, attack complexity, privileges required, and exploit code maturity [62].

To start the attack on the q^{th} TG, the attacker firstly needs to compromise the control center CC_q. Specifically, the attacker deploys anomaly ROB(1) to gain access to the server privilege $user(1)$ of CC_q by exploiting $< 0, 1 >$. Once CC_q is compromised, adjacent $< 1, 2 >$ of the substation $S_{q,1}$ can be exploited in a similar manner. Vulnerabilities in cascade are exploited sequentially. In Fig. 5.2, total 3 feasible attack routes can be observed:

A1. $CC_q \rightarrow S_{q,1} \rightarrow S_{q,2c}$

A2. $CC_q \rightarrow S_{q,1} \rightarrow S_{q,2b}$

A3. $CC_q \rightarrow S_{q,1} \rightarrow S_{q,2a} S_{q,3a}$

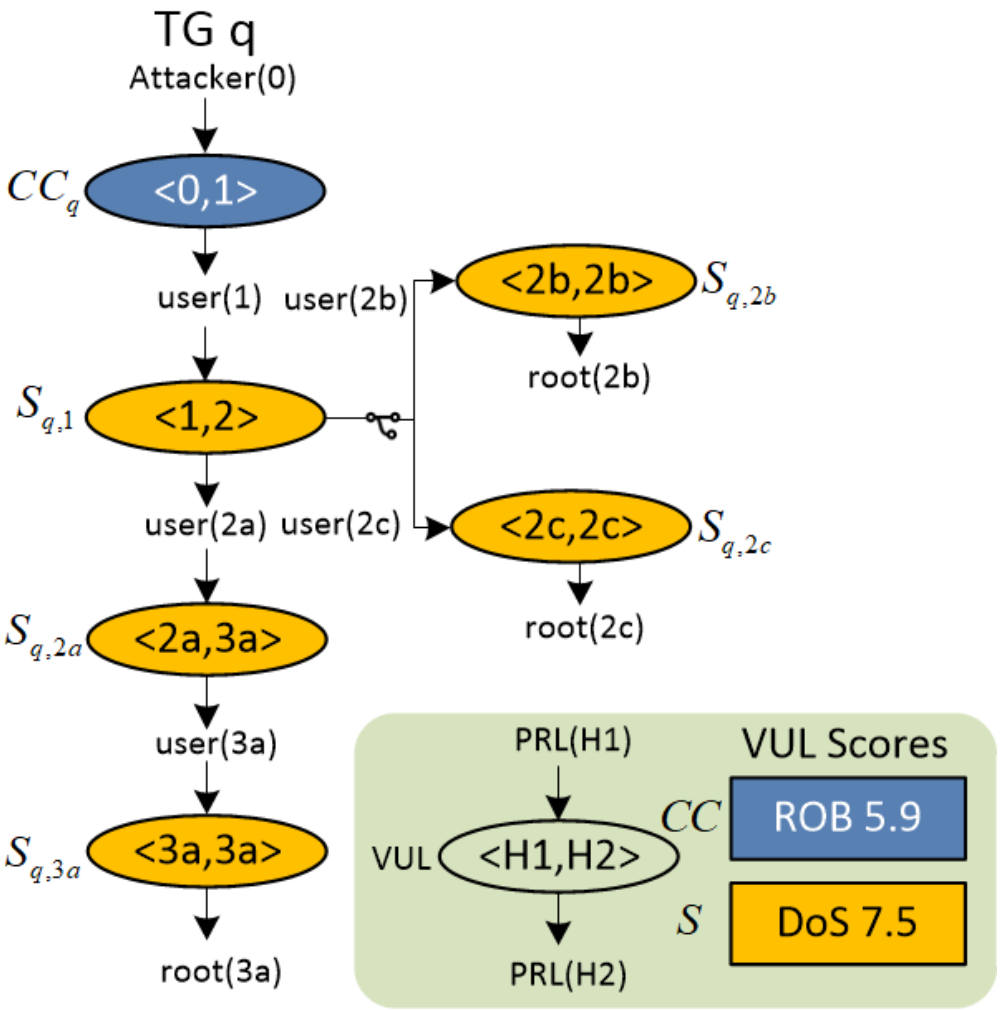


Figure 5.2: Attack graph of the proposed Epidemic Network Model.

In a physical sense, exploiting the vulnerability means the attacker breaches the server firewall to gain the server privilege to manipulatively command the substation. To compromise a substation server, its corresponding vulnerability and all preceding vulnerabilities must be exploited in the first place. After the substation server is compromised, the attacker may send counterfeit commands to the protective relays to disconnect the major substation IED from grid operations.

A security metric used extensively in reliability assessment is the SCT T_c. In Definition 1, T_c quantifies the time taken by the attacker to bring the substation down. Considering the attack graph, T_c is logically synthesized with a BN [60]. The SCT T_c is synthesized based on the individual sojourn times t_s of the vulnerabilities v_h. t_s is positively correlated to T_c and the overall system reliability. The smart technologies being considered in this work including smart monitoring [70] and job thread assignment [71] will be introduced in the subsequent subsection. In the job assignment, t_s corresponds to the memory thread resource in the cyber-physical elements assigned to the operational task. In smart monitoring, the CPS elements deploy preventive and corrective measures which boost substation security. The probability of exploiting vulnerability v_h depends on its score $\varsigma(v_h)$. The conditional probability $p(c_h v_h)$ can be determined by the vulnerability v_h and all the preceding vulnerabilities. The total probability of successful exploitation $p(c_h)$ is the summation of $p(v_h \wedge c_h)$, which is the product of $p(v_h)$ and $p(c_h v_h)$.

The cyber epidemic model in this chapter is initiated by a malicious attack on respective TGs, whose mathematical model is conveyed in Definition 2. The cyber epidemic model that infects a vulnerability node may stochastically spread to an adjacent vulnerability node set ζ. State sequence of a specific substation is determined by the infection time vector $\overrightarrow{T}_{epi}$

Definition 1: Epidemic Substation Compromise Time

$$T_c = \frac{\Sigma_{v_h \in V} t_s(v_h) p(v_h \wedge c_h)}{p(c_h)} \tag{5.1}$$

Job Assignment:

$$t_\beta(v_h) = \begin{cases} t_S(J_1, \lambda, \mu) = \frac{1}{\lambda} \\ t_S(J_2, \lambda, \mu) = \frac{1}{\lambda} + \frac{1}{2\lambda(1-p_1)} \\ t_S(J_3, \lambda, \mu) = \frac{1}{\lambda} + \frac{1}{2\lambda(1-p_1)} + \frac{1}{2\lambda(1-p_1)} + \frac{1}{3\lambda(1-p_1)(1-p_2)} \end{cases}, \tag{5.2}$$

$$\begin{cases} p_1 = \Pr[Y_1 > \mathbb{U}] & = \frac{\mu}{\mu+\lambda} \\ p_2 = \Pr[\min\{Y_1, Y_2\} > \mathbb{U}] & = \frac{\mu}{\mu+2\lambda} \end{cases} \tag{5.3}$$

Smart Monitoring:

$$(\lambda_c, \mu_c) = (\sum_{i=0}^{N} \lambda_i, \frac{\lambda_c * P_{Up}}{1 - P_{Up}}) \tag{5.4}$$

$$\begin{cases} P_{Up_b} & = \frac{\mu_b}{\mu_b+\lambda_b} < P_{Up} = \frac{\mu_c}{\mu_c+\lambda_c} \\ \mu_b & = \mu_0 \\ \mu_b & \leq \mu_i, 1 \leq i \leq N \\ \lambda_b & = \sum_{i=0}^{N+M} \lambda_i \end{cases} \tag{5.5}$$

Epidemic Network Model:

$$p(v_h) = \frac{\varsigma(v_h)}{10} \tag{5.6}$$

$$p(c_h|v_h) = \begin{cases} U(0.8, 1) * 1_{\{c_h = T\}}, h = 1 \\ p(c_h|v_h \wedge (v_1 \vee ... \vee v_{h-1})), n \geq h \geq 2 \end{cases} \tag{5.7}$$

$$p(v_h \wedge c_h) = p(v_h) * p(c_h|v_h) \tag{5.8}$$

$$p(c_h) = \sum_{l=1}^{n} p(v_l \wedge c_h) \tag{5.9}$$

and recovery time vector $\overrightarrow{T}_{rec}$ based on the SCTs of ζ and binomially distributed recovery times of ζ, respectively. To consider the cyber risks spreading in the large-scale network, external epidemic infection time Z_{epi} and recovery time R_{epi} are respectively included in

Definition 2: The proposed Cyber Epidemic Model

$$EN(S_x) = \mathbf{1}_{\mathbb{P}_v \geq p_{atk}} \tag{5.10}$$

$$p_{atk} = \frac{T_{rec}}{T_{epi} + T_{rec}} \tag{5.11}$$

$$\mathbb{P}_\nu \sim U(0,1) \tag{5.12}$$

$$\mathbb{B}_\zeta \sim Bin(1,c) \tag{5.13}$$

$$\overrightarrow{T}_{epi} = [\hat{T}_{c,1} \ldots \hat{T}_{c,\gamma}\ Z_{epi}] \tag{5.14}$$

$$\overrightarrow{T}_{rec} = [\hat{T}_{r,1} \ldots \hat{T}_{r,\gamma}\ R_{epi}] \tag{5.15}$$

$$\overrightarrow{\boldsymbol{T}}_r = \{\varepsilon \sum_{\Gamma} \mathbb{B}_\Gamma\} \tag{5.16}$$

$$T_{rec} = \max(\overrightarrow{T}_{rec}) \tag{5.17}$$

$$T_{epi} = E[\overrightarrow{T}_{epi}] \tag{5.18}$$

augmented $\overrightarrow{T}_{epi}$ and $\overrightarrow{T}_{rec}$. The intensity of the epidemic attack can also be adjusted by the basic reproduction number and graphical edge coupling number c. The substation infection time T_{epi} and recovery time T_{rec} are estimated by the maximum and expected values of the respective vectors. Using T_{epi} and T_{rec}, the probability of cyberattack infection p_{atk} is then calculated and compared with a uniform variate to determine whether the substation server is compromised by the cyberattack.

