國立臺灣大學管理學院資訊管理研究所

碩士論文

Department of Information Management

College of Management

National Taiwan University

Master Thesis

考量惡意攻擊與天然災害下確保服務持續性之有效資源配置策略

Effective resource allocation strategies to assure service continuity considering malicious attacks and natural disasters

李佳玲

Chia Ling Lee

指導教授：林永松 博士

Advisor: Frank Yeong-Sung Lin, Ph.D.

中華民國 102 年 7 月

July 2013

國立臺灣大學碩士學位論文
口試委員會審定書

考量惡意攻擊與天然災害下確保服務持續性之有效資源配置策略

本論文係李佳玲君（學號 R00725045）在國立臺灣大學資訊管理學系、所完成之碩士學位論文，於民國 102 年 7 月 26 日承下列考試委員審查通過及口試及格，特此證明

口試委員：　　　　　　　　林永松

所　　長：

致謝

研究所兩年的時間一下就過去了，十分感謝林永松老師在這期間的悉心指導與建議，才能使論文順利完成。並且也從老師身上學習到很多，對研究的態度、做事的方法條理等，都讓我受益良多。也感謝輔仁大學資工系的呂俊賢教授、台北大學資工系的莊東穎教授以及清華大學電機系的趙啟超教授撥冗擔任口試委員，提供很多寶貴的建議，讓整個論文能夠更加完善。

此外也要猷順學長這段期間的幫助與指導，耐心的協助我們解決大大小小的問題，論文也才能夠順利的完成。也感謝一起奮鬥的聿軒、端駿以及其他研究所的同學，一起討論、寫程式、吃飯、聊天，讓寫論文的過程還有碩班的生活開心許多。同時也要感謝實驗室的學弟妹維文、怡棠、人華和怡蓁的協助和關心，未來該你們加油了！

最後我要感謝我的父母與家人，在我累的時候幫我打氣，聽我發牢騷，並且煮好吃的菜幫我恢復元氣，真是辛苦你們了！未來就該我認真工作照顧你們。也感謝其他朋友對我的關心和鼓勵，不時的送點心和飲料，讓我更開心的寫論文，未來也要一起加油努力！

李佳玲 謹致

于國立台灣大學資訊管理研究所

中華民國一百零二年七月

Thesis Abstract

Effective resource allocation strategies to assure service continuity considering malicious attacks and natural disasters

Name: Chia Ling, Lee

Advisor: Frank Yeong-Sung Lin, Ph.D.

Companies or governments rely on Internet to provide all kinds of service to customers and use Internet to propagate them in order to attract more customers to create more profits. Not only external customers, within the company, they also build their own intranet to handle daily operations. Once companies' network being broken, they cannot provide regular service to user and also cannot run the daily process which may cause serious problem. Therefore, according to some research, cyber-attacks still is the most significant risk that business worried about since cyber-attacks will cause serious damage to company.

In addition, in recent decades, damage caused by natural disaster becomes more and more serious and happened more frequently than before. The number of disaster events reported globally increased from 1,690 to 3,886 and the economic losses also increase dramatically. Hence, in our thesis we want to add natural disaster this environment variable to our scenario. Companies need to start to pay attention on it when they are building their system. We discuss earthquake, secondary disaster-fire and fire in our scenario.

In order to provide business continuity, we also adopt redundancy this defense strategy to increase survivability. It is an effective method to prevent service interruption. When nodes damage or temporary shutdown, they can activate redundancy immediately which can prevent service interrupted. There are also other defense strategies to help defender maximize their system survivability such as virtualization, deploying honeypot, and cloud security

Our purpose is to help defender find out effective defense strategy and resource allocation. Our problem is a bi-level problem and we use mathematical programming combined Monte Carlo Stimulation to help us solve this complex problem since there are various of attack and defense strategies and full of uncertainty. Furthermore, we will do both commander and defender enhancement process in order to find out better solution.

Keywords: Collaborative Attack, Network Survivability, Natural Disaster, Secondary Disaster, Redundancy, Resource Allocation, Optimization, Mathematical Programming, Stimulation

論文摘要

論文題目:考量惡意攻擊與天然災害下確保服務持續性之有效資源配置策略

作者：李佳玲

指導教授：林永松 博士

現在各行各業或是政府幾乎都會使用網路提供服務給客戶，並且公司內部也會使用網路來作為內網的連結，公司內部許多的系統也是要用到網路。駭客就很常針對這些元件、系統來做攻擊，要是攻擊成功，常常會造成很大的損失。最直接的就是無法提供服務，間接的也會造成顧客的不信賴，甚至機密資料遭受竊取所造成的後果更加嚴重。因此每年公司還是會花很多的資金在防止網路攻擊造成的損失，尤其最近很盛行的協同攻擊，容易造成更大的破壞力，公司需要納入考量。

最近天災頻傳，尤其地震帶來的災害更是大面積的破壞，像是日本311大地震、四川大地震，都造成很大的損失，另外地震伴隨的火災也常造成更嚴重的損害。另外火災也常因為擴散性造成整個區域的燒毀，整個廠房常常就付之一炬，並且其發生的頻率更是高過大型的天然災害幾百倍，累加起來的損失也是不容忽視。

我們的目標就是希望能夠找出有效的防禦方法，來幫助企業在面臨惡意攻擊和天然災害仍能維持提供一定水準的服務，維持服務不中斷。本研究採用了在實務

界很常使用的方法:redundancy 來讓服務不間斷。

本研究使用數學規劃合併 Monte Carlo Simulation 來解決這個複雜、充滿 randomness 的問題，用模擬的方式來模擬整個 network 以更貼近現實，找到有效的防禦方法。並且也會持續做 enhancement process 以找到最佳的資源配置。

關鍵字: 協同攻擊、天然災害、網路存活度、數學規劃法、模擬、備援、最佳化、資源配置

Table of Contents

List of Figures

List of Tables

Chapter 1 Introduction

1.1 Background

Internet has become one of the most significant technologies in this generation. We all need and use Internet every day. We use Internet to search information, receive e-mails, buy things, chat with friends, etc. Companies or governments also rely on Internet to provide all kinds of service to customers and also use Internet to propagate themselves in order to attract more customers to create more profits. Not only external customers, within the company, they also build their own intranet to handle daily operations. Once companies' network broken, they cannot provide regular service to user and also cannot run the internal process or might be inefficient which will cause serious loss.

In the worldwide, there will be a lot of hackers or criminal crimes want to attack to gain some profits or even for fun. According to the Symantec "2011 State of Security Survey" report [1], the top sources of security threats is hackers and the following are well-meaning insiders and targeted attacks as we can see at Figure 1-1. Business top worried event is cyber-attacks and the following are IT incidents caused by well-meaning insiders, internally generated IT-related threats, traditional criminal activity, brand-related events, natural disasters and terrorism as you can see at Figure

1-2. 1 means the most significant to business and 7 means least significant to business. Cyber-attacks still is the most significant risk that business worried about.