Fig. 5.3 further elaborates the cyber epidemic pattern initiated by a malicious attacker into respective TGs. Each node represents a vulnerability. In each TG, define the control center as the first node and the rest of the substations according to the cyber connection as laid out in the attack graph. The cyber node status is determined by the state sequences

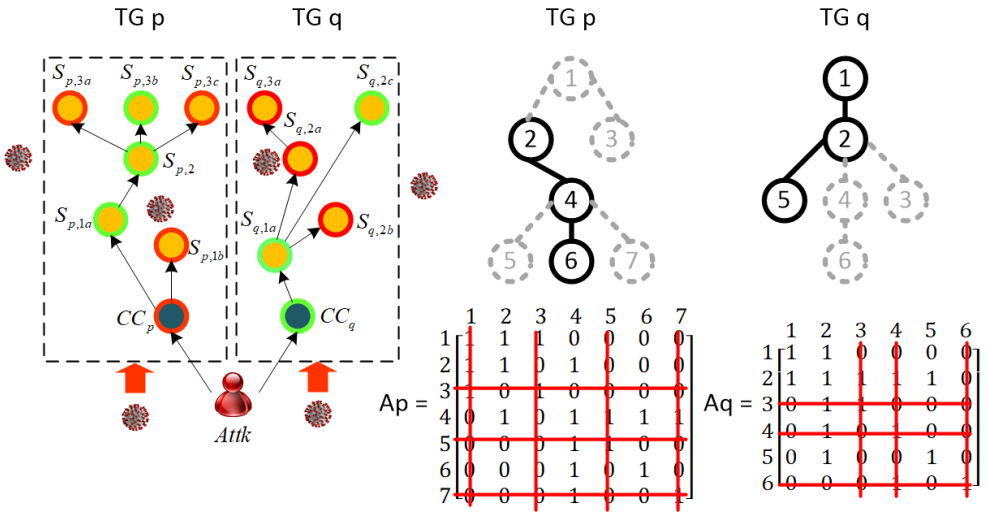


Figure 5.3: Graphical illustration of the cyber epidemic model.

in Definition 2. The infected nodes are grayed out from the healthy nodes. Since a cyber node can be infected by the external network, the infected nodes at any given time are not necessarily adjacent. TG_p and TG_q respectively have adjacency matrices A_p and A_q where entries of nodes have a value of 1 if the corresponding edge is connected, or 0 otherwise. By removing the rows and columns of the infected rows, good routes connecting healthy nodes can be obtained using a routing algorithm such as DFS [69]. Power dispatching action from the control center is feasible along the good routes passing through the control center, which is the case for TG_q only. The substations outside of the good routes indicate disconnection from power generation capacity, resulting in load curtailment in the TG. More details can be referred to [72] for cyber network modeling.

Fig. 5.4 depicts the typical process of epidemic-like propagation on a TG. The malicious attacker infiltrates the firewall of the control center through remote access network connected via a modem. Once the Ethernet in the control center is breached, the attacker can gain

access to the data storage, application server and operation of the workstation. Through infecting the network switch with malware, the attacker may further compromise the substation Intranet. Specifically, the attacker may obtain the privilege of the SCADA server, HMI and a WAP which control the substation operation via RTUs. On some occasions, the attacker may directly compromise the substation through WAP. The breaker operating units connected to RTUs coordinate the relays to provide overcurrent protection, overvoltage protection and differential protection. If the attacker hijacks the WAP, false commands can be sent to RTUs to modify the trip settings in different relays. By intentionally reducing the threshold value of the overcurrent relay, the circuit breakers can be tripped by the attacker when no physical fault condition is presented. A detailed survey further analyzed the impacts of various cyberattack scenarios in the power systems [20].

The substation state sequence $EN(S_x)$ is sampled subject to cyber epidemic described in Definition 2, with binary values 1 and 0 indicating the generation capacity G_cap connected to the specific substations to be either available or offline, respectively. If the substation server is infected by the cyberattack, the attacker could breach the server root privilege and send false tripping commands to the substation relays that cause generation offline. In Definition 2, $EN(S_x) * G_{cap}$ determines the upper bounds of online capacity G at each time step ν. Together with the load capacity D_{cap} and thermal limit constraints F_{cap}, the aggregate substation load loss $\sum_x K_x$ is minimized at each time step ν. The energy balance between the online generation supply and online load demand should always be maintained with load curtailment K_x being further bounded by the load capacity D_cap.

In the following subsection, the cyber-physical enhancement strategies on the substations will be presented.

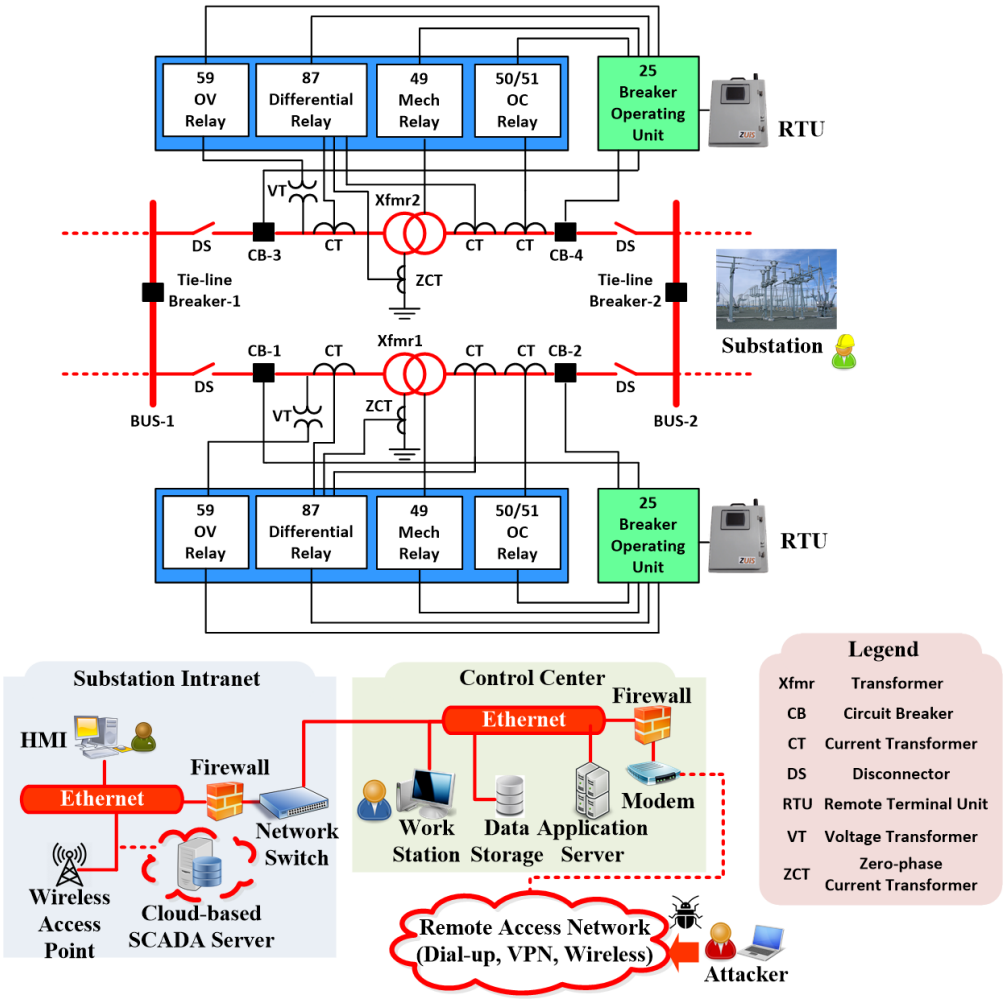


Figure 5.4: A typical cyber epidemic on a TG: from the control center to the substation.

Optimization 2: Reliability-based Load Curtailment Estimation

$$\min\{\Sigma_x \boldsymbol{K}_x\}_\nu \tag{5.19}$$

Subject to:

$$\boldsymbol{B\theta} + \boldsymbol{G} + \boldsymbol{K_x} = \boldsymbol{D_{cap}} \tag{5.20}$$

$$|\boldsymbol{F}| \leq \boldsymbol{F_{cap}} \tag{5.21}$$

$$\mathbf{0} \leq \boldsymbol{K_x} \leq \boldsymbol{D_{cap}} \tag{5.22}$$

$$\mathbf{0} \leq \boldsymbol{G} \leq EN(\boldsymbol{S_x}) * \boldsymbol{F_{cap}} \tag{5.23}$$

$$EN(\boldsymbol{\tau_x}) = \mathbf{1}_{\{\mathbb{P}_\nu \geq p_{atk}\}} \tag{5.24}$$

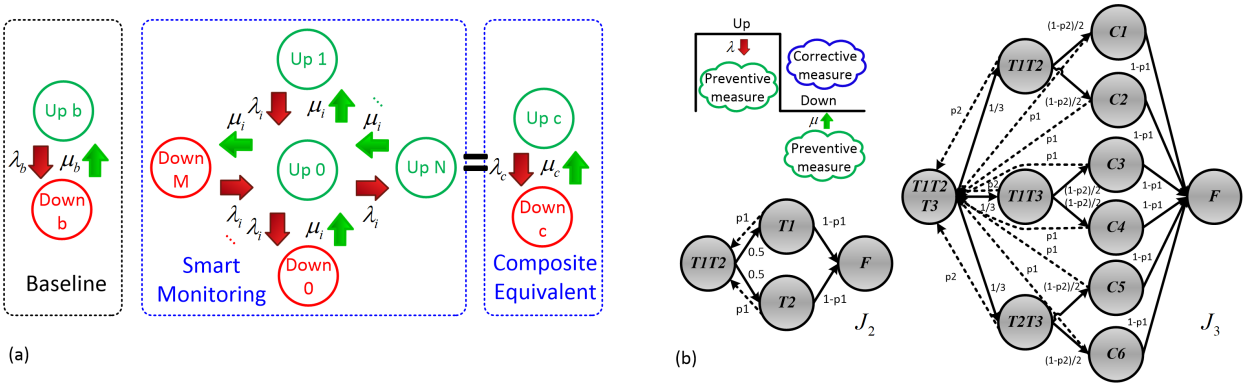


Figure 5.5: (a) A baseline Markovian model vs smart-monitoring Markovian model and its composite equivalent. (b) Markovian models for server job thread assignment: 2 threads (J_2) vs 3 threads (J_3).

5.2.1 Substation Cyber-Physical Enhancement

To enhance power system reliability, substation-oriented smart monitoring including SCADA systems and EMU may be worth investments. To compare the performance between the conventional power system and cyber-physical smart grid with sensing and remedial equipment, reliability modeling of the smart monitoring devices was performed in [70]. Fig. 5.5(a) shows a base case two-state reliability model with failure rate and repair rate (λ_b, μ_b). In Fig. 5.5(a), the smart monitoring reliability model has M+1 up states (Up_0 Up_M) and N+1 (Dn_0 Dn_N) down states, with failure rate and repair rates (λ_i, μ_i) among respective states. The smart monitoring model can be reduced to an equivalent composite two-state model with the composite failure rate and repair rate (λ_c, μ_c).

For the substation servers, ensuring IEDs within the substations function normally is critical, which is also dependent on the dependable computing capability. In typical opera-

tions of computing systems, portions of the memory are dynamically allocated to process-specific tasks. The scheduling strategies in [71] can be adapted to enable improved job thread assignment for our problem, in which multiple server threads are scheduled to carry out the same task command of IEDs to heighten the computing dependability against uncertainties.