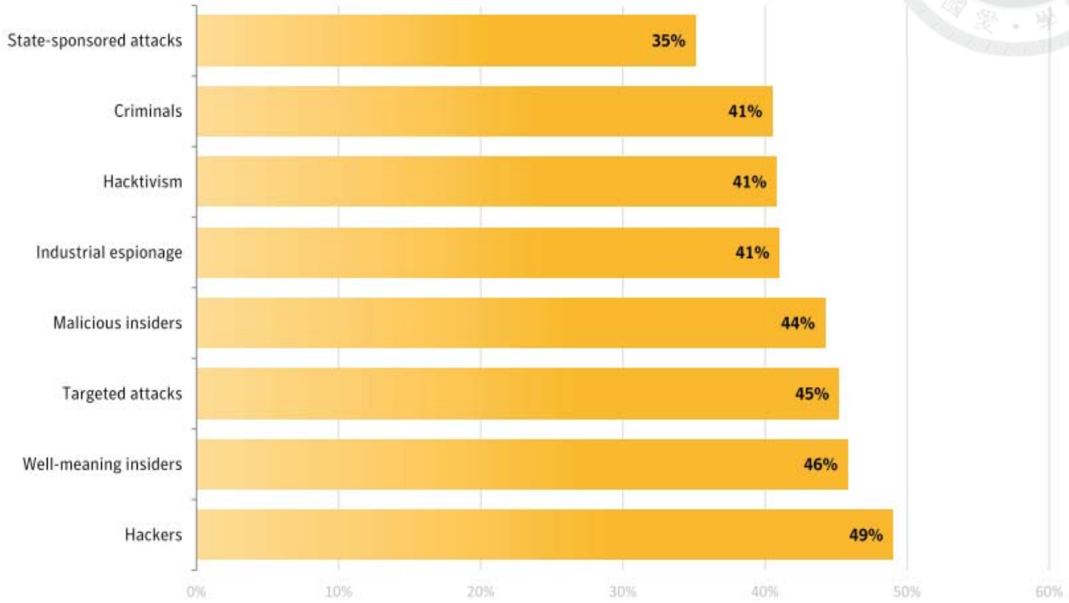


Figure 1-1: The sources of security threats' ranking [1]

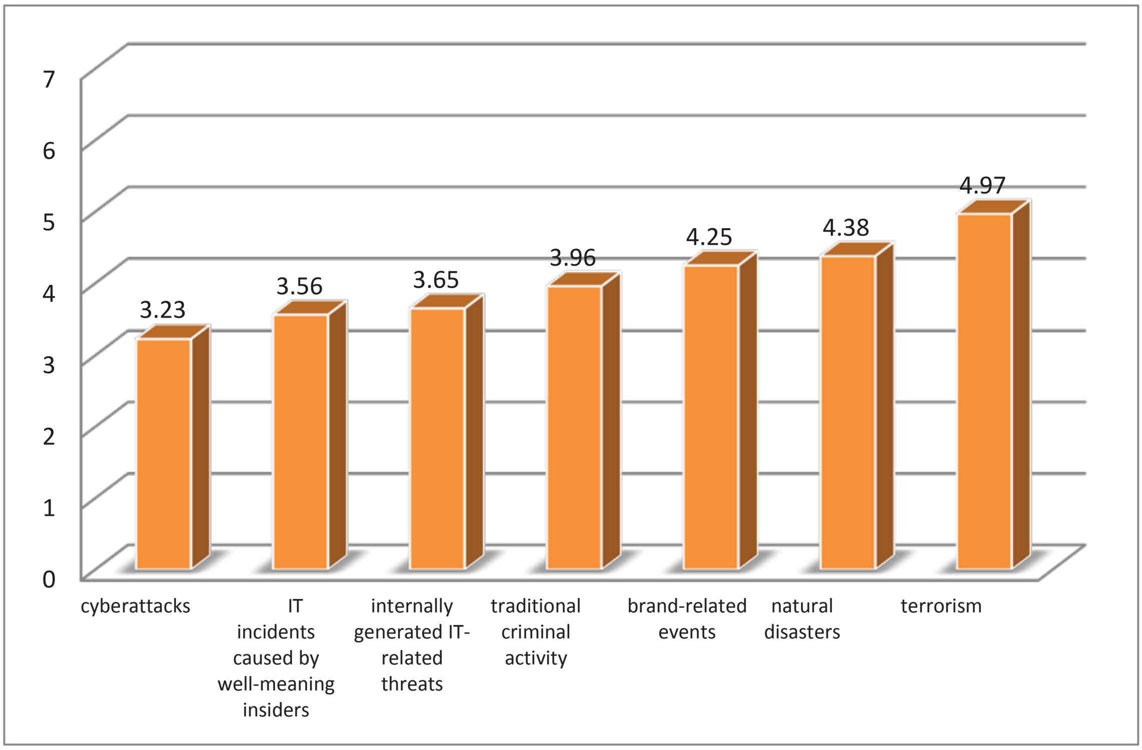


Figure 1-2: The business risk rank to business [1]

Cyber-attacks cause serious damage to company. According to Ponemon Institute “2012 Cost of Cyber Crime Study: United Kingdom” report [2]they divide into two parts: cost for external consequence and cost by internal activity center as shown in Figure 1-3 and Figure 1-4. Cyber-attacks may cause business operation disruption which may not only let legitimate users cannot use service but also internal operation cannot work, either. That will indirectly let companies’ revenue decrease. Attacker’s goal sometimes is to steal confidential information, if success it will cause serious problem. For example, Sony admitted 77 million PlayStation Network and Qriocity online service customers that their credit-card data, billing addresses and other personal information may have been stolen by a hacker [3. It caused Sony’s stock price dropped dramatically and Sony’s reputation severely damaged.