Fig. 5.5(b) shows a basic 2-thread (J_2) fault-tolerant job thread assignment procedure assigned with a critical server task in the substation SCADA server. The procedure includes total 4 states: both threads T1T2 carrying out the same task, either thread T_1 or T_2 executing the same task, and both threads fail (F) to perform the task, and the task is terminated by state F. Similarly, Fig. 5.5(b) also shows a 3-thread (J_3) fault-tolerant job thread assignment procedure with 11 states: all 3 threads T1T2T3 conducting the same task, 2 of the threads (T_1T_2, T_1T_3, T_2T_3) carrying out the same task, within 2 selected threads one of the threads further fails ($C_1 \sim C_6$), and all 3 threads fail (F) to perform the task, and the task is terminated by state F. The sojourn time of J_2 and J_3 are $t_s(J_2, \mu, \lambda)$ and $t_s(J_3, \mu, \lambda)$, respectively determined by the probabilities of state transition, duration of task operation, expected thread recruitment rate μ and thread residence rate λ. In this chapter, we will demonstrate the combined application of job thread assignment and smart monitoring can achieve improved grid reliability. In the job assignment, duration of the task operation and residual time of the job thread executing the task are assumed to be exponentially distributed to simplify the calculation.

5.2.2 *Strength of Interdependence*

The SCT T_c is the hypothetical effort where the individual substation privilege access would be obtained by the malicious attacker. Typically, SCTs of the target substations are considered mutually independent in reliability assessment. In this chapter, since all TGs are assumed to be participants of the proposed mutual insurance, the strength of interdependence in substations across the TGs is further studied. The sampled SCT vector $\overrightarrow{T}_c$ is synthesized by multiplying the SCT vector T_c by a uniform variate set $\mathcal{U}$ to produce the correlated loss pattern.

$$\hat{\boldsymbol{T}}_c = \boldsymbol{T}_c * \mathcal{U} \tag{5.25}$$

where $*$ is the element-wise product and $\mathcal{U} \sim U(0,1)$.

Indirect approach is necessary to embed the correlation factor into the uniform variate. Multivariate normal variate $N_c \sim N(0,\Sigma)$ is handy since it allows for specification of the correlation r in the covariance matrix Σ:

$$\Sigma = (1+r)\mathcal{J}_y - I_y \tag{5.26}$$

where y is the number of TGs, $\mathcal{J}_y$ is the all-one matrix, and I_y is the identity matrix.

Substituting $N_c = \{N_{c1}, \ldots, N_{cy}\}$ into the cumulative distribution function of the standard normal distribution Φ, a set of uniform variates can be obtained:

$$\mathcal{U} = \Phi(\{N_c\}) \tag{5.27}$$

where $\mathcal{U} = \{\mathcal{U}_{c1}, \ldots, \mathcal{U}_{cy}\}$ is the copula of the uniform distribution with correlation coefficient r.

In the next section, a cyber-insurance principle tailored to estimate the premiums of individual TGs will be introduced.

5.3 Proposed Insurance Premium Principle

5.3.1 Fundamentals

Due to the growing adoption of ICTs in power systems, more recently attentions have been paid to financial tools to hedge against the unforeseeable monetary losses induced by cyber risks.

A crucial characteristic of the mutual insurance is to account for the financial impacts on economically related entities. Due to the high unpredictability of cyberattack-caused losses, power system application of the mutual insurance can be especially challenging. The intended mutual insurance premium design should be tailored to TGs that feature a relatively small insured pool and large fluctuations in indemnities. Before introducing the detailed insurance design, first an overview on the basics coupled with our previous work is given.

VaR and TCE are statistical indices specifically for gauging risk percentile ϖ. VaR is the $100\varpi\%$ percentile of the loss $\mathcal{L}$. TCE is the average of the worst $100\varpi\%$ scenarios of the loss $\mathcal{L}$. Given the same level of ϖ, TCE is always larger than VaR. The relations among VaR, TCE and the loss $\mathcal{L}$ are described in **??**.

TCE premium design π_1 [24] is a mutual insurance allocated from the insured TGs. π_1

Definition 3: Tail Risk Measures for the loss $\mathcal{L}$

$$VaR_{\varpi}(\mathcal{L}) = \inf\{l : P(\mathcal{L} > l) \leq \varpi\}, \varpi \in (0,1) \tag{5.28}$$

$$TCE_{\varpi}(\mathcal{L}) = E[\mathcal{L}|\mathcal{L} > VaR_{\varpi}(\mathcal{L})] \tag{5.29}$$

$$\Pr[\mathcal{L} > VaR_{\varpi}(\mathcal{L})] = \varpi \tag{5.30}$$

$$TCE_{\varpi}(\mathcal{L}) > VaR_{\varpi}(\mathcal{L}), \forall \mathcal{L} \tag{5.31}$$

$$\Pr[\mathcal{L} > TCE_{\varpi}(\mathcal{L})] \leq \varpi \tag{5.32}$$

can gauge risk conservatively based on individual contributions to $TCE_{\varpi}(\sum_q \mathcal{L}_q)$. In extremely catastrophic events, π_1 would be beneficial. When the tail risk is small, π_1 may induce heavy financial burden on the TGs if no major loss events occur.

π_1 is devised with the third-party insurer operation in mind. When undesirably high premium quotes from π_1 occur, an insurance coalition among the TGs comes into play handily. The coalitional insurance manages to scale down the premium risk loading by evenly distributing the premiums across participating entities. The coalitional premium π_2 [25] is a mutual insurance based on the crowdfunding model that distributes the risk affordably with small risk loading. π_2 offers small loss coverage and is designed accounting for the fairness across the TGs. The commitment and the claim of π_2 can be flexibly adjusted on the participants discretion, which are herein set to be the TCE premium and the expected loss, respectively. π_2 optimizes affordability at the cost of small coverage. In the following subsection, a novel Shapley premium design π_3 is proposed as a middle ground between π_1 and π_2.

Definition 4: The proposed Shapley mutual insurance principle

$$\pi_3(\mathcal{L}_q) = \mathbb{C}_q(\mathbf{U}, \varepsilon_{q,k}) \tag{5.33}$$

$$\varepsilon_{q,k}(S) = C_k^y \delta_q^k (1-\delta_q^k)^{y-k} \sum_{q \in S} VaR_{\varpi}(\mathcal{L}_q) \tag{5.34}$$

$$\Gamma_{q,k}^* = \frac{y-k}{y-1} TCE_{\varpi}(\mathcal{L}_q) + \frac{k-1}{y-1} \sum_{q \in \mathbf{U}} TCE_{\varpi}(\mathcal{L}_q) \tag{5.35}$$

$$\Gamma_{q,k}^{\psi} = \psi(\Gamma_{q,k}^*) = \begin{cases} \Gamma_{q,k}^*, & if \sum_{q \in S} \Gamma_{q,k}^* \leq \sum_{q \in \mathbf{U}/S} \mathbb{C}_q \\ \frac{\sum_{q \in \mathbf{U} \setminus S} \mathbb{C}_q}{\sum_{q \in S} \Gamma_{q,k}^*}, & else \end{cases} \tag{5.36}$$

5.3.2 The Proposed Shapley Premium

The Shapley value [73]-[75] was introduced as a unique set of values fairly distributed across players in the cooperative games. Several basic properties should be mentioned before we present the premium design. In a cooperative game $G = (\mathbf{U}, \varepsilon)$ that contains a finite player set U whose respective costs correspond to a subset S are $\varepsilon(S)$, the Shapley value of the TG q is defined as follows:

$$\mathbb{C}_q(\mathbf{U}, \varepsilon) = \frac{\sum_{S \subseteq \mathbf{U} \setminus \{q\}} |S|!(|\mathbf{U}| - |S| - 1)![\varepsilon(S \cup \{q\}) - \varepsilon(S)]}{|\mathbf{U}|!} \tag{5.37}$$

Here we propose a cooperative-game based Shapley value design applied to the power system cyber-insurance to achieve risk loading able to better reflect the respective losses relative to the even distribution of premiums in the coalitional insurance.

In Shapley premium π_3, Shapley value $\mathbb{C}_q(\mathbf{U}, \varepsilon_{q,k})$ of the loss $\mathcal{L}_q$ serves as the premium. To handle typical risk lower than the tail risk, in the subset S including selected TGs,

Shapley cost $\varepsilon_{q,k}(S)$ is tailored based on the cumulative loss distributions δ_q smaller than $VaR_{\varpi}(\mathcal{L}_q), q \in S$. Since the typical risk in each TG varies, in $\varepsilon_{q,k}(S)$ the probability that the specific TGs are included in a subset S is determined by an unfair coin-tossing model applied to δ_q at varying k which is the number of TGs submitting their claims. For each of the TGs, the cooperative game G determines $\mathbb{C}_q(\mathbf{U}, \varepsilon_{q,k})$ by assigning the expected values of its marginal contribution. The constraint of rationality ensures $\mathbb{C}_q(\mathbf{U}, \varepsilon_{q,k})$ that no feasible cooperation can be formed if the cooperative cost is higher than the sum of the respective costs. In other words, the Shapley cooperative game G guarantees each of the mutual insurance participants a lower cost than the cost by itself. In this way, $\varepsilon_{q,k}(S)$ ensures that the Shapley premium $\pi_3(\mathcal{L}_q)$ is allocated according to the loss $\mathcal{L}_q$ of the TG, achieving the fairness across TGs.

The base indemnity Γ_q^* is the amount that each of the TGs can redeem from insurance when suffering from the loss event. Γ_q^* is proportionally allocated between the self-indemnity term $TCE_{\varpi}(\mathcal{L}_q)$ and the group-indemnity term $\sum_{q \in U} TCE_{\varpi}(\mathcal{L}_q)$ summed across all the participating TGs. The group-indemnity term weighs heavily as k increases, and vice versa. To ensure the budget sufficiency at various k, Γ_q^* is scaled down when exceeding the premium $\mathbb{C}_q$. Like π_1 and π_2, the formulation of π_3 also incentivizes the security investment by reducing the premium payment. Besides, π_3 is a mutual insurance that intends to be a financial mutual trust. In the case studies, we will show the majority of TGs with positive risk loading provides some margin to cushion against uncertainty. In the mutual insurance, outliers struck by unexpectedly high damages could partially be covered by the premium of other TGs, resulting in negative risk loading.

A major design goal of the insurance premium is to mitigate the risk insolvency to

restrain the risk higher than the indemnity. TCE premium π_1 offers good mitigation on the risk insolvency and is utilized as the claim term in π_3. Combining the advantages of π_1 and π_2, we will show in the case studies the proposed π_3 can substantially restrain the insolvency comparable to π_1 while providing a competitive premium package with low risk loading which is nearly as affordable as π_2. The mutual insurance premium estimation procedure is summarized in Algorithm 5.1.