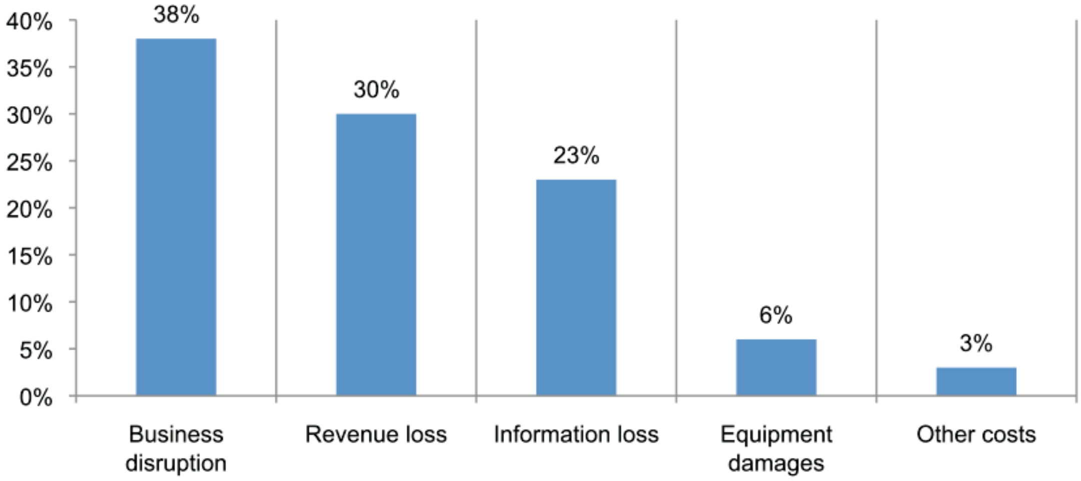


Figure 1-3: Percentage cost for external consequence [2]

Within the company, they also need spend lots of budget to recover their network after cyber-attacks and need to keep detecting abnormal behavior in order to decrease the probability of cyber-attacks happened.

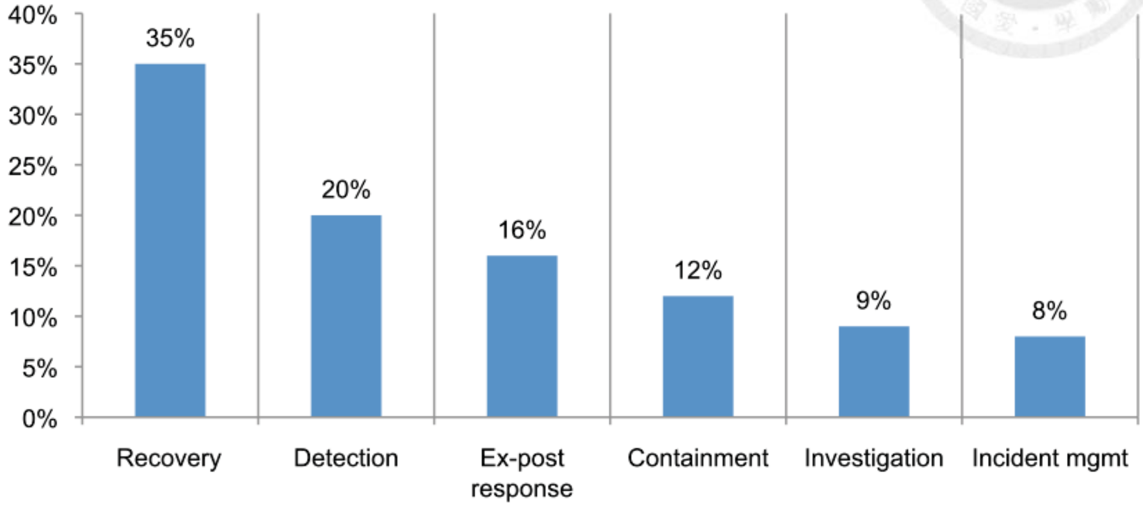


Figure 1-4: Percentage cost by internal activity center [2]

Worst of all, according to [1] review 3,300 businesses, ranging from five to more than 5,000 employees. About 41 percent think cyber security is more important today than before. In the Report of McAfee [4], there are many new malware being founded and updated into their database as showed in Figure 1-5. The total malware samples in the database are showed in Figure 1-6. Web application vulnerabilities also show as a rising trend as we can see in Figure 1-7 the report of IBM [5].

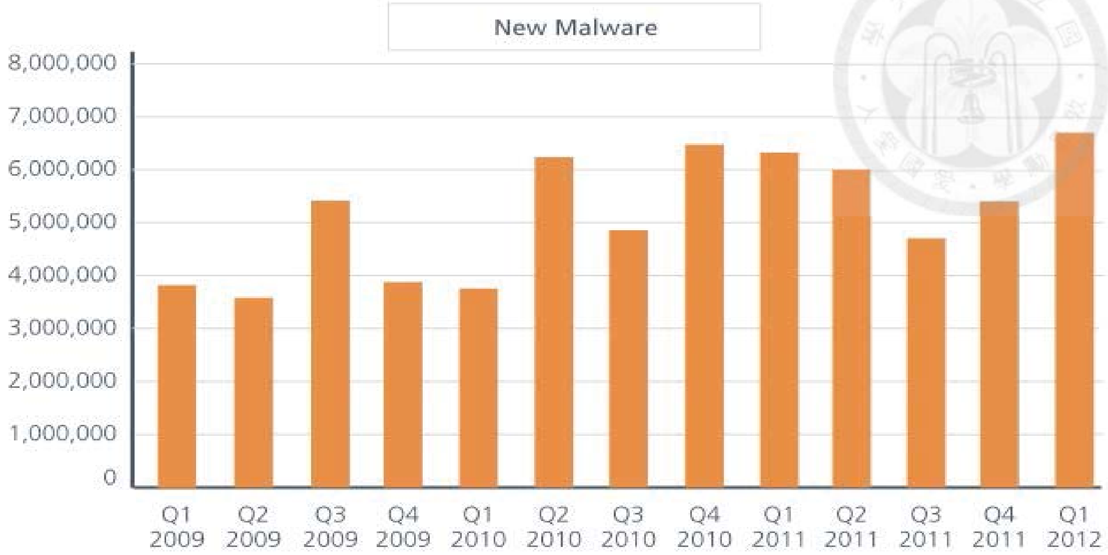


Figure 1-5: Numbers of New Malware [4]

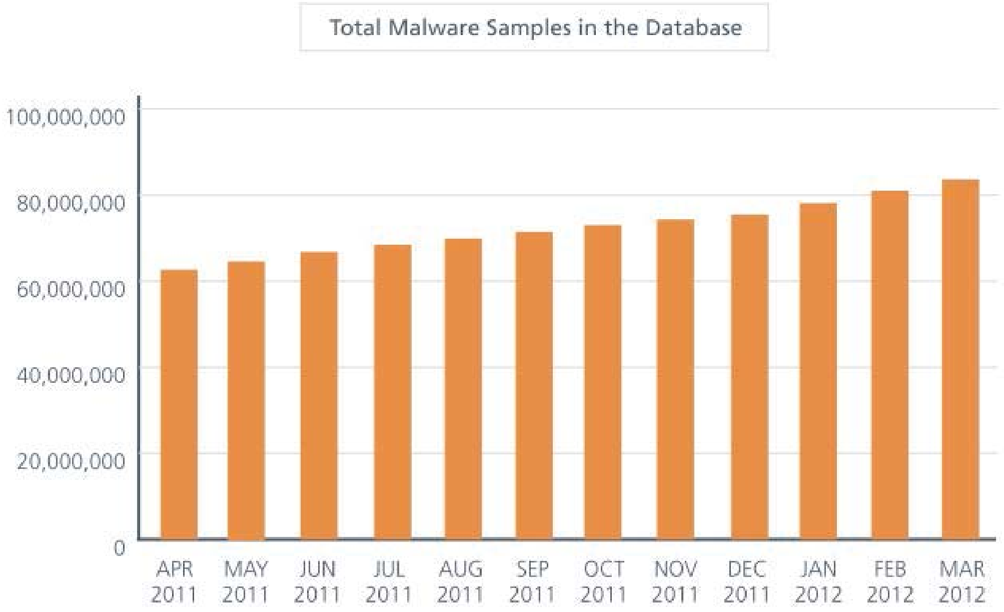


Figure 1-6: Total Malware samples in the database [4]