Algorithm 5.1: Mutual Insurance for Power System Stability

Input: $J_i, \mu, \lambda, C_q, S_{q,x}, v_h, r$
Output: $\pi_{\mathcal{L}_q}, \rho(\mathcal{L}_q), \Gamma_q^{\psi}$

```
function
    /* Stochastic model sampling preparation */
    for Each TG q do
        for Each substation x do
            Evaluate (λ_c, μ_c) based on Smart Monitoring.
            Substitute (λ_c, μ_c) into t_s(J_i) of Job Assignment.
        end
        Collect cyber network information (C_q, S_{q,x}, v_h)
        for Each substation x do
            Based on Definition1,
            Synthesize t_s(J_i, λ, μ) and v_h in BN.
            Compute T_c graphically using (C_q, S_{q,x}, t_s).
        end
    end
    /* Incorporate correlation in sampling */
    Synthesize T̂_c via inverse transform (4)-(6).
    Generate substation sequence EN(S_x) using Definition 2.
    Perform Oprimization 1 to obtain L_q in each TG q.
    /* Premium estimation using cyber-insurance principle */
    Estimate premium designs π_1(L_q), π_2(L_q), π_3(L_q).
    Estimate TG indemnities Γ_q^ψ(π_1), Γ_q^ψ(π_2), Γ_q^ψ(π_3).
end
```

The proposed cybersecurity mutual insurance model shown in Fig. 5.6 can be elaborated as follows: (1) Epidemic cyber-physical system model. The cyber attacker injects the epidemic virus through Internet that penetrates the firewall of a TG. Within the TG, a

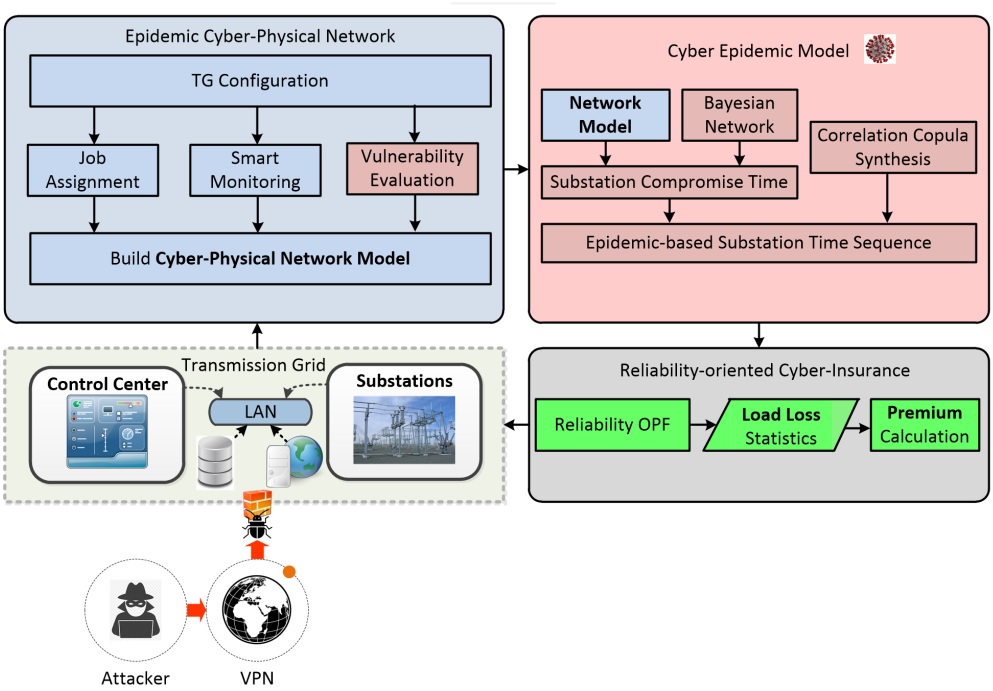


Figure 5.6: Flowchart of the proposed cybersecurity mutual insurance model, comprising (I) epidemic cyber physical system modeling, and (II) cyber-insurance design.

control center and substations interconnected via the LAN are stochastically infected by the cyber epidemic with certain probabilities. The proposed cyber-physical network model (Definition 1) accounts for the defensive capability of the TG depending on both the hardware investment and software strategy development, in addition to its intrinsic vulnerabilities. With the above information, the substation state sequence (Definition 2) can be synthesized considering the interdependence strengths across the TGs.

(2) Cyber-insurance design. Taking the state sequence generated by the cyber epidemic, load curtailment of the respective TGs is calculated with the reliability analysis (Optimization 1). Using the marginal distribution of load loss statistics of the individual TGs, cyber premiums are estimated according to the proposed Shapley premium which incorporates the merits of both TCE premium and coalitional premium. In the following section, the proposed Shapley premium design at various strengths of interdependence and cyber-physical defense investment will be verified in the simulated case studies.

5.4 Simulation Results

Case studies are performed to validate the proposed reliability assessment framework and cyber insurance model. As shown in Fig. 5.7, we deployed a benchmark IEEE RTS-GMLC [76]. The IEEE RTS-GMLC is a major update from the IEEE RTS-96 [59] by incorporating the increasing share of renewable energy resources such as wind and solar energies. To study the effectiveness of mutual insurance, we divided the 3-area test system into 5 TGs. We further augmented the IEEE RTS-GMLC by incorporating the epidemic cyber network as the cyberattack model. The cyberattack parameters of the epidemic network are

assigned as follows: $Z_{epi} = 2000$ hrs, $R_{epi} = 4$ hrs, $\varepsilon = 2$, and $c = 0.8$.

To make a preliminary comparison on the system risk in the test system under various scenarios, risk indices estimating load curtailment and fault coverage are adopted from [77]. Denote LC as the load curtailment and FC as the number of faulty buses at the m-th time step. The ELC and the EFC are defined as follows:

$$ELC = \frac{1}{N_m} \sum_{m=1}^{N_m} LC_m^T \tag{5.38}$$

$$EFC = \frac{1}{N_m} \sum_{m=1}^{N_m} FC_m^T \tag{5.39}$$

Parameters of the cyber-physical elements installed in the substations are listed in Table 5.1. When the substations smart monitoring is functional, the server is connected to other elements. Otherwise, the server is disconnected from other elements. Six scenarios are studied to demonstrate the effectiveness of the job assignment and smart monitoring. As shown in Table 5.2, the deployment of job assignment and smart monitoring technologies enhances the security and reliability of power supply by effectively reducing the load curtailment and faulty-bus count. With the job assignment, Scenario 2 improves more than 20% from Scenario 1 in both ELC and EFC. With the smart monitoring technology enforced, Scenario 4 has 7% improvement on ELC and EFC from Scenario 1. In Scenarios 5 and 6, smart monitoring on top of the job assignment can further improve several percent compared with the situations of job assignment implemented alone in Scenarios 2 and 3.

The reliability-based OPF is carried out in MCS based on the state sampling method. The sampled period is 40 years with hourly time steps. Specifically, the server job thread assignment and the smart monitoring deployment within the substations mutually determine

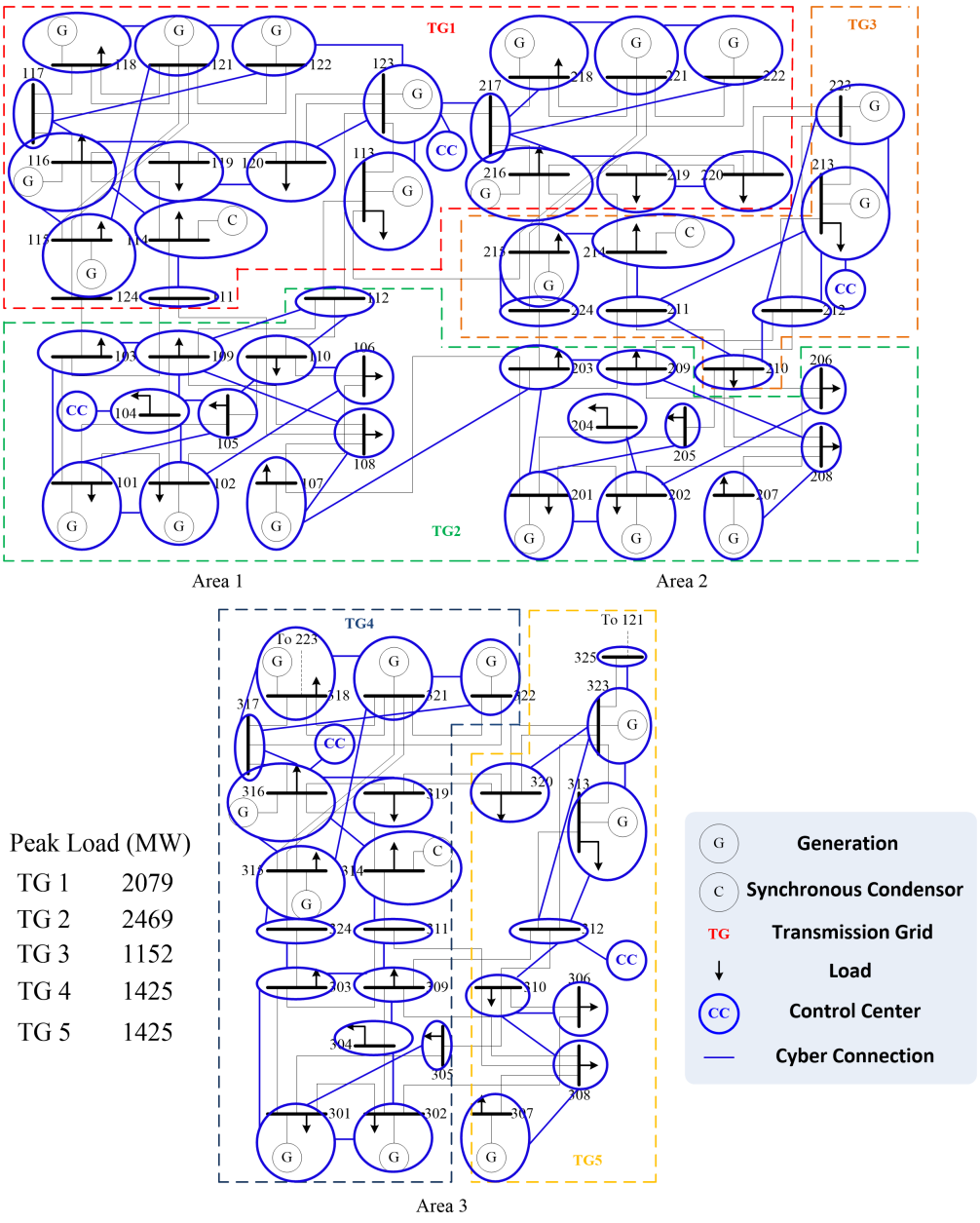


Figure 5.7: TG Zones in the modified IEEE RTS-GMLC including the epidemic cyber network.

Table 5.1: Cyber-Physical Element Parameters

Element	Failure rate $\lambda(h^{-1})$	Repair rate $\mu(h^{-1})$	Reliability	State
Server (Attacked)	1/9200	1/48	0.9948	Dn_b
Server	1/14000	1/48	0.9966	Dn_0
Bus	1/876000	1/6	0.999993	Dn_1
Switch	1/45000	1/48	0.9989	Dn_2
Optical fiber	1/500000	1/12	0.999976	Up_1
EMU	1/87600	1/24	0.9997	Up_2

Table 5.2: Reliability-Assessment Results of Example Scenarios

Scenarios		ELC (p.u.)	Improvement	EFC	Improvement
1	(J_1, μ_b, λ_b)	0.2398	–	12.915	–
2	(J_2, μ_b, λ_b)	0.1852	22.77%	9.9233	23.17%
3	(J_3, μ_b, λ_b)	0.1471	38.66%	7.7812	39.75%
4	(J_1, μ_c, λ_c)	0.2212	7.66%	11.930	7.63%
5	(J_2, μ_c, λ_c)	0.1693	29.40%	9.0138	30.21%
6	(J_3, μ_c, λ_c)	0.1334	44.37%	7.0239	45.62%

the compromise time of the substation SCADA server. Cyberattacks that penetrate the substation servers may sabotage the operation by gaining root privilege to send out spurious commands to protection relays for disconnecting generation from the grid, causing physical load losses. The load loss statistics is then converted into the monetary reliability worth to estimate the cybersecurity insurance premiums of participating TGs.

To further examine the merits of the proposed Shapley premium design over the previous ones, two case groups are created to compare job thread assignment, smart monitoring, and correlation coefficients at varying degrees.

Case Group 1: Based on Scenario 1 (J_1, μ_b, λ_b) where in the substation only a single job thread is available without smart monitoring.

Case Group 2: Based on Scenario 6 (J_3, μ_c, λ_c) where the strongest job assignment and substation smart monitoring are enforced.

To explore the loss characteristics in Case Group 1, Table 5.3 summarizes the expected values, SDs, and CoVs under various strengths of correlation r. CoV is obtained from the SD being divided by the expected value. The expected values come close to SDs, resulting in CoVs only fluctuating in a small range of [0.74 1.13]. Since a stronger correlation r signifies the infectiousness of the epidemic model and tends to bring higher expected losses, the common cyber risk across TGs also increases. In Case Group 2, the incentive of investing on cyber-physical enhancement can be observed from Table 5.4 that expected losses are reduced substantially and reduction of SDs occurs to a lesser extent, with CoVs lying in [0.88 1.33].

In Fig. 5.8, the sampled interdependence strengths among the TGs are demonstrated in the Pearson correlation matrix. The correlation is symmetric and correlation between each of the two TGs can be observed in the off-diagonal entries. Fig. 5.8(a) depicts the

Table 5.3: Case Group 1: Expected Values (M$), Standard Deviations (M$) and Coefficients of Variation of Monetary Loss in the TGs

$r = 0$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**
$E[\mathcal{L}_q]$	4.42	7.10	2.76	3.49	3.92
SD	4.83	5.97	2.88	3.69	3.29
CoV	1.09	0.84	1.05	1.06	0.84
$r = 0.5$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**
$E[\mathcal{L}_q]$	4.60	9.82	3.66	3.79	4.02
SD	5.04	10.5	3.51	4.29	2.99
CoV	1.10	1.07	0.96	1.13	0.74
$r = 1$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**
$E[\mathcal{L}_q]$	7.45	12.7	3.97	4.74	5.28
SD	5.89	11.2	3.34	4.11	4.67
CoV	0.79	0.88	0.84	0.87	0.88

Table 5.4: Case Group 2: Expected Values (M$), Standard Deviations (M$) and Coefficients of Variation of Monetary Loss in the TGs

$r = 0$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**
$E[\mathcal{L}_q]$	2.48	3.96	1.94	1.53	1.82
SD	3.30	3.83	2.04	1.91	1.91
CoV	1.33	0.97	1.05	1.25	1.05
$r = 0.5$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**
$E[\mathcal{L}_q]$	2.79	5.73	2.60	1.89	2.69
SD	3.72	6.92	2.30	2.46	2.61
CoV	1.33	1.21	0.88	1.30	0.97
$r = 1$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**
$E[\mathcal{L}_q]$	5.02	7.01	3.70	2.19	3.06
SD	4.95	6.99	3.51	2.38	3.46
CoV	0.99	1.00	0.95	1.09	1.13

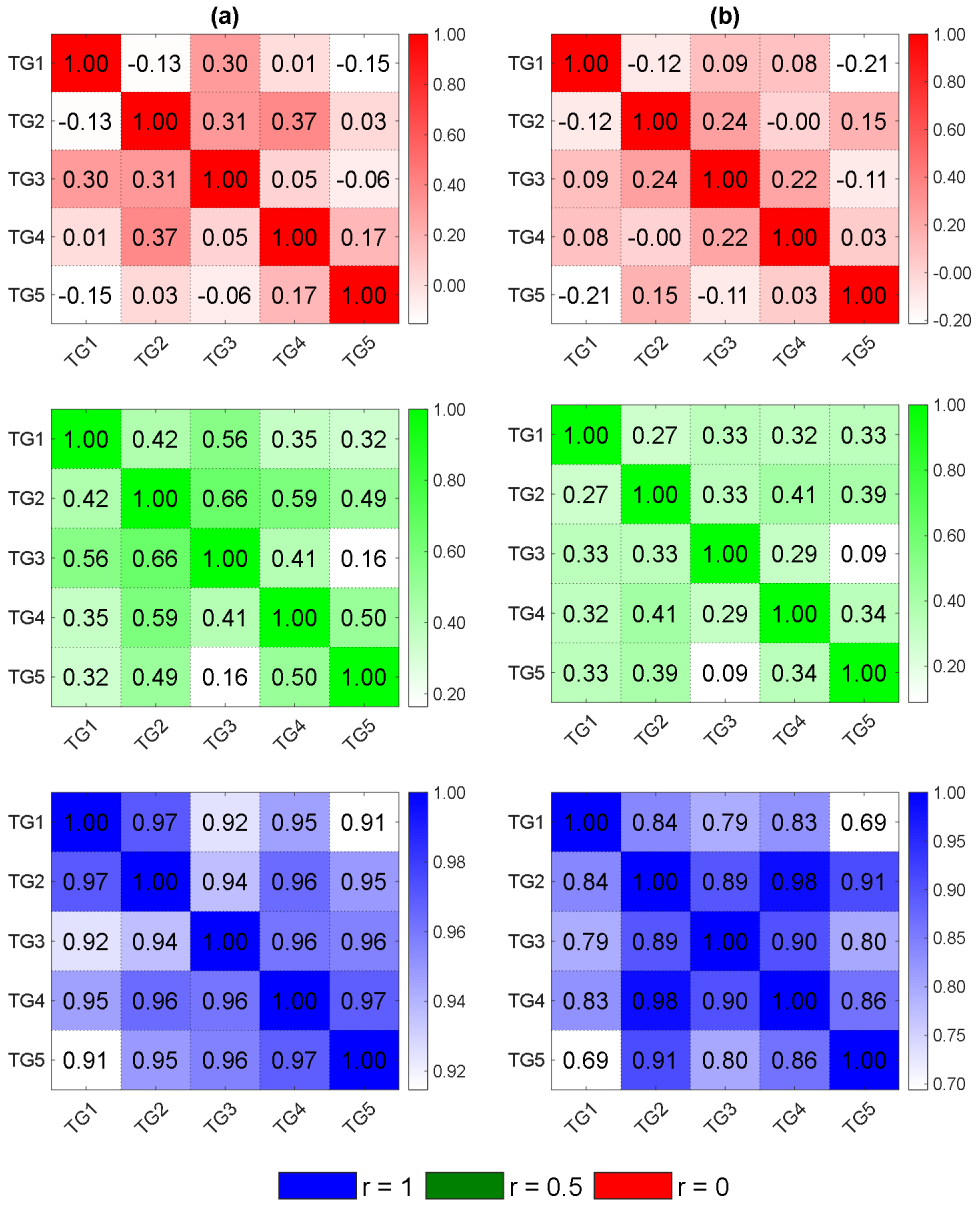


Figure 5.8: Interdependence strengths of the loss profile in the TGs in (a) Case Group 1 (b) Case Group 2.

correlation matrix of the Case Group 1. When $r = 0$, the interdependence strengths across the TGs are close to 0 with higher correlations between the neighboring TGs in the same areas. The correlations range around 0.45 as r increases to 0.5. When $r = 1$, the correlations across all TGs are above 0.9. The correlation matrix in Case Group 2 is as shown in Fig. 5.8(b). Due to reduced load losses, the correlations are in general weakened between the same pair of TGs in Case Group 1.

Insurance premiums are designed to prepare TGs for catastrophic losses induced by probable cyberattack events. For interconnected TGs, mutual insurance accounting for respective marginal loss statistics would be a sensible option. The premium with a high-risk loading offers solid indemnity, which may however be less financially appealing to potential participants. An ideal premium design should be meticulously tailored to avoid excessive financial burdens while providing sufficient loss indemnities for the insured parties. The highly infectious nature of the cyber epidemic model dictates a heavily skewed tail risk.

To validate the design of the proposed cyber-insurance principle, we herein compare (a) TCE premium π_1, (b) Coalitional premium π_2, and (c) Shapley premium π_3 of this chapter at various degrees of correlation of the TGs. The TCE Premium is the most conservative design predominantly responsive to the tail risk, providing great redundancy at the cost of high-risk loading. On the contrary, the Coalitional Premium is the most affordable package by excluding extreme high-loss events with low probabilities. The Shapley Premium is cooperative and tailored to add further coverage against the tail risk, striking a balance between the affordability and loss coverage.

To gauge the relative premium burden against the expected risk, RLC is defined as follows:

$$\rho(\mathcal{L}_q) = \frac{\pi(\mathcal{L}_q)}{E[\mathcal{L}_q]} - 1 \tag{5.40}$$

where $\rho(\mathcal{L}_q)$ should be generally positive to gather sufficiency budget for loss coverage. While positive RLC is preferable as preparation for the unexpected extreme risk, excessively high RLC would discourage the TGs from joining the mutual insurance. $\Gamma_q^{\psi} = \max_k \Gamma_{q,k}^{\psi}$ is the indemnity that the TGq can at most redeem from a loss.

In [17], the indemnities of $\pi_1(\mathcal{L}_q)$ are not clearly specified since the original design is tailored to a third-party insurer. In this chapter, all premium designs are assumed to be mutual insurance. All participating entities are both insurers and insureds. For the sake of brevity, the indemnities of $\pi_1(\mathcal{L}_q)$ are proportionally allocated based on $\Gamma_q^{\psi}(\pi_2)$:

$$\Gamma_q^{\psi}(\pi_1) = \sum_q \pi_1(\mathcal{L}_q) * \frac{\Gamma_q^{\psi}(\pi_2)}{\sum_q \Gamma_q^{\psi}(\pi_2)} \tag{5.41}$$

π_1, π_2, and π_3 are respectively evaluated based on the loss statistics extracted from the two case groups with heavy tail risks. Characteristics of each design will be further elaborated numerically as follows.