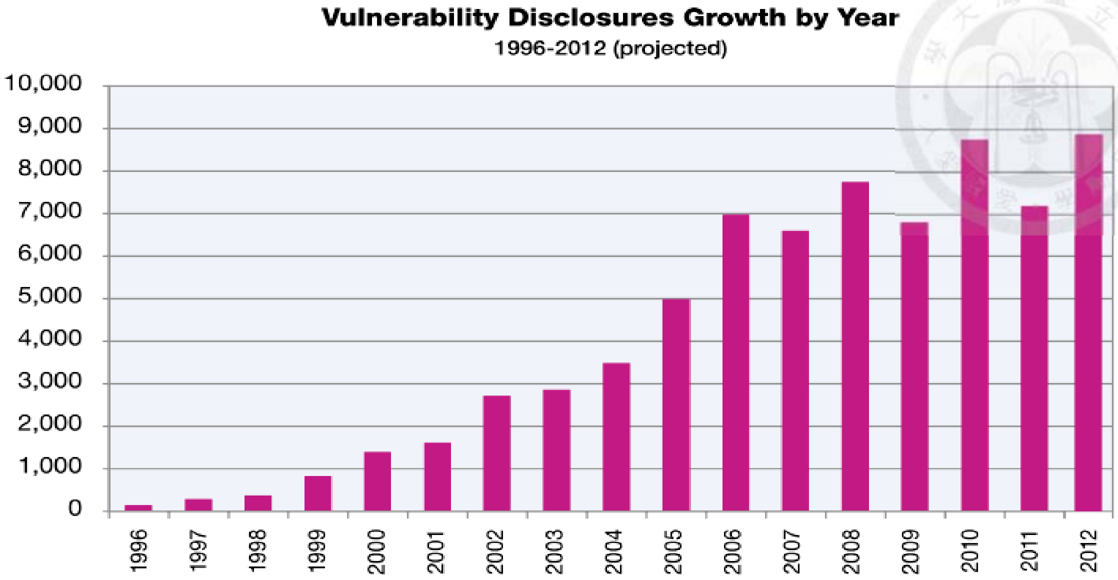


Figure1-7: Vulnerability Disclosures Growth by Year [5]

The following Figure 1-8 shows the top attacking type in 2012. “Unreported” category is because insufficeint logging or publid disclosure resistance. We still can see the following rank order is SQL injection, Denial of servvice, banking Trojan and so on.

Since cyber-attacks caused serious damage every year, companies spend lots of money to secure their network in order to provide safe network to decrease the loss. More than 10% companies spend 18.6% of their IT budget on security, 16.5% companies spend 16.5% of their IT budget on security and rest of the data is showed at Figure 1-9.

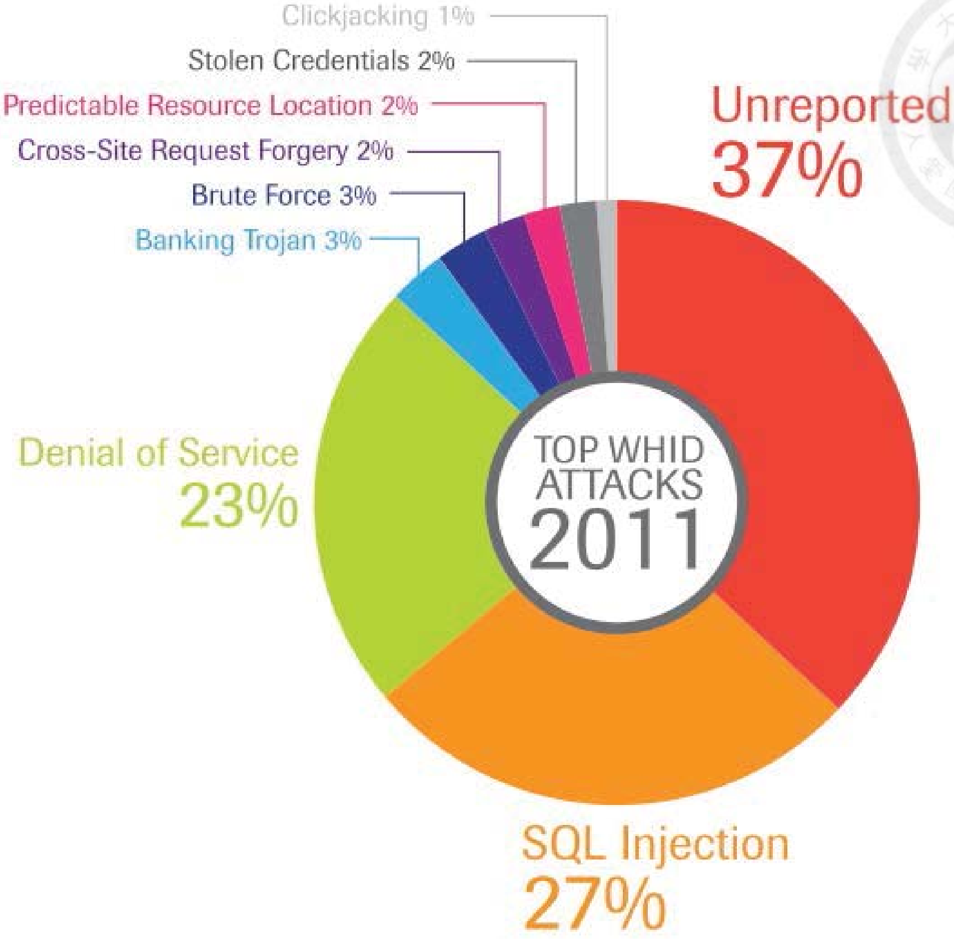


Figure 1-8: Top attacking type distribution in 2012 [6]