The premiums of Case Group 1 are shown in Table 5.5. In each TG, π_1, π_2, and π_3 are positively correlated with the strength of correlation r. π_1 has the most conservative payment schedule and can be financially burdensome. π_1 may penalize the participants with heavy risk loading when extreme catastrophic events do not happen. Cost-effectiveness of π_1 is unacceptably low because the maximum of ρ_1 exceeds 3. On the flip side, π_2 is an entry-level premium design devised to be the most affordable and evenly distributed package across the TGs. π_2 offers small indemnities and the premiums collected from the TGs. ρ_2 of some TGs can be slightly negative while the corresponding indemnities are supplemented by

Table 5.5: Actuarial Insurance Premiums (M$) in Case Group 1

$r = 0$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**
π_1	19.0	20.3	11.3	12.6	12.6
$\Gamma^{\psi}(\pi_1)$	15.3	18.8	13.1	14.1	14.6
ρ_1	3.30	1.87	3.11	2.60	2.22
π_2	4.93	6.51	4.35	4.78	5.07
$\Gamma^{\psi}(\pi_2)$	8.74	10.7	7.49	8.04	8.36
ρ_2	0.12	-0.08	0.58	0.37	0.29
π_3	4.06	7.97	3.25	4.92	5.91
$\Gamma^{\psi}(\pi_3)$	17.0	18.1	10.1	11.2	11.3
ρ_3	-0.08	0.12	0.18	0.41	0.51
$r = 0.5$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**
π_1	19.9	40.7	12.3	13.5	12.8
$\Gamma^{\psi}(\pi_1)$	19.0	26.5	17.7	17.8	18.2
ρ_1	3.32	3.14	2.37	2.57	2.19
π_2	5.33	7.37	5.28	5.26	5.48
$\Gamma^{\psi}(\pi_2)$	9.93	13.8	9.22	9.31	9.49
ρ_2	0.16	-0.25	0.44	0.39	0.36
π_3	4.39	8.26	6.47	5.99	6.81
$\Gamma^{\psi}(\pi_3)$	11.6	23.7	7.17	7.85	7.46
ρ_3	-0.05	-0.16	0.77	0.58	0.69
$r = 1$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**
π_1	20.5	40.8	12.5	13.9	17.9
$\Gamma^{\psi}(\pi_1)$	21.8	27.9	17.8	18.7	19.3
ρ_1	1.75	2.20	2.14	1.94	2.39
π_2	7.55	9.39	6.03	6.40	6.44
$\Gamma^{\psi}(\pi_2)$	14.1	18.1	11.5	12.1	12.5
ρ_2	0.01	-0.26	0.52	0.35	0.22
π_3	9.85	10.9	7.21	8.28	6.86
$\Gamma^{\psi}(\pi_3)$	16.2	32.2	9.84	11.0	14.2
ρ_3	0.32	-0.15	0.81	0.75	0.30

Table 5.6: Actuarial Insurance Premiums (M$) in Case Group 2

$r = 0$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**
π_1	12.1	12.2	7.51	7.49	7.60
$\Gamma^{\psi}(\pi_1)$	9.47	10.5	9.11	8.84	9.03
ρ_1	3.90	2.08	2.87	3.91	3.18
π_2	2.80	3.77	2.77	2.43	2.67
$\Gamma^{\psi}(\pi_2)$	4.91	5.42	4.72	4.58	4.68
ρ_2	0.13	-0.05	0.43	0.60	0.47
π_3	2.21	4.51	2.78	0.87	1.90
$\Gamma^{\psi}(\pi_3)$	7.72	7.75	4.78	4.77	4.84
ρ_3	-0.11	0.14	0.43	-0.43	0.04
$r = 0.5$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**
π_1	13.7	26.4	8.00	9.19	8.19
$\Gamma^{\psi}(\pi_1)$	12.5	17.1	12.2	11.1	12.4
ρ_1	3.89	3.60	2.07	3.87	2.04
π_2	3.22	4.37	3.52	2.89	3.57
$\Gamma^{\psi}(\pi_2)$	6.02	8.23	5.88	5.34	5.95
ρ_2	0.15	-0.24	0.35	0.53	0.32
π_3	2.27	4.69	5.30	1.32	2.42
$\Gamma^{\psi}(\pi_3)$	7.41	14.3	4.34	4.98	4.44
ρ_3	-0.19	-0.18	1.04	-0.29	-0.10
$r = 1$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**
π_1	17.3	26.7	11.8	9.95	14.2
$\Gamma^{\psi}(\pi_1)$	17.2	20.0	15.3	13.1	14.4
ρ_1	2.45	2.80	2.19	3.54	3.64
π_2	5.18	5.84	4.72	3.78	4.08
$\Gamma^{\psi}(\pi_2)$	9.01	10.5	8.02	6.89	7.54
ρ_2	0.03	-0.17	0.28	0.72	0.33
π_3	6.24	6.55	6.10	1.80	3.11
$\Gamma^{\psi}(\pi_3)$	10.6	16.3	7.20	6.07	8.65
ρ_3	0.24	-0.07	0.65	-0.18	0.02

other TGs. However, the worse risk of π_2 beyond expected losses could barely be covered. π_3 rewards TGs of relatively low risk loading with high indemnities. While π_1 provides higher indemnities than π_3, π_3 offers affordability comparable to the coalitional platform of π_2. The proposed π_3 has its costs close to π_2 and substantially alleviates the insolvency hazard of π_2. While ρ_2 spans from -0.26 to 0.58, ρ_3 is dispersed in $[-0.16\ 0.81]$, a typical range of risk loading across TGs. Relative to π_2, π_3 offers a wider margin in ρ_3 to guarantee sufficient budget to cover individual risk.

In Table 5.6, risk loading of the TGs in Case Group 2 generally increase due to the enhanced security measure that reduces tail risk profile. ρ_1 has a maximum close to 4 and could be too high to motivate entities to participate in. π_2 is evenly distributed against average risk, with ρ_2 lying in $[-0.24\ 0.72]$. π_3 renders ideal risk loading ρ_3 to rarely exceed 1. High capacity of indemnity and low risk loading make the proposed π_3 a potentially compelling insurance model in practice.

The probability of insolvency $\Phi(\pi)$ is another risk measure which quantifies the capability of the insurance to mitigate the insolvency. $\Phi(\pi)$ is defined as the probability that the loss is greater than the indemnity:

$$\Phi(\pi) = \Pr[\mathcal{L}_q > \Gamma_q^{\psi}(\pi)] \tag{5.42}$$

As shown in Table 5.7, in Case Group 1, it can be observed that π_1 generally provides the best insolvency alleviation with lowest probabilities of insolvency. In fact, π_1 is such a conversative premium design against risk that the insolvency in some cases is 0. While π_3 leads to the insolvency being lower than π_2 and greater than π_1, π_3 has the affordability

Table 5.7: Insolvency Probability (%) of Actuarial Insurance Premiums in Case Groups 1,2

Case Group 1					
$r = 0$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**
$\Phi(\pi_1)$	7.50	7.50	0	0	0
$\Phi(\pi_2)$	10.0	17.5	7.50	15.0	10.0
$\Phi(\pi_3)$	7.50	7.50	5.00	7.50	5.00
$r = 0.5$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**
$\Phi(\pi_1)$	5.00	7.50	0	0	0
$\Phi(\pi_2)$	7.50	27.5	12.5	17.5	5.00
$\Phi(\pi_3)$	7.50	7.50	12.5	17.5	5.00
$r = 1$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**
$\Phi(\pi_1)$	0	12.5	0	0	0
$\Phi(\pi_2)$	15.0	20.0	7.50	10.0	10.0
$\Phi(\pi_3)$	15.0	12.5	10.0	15.0	10.0
Case Group 2					
$r = 0$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**
$\Phi(\pi_1)$	7.50	10.0	0	0	2.50
$\Phi(\pi_2)$	20.0	25.0	10.0	5.00	2.50
$\Phi(\pi_3)$	7.50	20.0	10.0	5.00	2.50
$r = 0.5$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**
$\Phi(\pi_1)$	7.50	7.50	0	0	0
$\Phi(\pi_2)$	10.0	27.5	15.0	7.50	20.0
$\Phi(\pi_3)$	7.50	7.50	15.0	7.50	20.0
$r = 1$	**TG1**	**TG2**	**TG3**	**TG4**	**TG5**
$\Phi(\pi_1)$	2.50	7.50	0	0	2.50
$\Phi(\pi_2)$	12.5	25.0	15.0	5.00	7.50
$\Phi(\pi_3)$	10.0	7.50	15.0	5.00	5.00

superior to π_1. In Case Group 2, when the cyber risk is significantly reduced, π_3 can control the insolvency to be as low as or even lower than π_1. In this sense, π_3 offers an economical option with relatively sufficient insolvency mitigation.

CHAPTER 6. CONCLUSION AND OUTLOOK

6.1 Conclusion

• In Chapter 3, a new actuarial insurance principle is designed for a single insurer undertaking the cyber risks transferred from the power system TGs. In each TG, the cyber premium is determined according to the intrusion tolerant capability of the SCADA system. A Stackelberg Security game model is developed to optimally allocate the stochastic defense resource coverage that is unpredictable by the attacker. Investment on the defense resource coverage to enhance the intrusion tolerance capability of the SCADA systems better protects the substations from failure. As shown in the case studies, the proposed actuarial insurance principle incentivizes the TGs with higher intrusion tolerance capability by reduced premiums.

• Considering the increasing cyber vulnerabilities, it is possible that purchase of cyber-insurance might become mandatory in the future for TGs and electric utilities. Cyber-insurance could be further integrated as a part of the operation cost. The TGs and electric utilities would be able to avoid high premiums by complying with more rigorous security standards mandated by the national ERO such as the NERC. Since cyberattacks are becoming more and more prevalent along with the widespread use of leading-edge ICTs, the trend of increasing cyberattacks is expected to continue. Although cyberattacks causing large-scale load losses are uncommon thus far, cyber-insurance should be developed as a promising tool for transferring the risks and combatting the consequential cybersecurity threats.

• Due to the potential consequential losses caused by cyber threats on power grids, the estimated premiums are relatively high compared to those of the traditional insurance models. Preliminary studies show that a longer insurance contract can effectively reduce the annual premium. As the proposed cybersecurity insurance model is innovative to cyber risk pricing, we do anticipate some practical issues in the implementation. To apply the proposed model, dynamic modeling is required in contrast to the static settings in this paper: the interactions between the insurer and the TGs and their behaviors along time need to be taken into consideration. Specifically, when the insurer expands business and covers more TGs, we require the addition of new TGs not to increase the premiums of the existing TGs under the given insurance principle. These issues are being analyzed through studying theoretical properties of the proposed cybersecurity insurance model.

• In Chapter 4, a coalitional cyber-insurance framework is proposed based on power system reliability assessment accounting for cyber-vulnerability. Different from the TCE premium that conservatively ensures loss coverage of the TGs, the coalitional premium is designed to alleviate the RLC across the TGs especially at high defense coverage. Also, the proposed coalitional cyber-insurance design does not involve the third-party insurer. In addition, a graphic intrusion model is proposed to encompass the interdependence of network vulnerabilities and synthesize the stochastic cybersecurity metric based on the intrusion routes.

• As shown in the case studies, a higher defense level is incentivized by the reduced premiums according to the proposed actuarial principle. This paper is an attempt to establish an innovative cyber-insurance design incorporating integrated long-term reliability-vulnerability assessment for power grids. Possible future work on this research topic includes insurance package design customized to the needs of individual TGs. Since dependence among the

TGs is always one crucial factor when calculating the insurance premiums, the dependence factors of cyber risks may be separately estimated to further improve the fairness of the premium design.

• In Chapter 5, a mutual insurance premium principle for financially hedging against cyber risks is designed to distribute the cyber risks across the participating TGs. It presents an augmented reliability evaluation framework including the epidemic model of cyberattacks coupled with reliability enhancement technologies including smart monitoring and job assignment, as well as a mutual insurance model which estimates the premiums based on the reliability-based loss profiles. The premiums are collected to provide a sufficient indemnity for potential cyberattack-induced losses. The mutual premium, determined by the loss statistics in the cooperative game, intends to sufficiently alleviate the financial risk of TGs against cyberattacks while being relatively affordable.

6.2 Outlook

• Future work can also be extended but not limited to the coalition of the insurers to distribute the cyber risks and reach more affordable insurance packages. Moreover, a platform can be established for the insurers and TGs to negotiate the premiums based on the available information revealed by the TGs. In the premium designs, the transparency of the operating history and cyber incidents of the TGs should be encouraged and incentivized. To promote the cyber-insurance, premium packages may be re-designed or adjusted to be more flexible according to actual situations of the respective TG, with partial coverage on the potential monetary losses with stricter conditions and limitations. Furthermore, novel

studies for optimally allocating the defense resources may be performed to manage cyber risks with advanced game theories. The study will also be extended to the distribution network level such that the cyber-insurance premium framework will be directly related to the electric utilities.

REFERENCES

[1] N. Kshetri and J. Voas, "Hacking Power Grids: A Current Problem," Computer, vol. 50, no. 12, pp. 91-95, 2017.

[2] "Atlanta officials reveal worsening effects of cyber attack," June 6, 2018. [Online]. Available: https://www.reuters.com/article/us-usa-cyber-atlanta-budget/atlanta-officials-reveal-worsening-effects-of-cyber-attack-idUSKCN1J231M.

[3] "Experts assess damage after first cyberattack on U.S. grid," May 6, 2019. [Online]. Available: https://www.eenews.net/stories/1060281821.

[4] "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Mar. 3, 2016. [Online]. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[5] North American Electric Reliability Corporation (NERC), "2019 State of Reliability," NERC, June 2019. [Online]. Available: `https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2019.pdf`.

[6] North American Electric Reliability Corporation, "CIP standards." [Online].Avail able: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[7] National Institute of Standards and Technology, "Cybersecurity Framework Version 1.1 (April 2018)" [Online]. Available: https://www.nist.gov/cyberframework/framework.

[8] A. Ashok, M. Govindarasu and J. Wang, "Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid," in Proceedings of the IEEE, vol. 105, no. 7, pp. 1389–1407, July 2017.

[9] S. Sridhar and M. Govindarasu, "Model-Based Attack Detection and Mitigation for Automatic Generation Control," in IEEE Transactions on Smart Grid, vol. 5, no. 2, pp. 580–591, March 2014.

[10] C.–W. Ten, C. Liu and G. Manimaran, "Vulnerability Assessment of Cybersecurity for SCADA Systems," in IEEE Transactions on Power Systems, vol. 23, no. 4, pp. 1836-1846, Nov. 2008.

[11] N. Liu, J. Zhang, H. Zhang and W. Liu, "Security Assessment for Communication Networks of Power Control Systems Using Attack Graph and MCDM," in IEEE Transactions on Power Delivery, vol. 25, no. 3, pp. 1492–1500, July 2010.

[12] C.–W. Ten, C. Liu and M. Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees," 2007 IEEE Power Engineering Society General Meeting, Tampa, FL, USA, 2007, pp. 1–8.

[13] H. Holm, K. Shahzad, M. Buschle and M. Ekstedt, "$P^2CySeMoL$: Predictive, Probabilistic Cyber Security Modeling Language," in IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 6, pp. 626–639, 1 Nov.–Dec. 2015.

[14] L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia. "An attack graph–based probabilistic security metric," in IFIP Annual Conference on Data and Applications Security and Privacy, pp. 283-296. Springer, Berlin, Heidelberg, Germany, 2008.

[15] M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel. "Time–to–compromise model for cyber risk reduction estimation," in Quality of Protection, pp. 49-64. Springer, Boston, MA, USA, 2006.

[16] A. Zieger, F. Freiling and K. Kossakowski, "The β–Time–to–Compromise Metric for Practical Cyber Security Risk Estimation," 2018 11th International Conference on IT Security Incident Management & IT Forensics (IMF), Hamburg, Germany, 2018, pp. 115–133.

[17] Y. Zhang, L. Wang, Y. Xiang and C.–W. Ten, "Power System Reliability Evaluation with SCADA Cybersecurity Considerations," in IEEE Transactions on Smart Grid, vol. 6, no. 4, pp. 1707–1721, July 2015.

[18] L. Wang, S. Jajodia, A. Singhal, and S. Noel. "k–zero day safety: Measuring the security risk of networks against unknown attacks," in European Symposium on Research in Computer Security, pp. 573–587. Springer, Berlin, Heidelberg, Germany, 2010.

[19] V. Venkataramanan, A. K. Srivastava, A. Hahn and S. Zonouz, "Measuring and Enhancing Microgrid Resiliency Against Cyber Threats," in IEEE Transactions on Industry Applications, vol. 55, no. 6, pp. 6303–6312, Nov.–Dec. 2019.

[20] C.–W. Ten, K. Yamashita, Z. Yang, A. V. Vasilakos and A. Ginter, "Impact Assessment of Hypothesized Cyberattacks on Interconnected Bulk Power Systems," in IEEE Transactions on Smart Grid, vol. 9, no. 5, pp. 4405–4425, Sept. 2018.

[21] A. Marotta, F. Martinelli, S. Nanni, A. Orlando, and A. Yautsiukhin, "Cyber-insurance survey," Computer Science Review, vol. 24, pp. 35-61, May 2017.

[22] R. Pal, L. Golubchik, K. Psounis and P. Hui, "Will cyber-insurance improve network security? A market analysis," IEEE INFOCOM 2014 – IEEE International Conference on Computer Communications, Toronto, ON, Canada, April-May 2014, pp. 235–243.

[23] S. Feng, Z. Xiong, D. Niyato and P. Wang, "Competitive Security Pricing in Cyber-Insurance Market: A Game-Theoretic Analysis," 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL, USA, Aug. 2018, pp. 1–5.

[24] P. Lau, W. Wei, L. Wang, Z. Liu and C. -W. Ten, "A Cybersecurity Insurance Model for Power System Reliability Considering Optimal Defense Resource Allocation," in IEEE Transactions on Smart Grid, vol. 11, no. 5, pp. 4403–4414, Sept. 2020.

[25] P. Lau, L. Wang, Z. Liu, W. Wei and C. -W. Ten, "A Coalitional Cyber-Insurance Design Considering Power System Reliability and Cyber Vulnerability," in IEEE Transactions on Power Systems, vol. 36, no. 6, pp. 5512-5524, Nov. 2021.

[26] M. Xu and L. Hua. "Cybersecurity insurance: Modeling and pricing," North American Actuarial Journal 23, no. 2 (2019): 220-249.

[27] C. Lai, G. Medvinsky, and B. Clifford Neuman. "Endorsements, licensing, and insurance for distributed system services," in Proceedings of the 2nd ACM Conference on Computer and Communications Security, pp. 170-175. 1994.

[28] "U.S. Cyber Market Outlook," Oct. 4, 2021. [Online]. Available: https://www.rpsins.com/knowledge-center/items/us-cyber-market-outlook/

[29] "The Evolution of Cyber Insurance," Jan. 23, 2020. [Online]. Available: https://prowritersins.com/cyber-insurance-blog/cyber-insurance/

[30] "Ransomware epidemic triggers major shift in cyber insurance market," Aug. 26, 2021. [Online]. Available: https://www.insurancebusinessmag.com/us/news/specialty-insurance/ransomware-epidemic-triggers-major-shift-in-cyber-insurance-market-307973.aspx

[31] "Baltimore transfers $6 million to pay for ransomware attack; city considers insurance against hacks," Aug. 28, 2019. [Online]. Available: https://www.baltimoresun.com/politics/bs-md-ci-ransomware-expenses-20190828-njgznd7dsfaxbbaglnvnbkgjhe-story.html

[32] "Biden official says ransomware will be addressed at every stop of President's foreign trip," June 12, 2021. [Online]. Available: https://www.cnn.com/world/live-news/biden-g7-summit-updates-06-12-2021-intl/h_ aa0f992358d2bf506901ffc19bd48df5

[33] "What You Need To Know About The Kaseya Ransomware Attack; And Why You Shouldnt Be Surprised," July 8, 2021. [Online]. Available: https://www.bitsight.com/blog/kaseya-ransomware-attack

[34] "2020 Saw 6% Rise in Number of CVEs Reported," Jan. 14, 2021. [Online]. Available: https://www.infosecurity-magazine.com/news/2020-saw-6-rise-in-number-of-cves/

[35] "The five worst cyberattacks against the power industry since 2014," Apr. 02, 2020. [Online]. Available: https://www.power-technology.com/features/the-five-worst-cyberattacks-against-the-power-industry-since2014/

[36] "Ukraine power cut 'was cyber-attack'," Jan. 11, 2017. [Online]. Available: https://www.bbc.com/news/technology-38573074

[37] "A cyber attack in Saudi Arabia failed to cause carnage, but the next attempt could be deadly," Mar. 20, 2018. [Online]. Available: https://www.independent.co.uk/news/long_reads/cyber-warfare-saudi-arabia-petrochemical-security-america-a8258636.html

[38] "Cyber Insurance Market Set to Grow at a CAGR of 21.4% by 2031: Visiongain Research Inc.," Aug. 12, 2021. [Online]. Available: https://www.globenewswire.com/en/news-release/2021/08/12/2279931/0/en/Cyber-Insurance-Market-Set-to-Grow-at-a-CAGR-of-21-4-by-2031-Visiongain-Research-Inc.html

[39] "Re/Insurance Cyber Rates Could Double Before 2023, as Attacks Skyrocket: S& P," Sep. 30, 2021. [Online]. Available: https://www.insurancejournal.com/news/international/2021/09/30/634535.htm

[40] "What Is Cyber Insurance, and Why Is It In High Demand?," June 1, 2021. [Online]. Available: https://www.gao.gov/blog/what-cyber-insurance%2C-and-why-it-high-demand

[41] "Cyber Insurance Market Growth & Performance," Dec. 22, 2020. [Online]. Available: https://amtrustfinancial.com/blog/agents/growth-of-the-cyber-insurance-market-agents

[42] "Cyber Risks In A New Era: Reinsurers Could Unlock The Cyber Insurance Market," Sep. 29, 2021. [Online]. Available: https://www.spglobal.com/ratings/en/research/articles/210929-cyber-risks-in-a-new-era-reinsurers-could-unlock-the-cyber-insurance-market-12118547

[43] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation," IEEE Trans. Power Syst., vol. 31, no. 6, pp. 4379-4394, Nov. 2016.