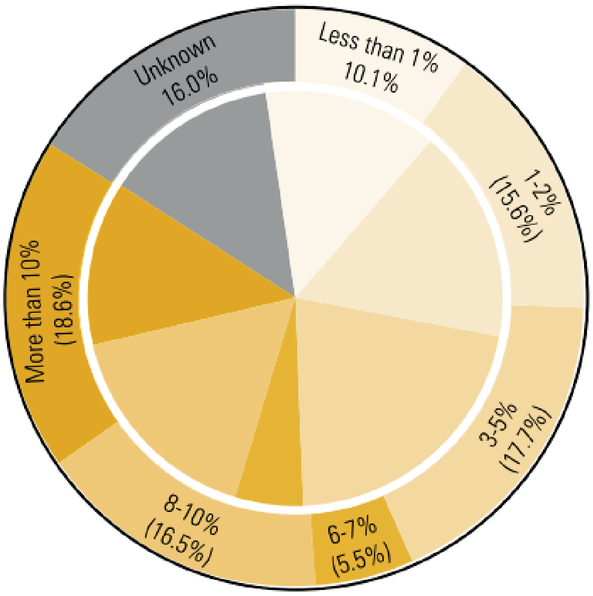


Figure 1-9: Percentage of IT budget spent on security [7]

Another issue is natural disaster. Even though natural disaster is the sixth significant business risk as we mentioned before in Figure 1-2, but recent decades, natural disaster brings damage become more and more serious and happened more frequently than before. As you can see in Figure 1-10 and Figure 1-11, the number of disaster events reported globally increased from 1,690 to 3,886 and the economic losses also increase a lot [8]. Based on the reported losses of all types of disasters in the EM-DAT database, the modelled economic exposure of Asia-Pacific sub regions indicates that estimated economic losses associated with all disasters continue to grow every year with the increasing exposure [9].

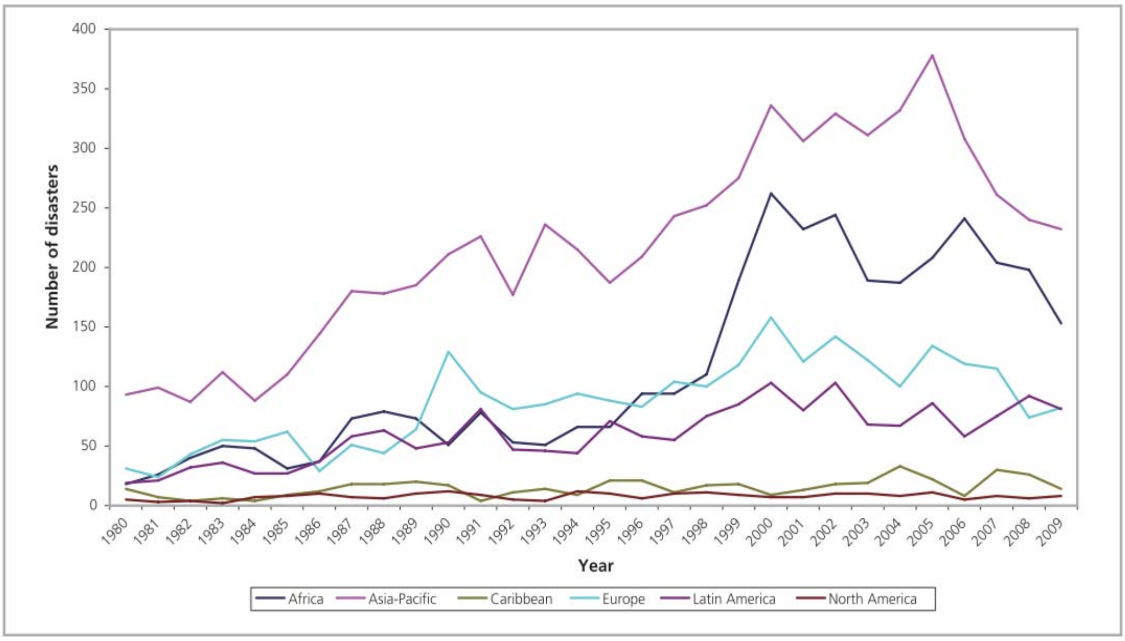


Figure 1-10: Reported disasters, by global region, 1980-2009 [8]

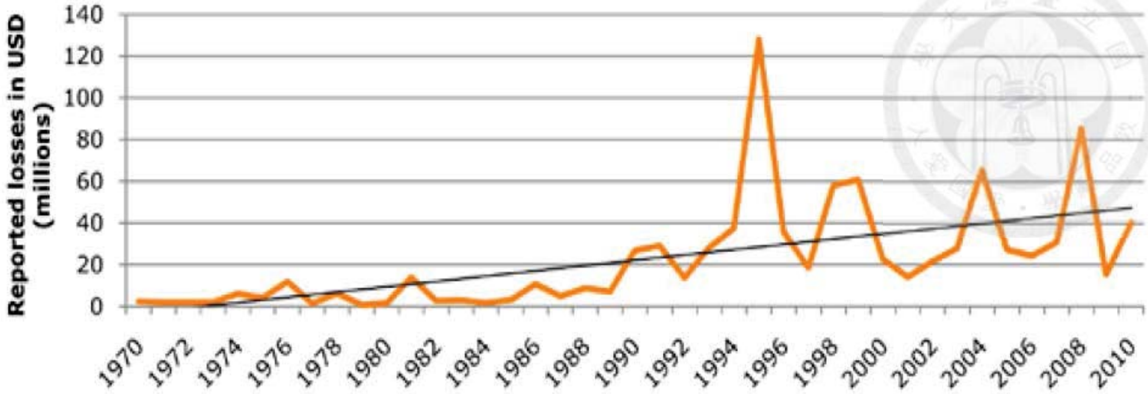


Figure 1-11: Economic losses due to disasters in Asia and Pacific [9]

1.2Motivation

As technology make progress, advanced attack tools and strategies are developed in these days just like we mentioned like Figure 1-5. Anti-virus can find new virus every day and also have more virus which are not found, yet. Also, there is a new attack method called collaborative attack which might represent the next generation cyber-attacks [10]. Collaborative attack becomes popular and being used frequently recently. Using collaborative attack which is more than two attackers attack together can enhance success probability and can spend relatively fewer budgets to compromise the target which is good news to attackers; attackers can use budget efficiently and have more chance to win the competition. Hence, companies need to considered all kinds of attacking strategy, tools and method in order to come up with a better defense strategy to against cyber-attacks,

On the other hands, since natural disaster happened more frequently in recent decades and cause huge damage no matter in casualty or economic loss as we mentioned before in Figure 1-10 and Figure 1-11. Also, many huge natural disasters happened in recent years, such as Japan 311 tsunami, Sichuan Province earthquake, Hurricane Katrina and so on which often let us losses heavily. Many companies' engine room or the whole plant are destroy by natural disaster which may cause company's operation shut down and cannot provide service to their clients. Therefore, in this paper we want to add natural disaster this environment variable to our scenario in order to let defender can add this factor to their future planning phase to prevent in advance. Companies need to start considering this part of damage and take some counterplans to deal with it.

Our purpose is to help companies to find an efficiency way to deal with varieties of threats. In nowadays, there also have all kinds of dense strategy and method to increase their defense intensity. In [11], their main purpose is to find the most appropriate defense strategy under different attacking conditions based on game theory and contrariwise. We also want to find out which defense methods are much useful. The common defense methods are firewall, anti-virus software, anti-spyware software, etc. In addition to those common defense mechanisms, we add other defense technology called reactive defense like honeypot, virtualization, cloud security service, etc. Besides, since companies need to face natural disaster's wreck, we use a common mechanism to help them can continue providing service. Redundancy is an effective way to make sure service won't be interrupted. Especially face natural disaster easily causes large-scale destruction and the same area usually will be destroyed, too. Remote backup can take over and keep providing service to users.

When choosing defense strategies, defender only can use limited budget to protect their network. Our goal is to use limited budget to protect the network, so defender need to well-arranged resource allocation between proactive defense resource and reactive defense resource and find out most effective way to deal with different kinds of attacking strategy and natural disaster under the assumption that attackers can maximized service compromise probability.

1.3Literature Survey

1.3.1 Survivability

In our thesis, we use survivability as the metric to evaluate system or network performance. We are not using "activate" or "failure" only two statuses to display system's status. Survivability can show more than just two statuses. We adopt [12] clear definition of survivability as below: "*We define survivability as the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents. We use the term system in the broadest possible sense, including networks* *and large-scale systems of systems.*” Therefore, in our scenario is defender needs to face malicious attack , natural disaster or other threats still can provide good enough service to legitimate users in a timely manner. There are more definitions of survivability in Table 1-1.

Table 1-1: Summary of Definitions of Survivability

NO	Definition	Researcher(s)	Year	Origin
1	We define survivability as the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents. We use the term system in the broadest possible sense, including networks and large-scale systems of systems	R.J. Ellison, D.A. Fisher, R.C. Linger, H.F. Lipson, T. Longstaff, and N.R. Mead	1997	[12]
2	Survivability is the capacity of a system to provide essential services even after successful intrusion and compromise, and to recover full services in a timely manner.	H.F. Lipson, N.R. Mead, and R.C. Linger	1998	[13]
3	The capability of a network system to complete its mission in a timely manner, even if significant portions are incapacitated by attack or accident.	N.R. Mead	1999	[14]
4	In this work, we address survivability to	D. Medhi and D.	2000	[15]

	provide network design and management procedures towards minimizing the impact of failures on multi-networks.	Tipper		
5	A survivable system is one that satisfies It’s survivability specification of essential services and adverse environments.	A.P. Moore and R.C. Linger	2001	[16]
6	Survivability is the ability of a given system with a given intended usage to provide a pre-specified minimum level of service in the event of one or more pre-specified threats.	V.R. Westmark	2004	[17]
7	In this research, survivability is considered from two perspectives: (1) lost capacity over time, and (2) how often an outage impact threshold is exceeded.	A. Snow, G. Weckman, and P. Rastogi	2005	[18]
8	In the design of secure and survivable wireless sensor networks, survivability implies that networks should have the capability to operate under node failures and attacks.	D. Tipper, K. Lu, and Y. Qian	2007	[19]
9	Survivability can conceptually be considered as a system's capability to endure catastrophic failures, such as a network system under malicious intrusions, but still preserve mission	A.W. Krings and Z. Ma	2008	[20]

	critical functionalities.			
10	Survivability is the system’s ability to continuously deliver services in compliance with the given requirements in the presence of failures and other undesired events.	P.E. Heegaard, and K.S. Trivedi	2009	[21]
11	Survivability is viewed as the capability of the system to deliver certain degree of services in the advent of failure.	J. Huang, J. Jiang, and L. Zhang	2010	[22]

1.3.2 Collaborative Attack

Traditionally, hackers often attack alone which is known as individual cyber-attacks. Beside the individual attack, there are more and more collaborative attacks have been disclosed. Recently, collaborative attack becomes more popular. Collaborative attacks might represent the next generation cyber-attacks [10]. Collaborative attacks are launched by multiple attackers which gives them some advantages. By adopting collaborative attack, attackers in the attacking group can share their information, resource, allocate the tasks and synchronize to do the cooperation before or during the attack. There are some advantages of collaborative attack shows in [23]. First, coordinated attacks could be designed to avoid detection. Second, it is difficult to differentiate between decoy and actual attacks. Third, there is a large variety of coordinated attacks.

There is another special effect when adopt collaborative attack called “synergy”. Synergy is a phenomenon that “1+1>2” which is means the sum of two attackers’ works is less than they work together. We will introduce in detail in chapter 2.

Based on the above advantages, if attackers want to attack critical components, they can adopt collaborative attack which is more powerful than single attackers and it will have higher success probability.

1.3.3 Natural disaster

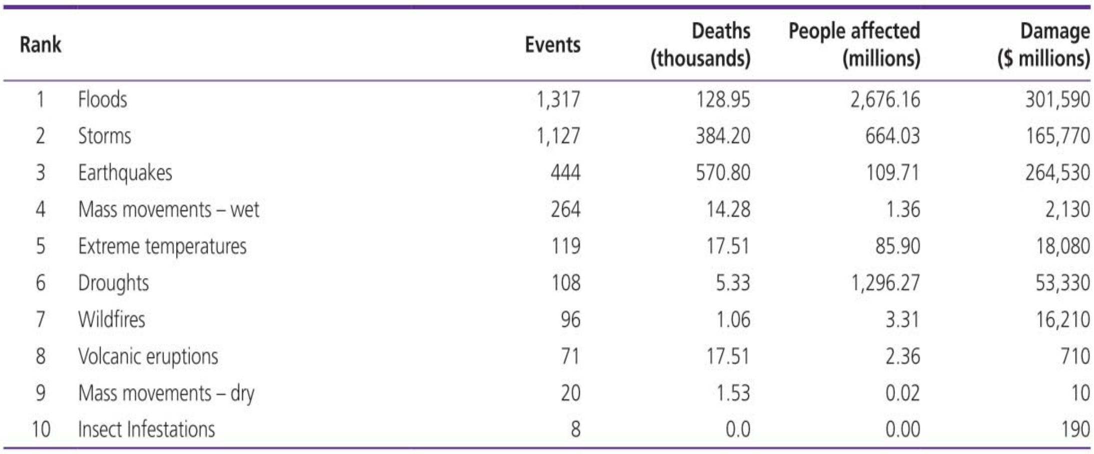
As we mentioned before, since natural disaster happened more frequently in recent decades and will cause serious damage (Figure 1-10 and Figure 1-11), so we want to add natural disaster this factor into discuss.