[44] B. B. Madan, K. Goeva-Popstojanova, K. Vaidyanathan, and K. S. Trivedi, "A method for modeling and quantifying the security attributes of intrusion tolerant systems," Perform. Eval., vol. 56, nos. 1-4, pp. 167-186, Mar. 2004.

[45] A. Rakhshan and H. Pishro-Nik, "Introduction to Probability, Statistics, and Random Processes: Statistics and Random Processes," Kappa Research, LLC, Blue Bell, PA, USA, 2014, Ch. 12, pp. 703-723.

[46] J. Dhaene, A. Tsanakas, E. A. Valdez, and S. Vanduffel, "Optimal capital allocation principles," J. Risk Insurance, vol. 79, no. 1, pp. 1-28, 2012.

[47] W. W. Weaver and P. T. Krein, "Game-theoretic control of small-scale power systems," IEEE Trans. Power Del., vol. 24, no. 3, pp. 1560-1567, Jul. 2009.

[48] D. Korzhyk, Z. Yin, C. Kiekintveld, V. Conitzer, and M. Tambe, "Stackelberg vs. Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness," J. Artif. Intell. Res., vol. 41, pp. 297-327, May 2011.

[49] P. Paruchuri, J. P. Pearce, J. Marecki, M. Tambe, F. Ordonez, and S. Kraus, "Efficient algorithms to solve Bayesian Stackelberg games for security applications," in Proc. 23rd Assoc. Adv. Artif. Intell. (AAAI) Conf. Artif. Intell., Chicago, IL, USA, Jul. 2008, pp. 1559-1562.

[50] J. Pita et al., "Deployed ARMOR protection: The application of a game theoretic model for security at the Los Angeles international airport," in Proc. 7th Int. Conf. Auton. Agents Multiagent Syst. (AAMAS), Estoril, Portugal, May 2008, pp. 125-132.

[51] J. Pita, M. Tambe, C. Kiekintveld, S. Cullen, and E. Steigerwald, "GUARDS: Game theoretic security allocation on a national scale," in Proc. 10th Int. Conf. Auton. Agents Multiagent Syst. (AAMAS), vol. 1. Taipei, Taiwan, May 2011, pp. 37-44.

[52] J. Tsai, Z. Yin, J. Kwak, D. Kempe, C. Kiekintveld, and M. Tambe, "Urban security: Game-theoretic resource allocation in networked domains," in Proc. 24th Assoc. Adv. Artif. Intell. (AAAI) Conf. Artif. Intell., Atlanta, GA, USA, Jul. 2010, pp. 881-886.

[53] E. Shieh et al., "Protect: A deployed game theoretic system to protect the ports of the United States," in Proc. 11th Int. Conf. Auton. Agents Multiagent Syst. (AAMAS), vol. 1, Valencia, Spain, Jun. 2012, pp. 13-20.

[54] B. An, J. Pita, E. Shieh, M. Tambe, C. Kiekintveld, and J. Marecki, "GUARDS and PROTECT: Next generation applications of security games," in Proc. ACM Special Interest Group Econ. Comput. (SIGecom) Exchanges, 2011, pp. 31-34.

[55] C. Kiekintveld, M. Jain, J. Tsai, J. Pita, F. Ordez, and M. Tambe, "Computing optimal randomized resource allocations for massive security games," in Proc. 8th Int. Conf. Auton. Agents Multiagent Syst. (AAMAS), Budapest, Hungary, May 2009, pp. 689-696.

[56] M. Jain et al., "Software assistants for randomized patrol planning for the LAX airport police and the federal air marshal service," Inst. Oper. Res. Manag. Sci. J. Appl. Anal., vol. 40, no. 4, pp. 267-290, 2010.

[57] J. Tsai, S. Rathi, C. Kiekintveld, F. Ordez, and M. Tambe. "IRIS A tool for strategic security allocation in transportation networks," in Proc. 8th Int. Conf. Auton. Agents Multiagent Syst. (AAMAS), Budapest, Hungary, May 2009, pp. 37-44.

[58] D. Korzhyk, V. Conitzer, and R. Parr, "Complexity of computing optimal stackelberg strategies in security resource allocation games," in Proc. 24th Assoc. Adv. Artif. Intell. (AAAI) Conf. Artif. Intell., Atlanta, GA, USA, Jul. 2010, pp. 805-810.

[59] C. Grigg et al., "The IEEE reliability test system-1996. A report prepared by the reliability test system task force of the application of probability methods subcommittee," IEEE Trans. Power Syst., vol. 14, no. 3, pp. 1010-1020, Aug. 1999.

[60] W. Nzoukou, L. Wang, S. Jajodia and A. Singhal, "A Unified Framework for Measuring a Network's Mean Time-to-Compromise," 2013 IEEE 32nd International Symposium on Reliable Distributed Systems, Braga, Portugal, 2013, pp. 215-224.

[61] N. Poolsappasit, R. Dewri and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs," in IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 1, pp. 61-74, Jan.-Feb. 2012.

[62] M. Schiffman, "Common Vulnerability Scoring System (CVSS)," `http://www.first.org/cvss/`

[63] L. Han, T. Morstyn and M. McCulloch, "Incentivizing Prosumer Coalitions with Energy Management Using Cooperative Game Theory," in IEEE Transactions on Power Systems, vol. 34, no. 1, pp. 303-313, Jan. 2019.

[64] C. Stevanoni, Z. De Grve, F. Valle and O. Deblecker, "Long-Term Planning of Connected Industrial Microgrids: A Game Theoretical Approach Including Daily Peer-to-Microgrid Exchanges," in IEEE Transactions on Smart Grid, vol. 10, no. 2, pp. 2245-2256, March 2019.

[65] K. Dehghanpour and H. Nehrir, "An Agent-Based Hierarchical Bargaining Framework for Power Management of Multiple Cooperative Microgrids," in IEEE Transactions on Smart Grid, vol. 10, no. 1, pp. 514-522, Jan. 2019.

[66] M. Touhiduzzaman, A. Hahn and A. K. Srivastava, "A Diversity-Based Substation Cyber Defense Strategy Utilizing Coloring Games," in IEEE Transactions on Smart Grid, vol. 10, no. 5, pp. 5405-5415, Sept. 2019.

[67] A. Sinha, F. Fang, B. An, C. Kiekintveld, and M. Tambe, "Stackelberg security games: Looking beyond a decade of success," Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence (IJCAI-18), Stockholm, Sweden, July 13-19, 2018, pp. 5494-5501.

[68] I. Vakilinia and S. Sengupta, "A Coalitional Cyber-Insurance Framework for a Common Platform," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 6, pp. 1526-1538, June 2019.

[69] P. Lammich and R. Neumann, "A framework for verifying depth-first search algorithms," Proceedings of the 2015 Conference on Certified Programs and Proofs (CPP-15), Mumbai, India, pp. 137-146, Jan. 2015.

[70] B. Falahati, Y. Fu and M. J. Mousavi, "Reliability Modeling and Evaluation of Power Systems with Smart Monitoring," in IEEE Transactions on Smart Grid, vol. 4, no. 2, pp. 1087-1095, June 2013.

[71] P. Ghazizadeh, R. Florin, A. G. Zadeh and S. Olariu, "Reasoning About Mean Time to Failure in Vehicular Clouds," in IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 3, pp. 751-761, March 2016.

[72] C. Wang, T. Zhang, F. Luo, F. Li and Y. Liu, "Impacts of Cyber System on Microgrid Operational Reliability," in IEEE Transactions on Smart Grid, vol. 10, no. 1, pp. 105-115, Jan. 2019.

[73] L. S. Shapley, "A value for n-person games." Contributions to the Theory of Games, 2(28), 307-317, 1953.

[74] L. S. Shapley, "Cores of convex games." International Journal of Game Theory, 1(1), 11-26, 1971.

[75] R. Serrano, "Cooperative games: Core and Shapley value," no. 2007-11. Working Paper, 2007.

[76] C. Barrows et al., "The IEEE Reliability Test System: A Proposed 2019 Update," in IEEE Transactions on Power Systems, vol. 35, no. 1, pp. 119-127, Jan. 2020.

[77] G. Cao et al., "Operational Risk Evaluation of Active Distribution Networks Considering Cyber Contingencies," in IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 3849-3861, June 2020.

CURRICULUM VITAE

Pikkin Lau

Education

Ph.D., University of Wisconsin-Milwaukee, Milwaukee, WI, Dec. 2021

M.S., Washington State University, Pullman, WA, Jul. 2017

B.S., National Taiwan University, Taipei, Taiwan, Jul. 2011

Dissertation Title

AN INSURANCE FRAMEWORK FOR CYBER-PHYSICAL POWER SYSTEMS CONSIDERING INTEGRATED CYBERSECURITY-RELIABILITY ASSESSMENT

Teaching Experiences

- Lab Instructor, Fundamentals of Electrical Engineering, University of Wisconsin-Milwaukee, Fall 2021.
- Lab Instructor, Electromechanical Energy Conversion, University of Wisconsin-Milwaukee, Spring 2018.
- Lab Instructor, Fundamentals of Electrical Engineering, University of Wisconsin-Milwaukee, Fall 2017.

Awards

- Chancellor's Graduate Student Award, Spring 2020.
- IEEE Transactions on Power Systems Outstanding Reviewer, 2020.

- IEEE Transactions on Power Systems Outstanding Reviewer, 2019.

Peer-reviewed Publications:

[1] **P. Lau**, W. Wei, L. Wang, Z. Liu and C. -W. Ten, "A Cybersecurity Insurance Model for Power System Reliability Considering Optimal Defense Resource Allocation," *in IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 4403-4414, Sept. 2020.

[2] **P. Lau**, L. Wang, Z. Liu, W. Wei and C. -W. Ten, "A Coalitional Cyber-Insurance Design Considering Power System Reliability and Cyber Vulnerability," *in IEEE Transactions on Power Systems*, vol. 36, no. 6, pp. 5512-5524, Nov. 2021.