- **Earthquake:**

There are all kinds of natural disaster, but most harmful might be earthquake. The [8] report also show the top 10 disaster types and their impact in Asia and Pacific in 1980 to 2009 as Table 1-2. Although flood and storm rank first and second, it is partly because these two natural disasters happened more frequently. Once big earthquake happened, it will cost serious damage no matter in casualties or economic loss. As you can see at Table 1-1, only 444 earthquakes caused 570,800 people dead which is four times larger than floods and loss 264,530,000,000 dollars which is greater than storms.

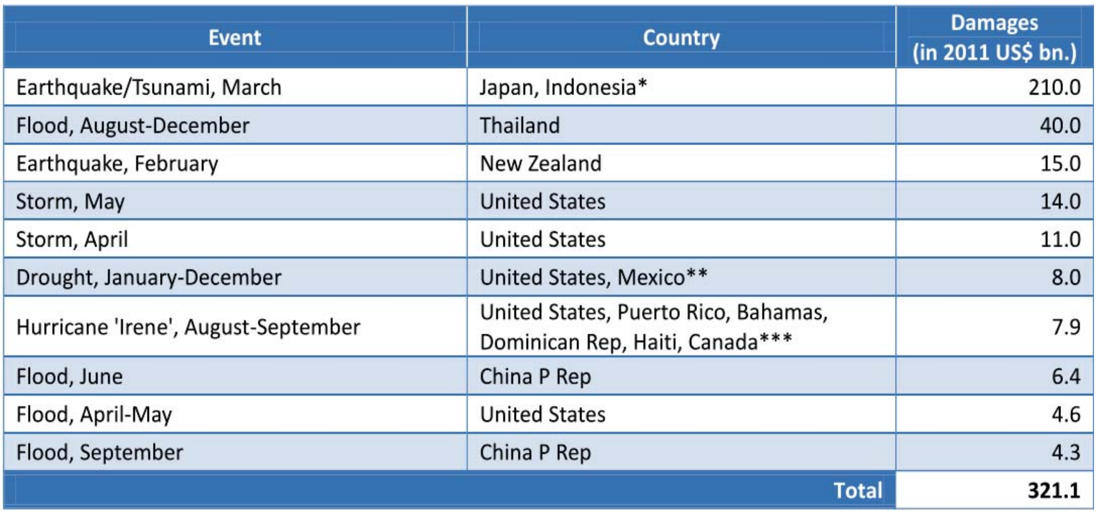
The top 10 natural disasters by economic damages are showed in Table 1-2 [24] and two of the top three are the earthquake. The damage caused by Japan 311 earthquake is the total loss of two-third. It shows that earthquake really causes large-scale and huge damage once it happened. Also because earthquake is un-predictable and both defender and attacker cannot prepare to its coming, so we choose earthquake this natural disaster to discuss.

Table 1-2: Top 10 disaster types and their impact, 1980-2009 [8]



Rank		Events	Deaths (thousands)	People affected (millions)	Damage ($ millions)
1	Floods	1,317	128.95	2,676.16	301,590
2	Storms	1,127	384.20	664.03	165,770
3	Earthquakes	444	570.80	109.71	264,530
4	Mass movements – wet	264	14.28	1.36	2,130
5	Extreme temperatures	119	17.51	85.90	18,080
6	Droughts	108	5.33	1,296.27	53,330
7	Wildfires	96	1.06	3.31	16,210
8	Volcanic eruptions	71	17.51	2.36	710
9	Mass movements – dry	20	1.53	0.02	10
10	Insect Infestations	8	0.0	0.00	190

Table 1-3: Top 10 natural disasters by economic damages [24]



Event	Country	Damages (in 2011 US$ bn.)
Earthquake/Tsunami, March	Japan, Indonesia*	210.0
Flood, August-December	Thailand	40.0
Earthquake, February	New Zealand	15.0
Storm, May	United States	14.0
Storm, April	United States	11.0
Drought, January-December	United States, Mexico**	8.0
Hurricane 'Irene', August-September	United States, Puerto Rico, Bahamas, Dominican Rep, Haiti, Canada***	7.9
Flood, June	China P Rep	6.4
Flood, April-May	United States	4.6
Flood, September	China P Rep	4.3
	Total	**321.1**

Besides, sometimes secondary disasters may bring more serious damage than primary disaster [25] such as fir following earthquake is an example. Earthquake accompanied by strong shaking easily causes gas systems and electrical systems damage which is the top reason that brings fire. In addition, outside of the building, pipelines and electric transmission lines are easily cause ignitions which resulting in a large-scale fire [26]. For example, the Osaka-Kobe earthquake in 1995 brings 285 ignitions and more than 1 billion meter squares being burned after the earthquake [27]. The California Earthquake of April 18, 1906 also cause more than 50 ignitions and the fire keep burning about 3 days [28]. Therefore, we not only need to watch out primary disaster but also pay attention to secondary disaster and even though we cannot predict it's coming but we can take some measure in advance in order to decrease to losses as many as possible.

- Fire:

Even though fire isn't a grave natural disaster compare to other natural disasters, we still want to add this factor to our thesis. Because fire also influences large range, its fit natural disaster's characteristic. Fire often spread to neighboring area and cause the whole area being destroyed totally. In the fire range, almost nothings can still work after the fire including those providing service's machine. Fire happened frequency is 300 times than flood as we can see in Table 1-4. In every year, fire also causes damage and loose also a big number it is part of because the probability happened fire is much higher than other natural disaster. According to the research from U.S Fire Administration there are 447,000 fires happened in America, cause2,635 people died in fire and loss 9,047,600,000 dollars in 2010 [29].

Table 1-4: Numbers of fire and damage, 2006-2010 [29]

Year	**Fires**	**Deaths**	**Dollar Loss**
2006	491,600	2,565	$9,724,100,000
2007	493,300	2,855	$10,542,900,000
2008	475,300	2,750	$11,620,400,000
2009	445,400	2,570	$10,183,500,000
2010	447,000	2,645	$9,047,600,000

1.3.4 Redundancy

Redundancy is an effective method to prevent service interruption and provide business continuity which is common using in industries [30]. When nodes damage or temporary shutdown, then they can activate redundancy in real time which can prevent service interrupted. Natural disasters often cause large-scale destruction and the degree of impairment is heavy and need more time to recover. In the meantime, defender can activate redundancy which can keep providing service during recovery. It can help companies to maintain business continuity.

Redundancy is a design principle of having one or more backup systems in case of failure of the main system [30]. Although the use of redundant components can improve the system reliability but it will also increases the system cost. Therefore, it is important to determine the optimal number of redundant components for each subsystem [31]. Hence, companies need to evaluate their budget and system's importance to determine the numbers of redundancy node and the level of redundancy, especially when budget has constraint. In chapter 2, we will introduce different kinds of redundancy which defender can choose based on their budget and need.

1.4 Thesis Organization

The remainder of this thesis is organized as followed. In Chapter 2, we will introduce in detail the problem which we want to solve, give an attack-defense scenario to make it clearer and our mathematical formulation. In Chapter 3, we will introduce our solution approach and Chapter 4 we will shows the environment and the final result of simulations. Finally, we will introduce conclusion and future work in Chapter 5.

Chapter 2 Problem Formulation

2.1 Problem Description

In this paper, we want to solve resource allocation problem. Attacker and defender only have limited budget. They need to use their resource effectively to attain their goal. Both of them need to evaluation their capability, resource and use appropriate strategy dealing with all kinds of situation. Besides, defender not only needs to worried about malicious attack also natural disasters' impact which may cause huge damage sometimes even more serious than malicious attack. Especially in nowadays, natural disaster frequently happened so defender must need to distribute some budget to prevent natural disaster and think about how to deal with it. Next, we will introduce attack strategy, defense method and natural disaster that we consider in detail.

2.1.1 Natural disaster

The following we list two natural disasters that we consider and each disasters has different characteristic.

- Earthquake:

Each earthquake has different energy, intensity level, degree of damage and impact range. Gutenberg–Richter law [16] expresses the relationship between the magnitudes and total number of earthquakes in any given region and time period of at least that magnitude [32]. Hence, we adopt the Gutenberg–Richter law to determine earthquake's intensity level by using the following formulations which can compute each intensity level's probability of occurrence.

$$\boldsymbol{log_{10}\lambda m = a - bM}$$

Where:

λm is the number of events having a magnitude ≥ M.

a and *b* are constants value and different location has different value.

Following the basic formulation, they extend a new equation by considering both lower threshold magnitude and the maximum magnitude, the mean annual rate of exceedance of an earthquake of magnitude [33].

$$\lambda\mathrm{m} = \mathrm{v}\frac{e^{-\beta(m-m_0)} - e^{-\beta(m_{max}-m_0)}}{1 - e^{-\beta(m_{max}-m_0)}}$$

Where:

$\mathrm{v} = e^{(\alpha-\beta m_0)}, m_0 \le m \le m_{max}$

$\alpha = 2.303\mathrm{a}, \beta = 2.303\mathrm{b}$

The result is a rate that each magnitude occurrence's probability. Therefore, we use this formulation to determine each earthquake will be what magnitude.

After determine earthquake intensity, we still need to decide its impact range and damage ratio. We use following formulation provide by Central Weather Bureau, Taiwan[45] to compute the peak ground celebration *Y.*

$$\mathrm{Y} = 0.0253e^{1.5873M}(R + 0.3155e^{0.6165M})^{-2.3027}$$

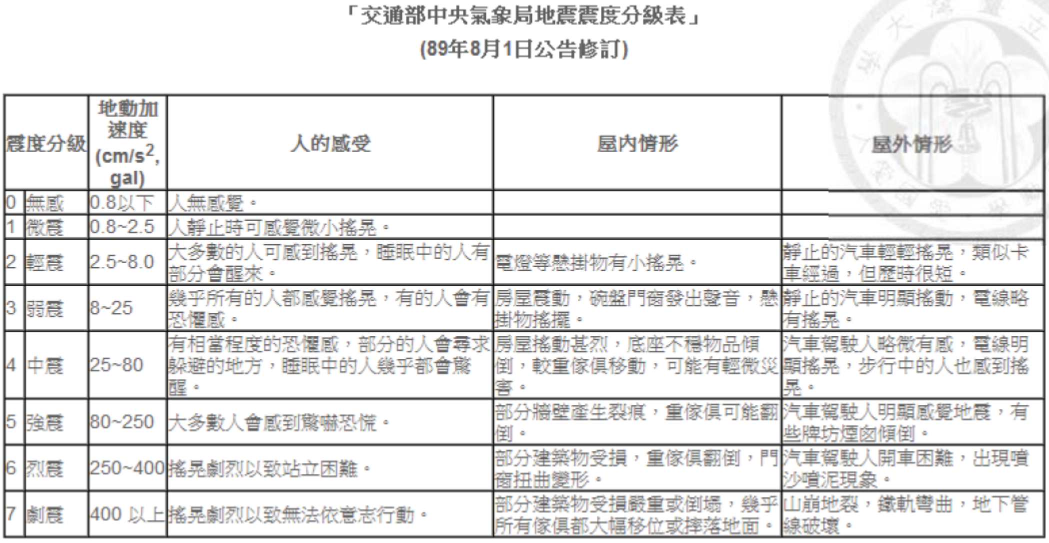
Where:

Y: *Y* is peak ground acceleration

M: *M* is earthquake magnitude

R: *R* is the distance between node and epicenter

We can use magnitude that previous computing into this formulation and we can get the peak ground acceleration *Y.* We adopt data providing by Central Weather Bureau, Taiwan as Figure 2-1 transferring peak ground acceleration into damage ratio. As you can see, different peak ground acceleration will cause different building destruction and people's feel; we will refer this data and generate damage ratio. Therefore, each node will compute its own peak ground acceleration based on different distance between epicenter and will has different damage ratio and based on this ratio will determine whether this node will be destroy or not.



「交通部中央氣象局地震震度分級表」
(89年8月1日公告修訂)

震度分級		地動加速度 (cm/s^2, gal)	人的感受	屋內情形	屋外情形
0	無感	0.8以下	人無感覺。		
1	微震	0.8~2.5	人靜止時可感覺微小搖晃。		
2	輕震	2.5~8.0	大多數的人可感到搖晃，睡眠中的人有部分會醒來。	電燈等懸掛物有小搖晃。	靜止的汽車輕輕搖晃，類似卡車經過，但歷時很短。
3	弱震	8~25	幾乎所有的人都感覺搖晃，有的人會有恐懼感。	房屋震動，碗盤門窗發出聲音，懸掛物搖擺。	靜止的汽車明顯搖動，電線略有搖晃。
4	中震	25~80	有相當程度的恐懼感，部分的人會尋求躲避的地方，睡眠中的人幾乎都會驚醒。	房屋搖動甚烈，底座不穩物品傾倒，較重傢俱移動，可能有輕微災害。	汽車駕駛人略微有感，電線明顯搖晃，步行中的人也感到搖晃。
5	強震	80~250	大多數人會感到驚嚇恐慌。	部分牆壁產生裂痕，重傢俱可能翻倒。	汽車駕駛人明顯感覺地震，有些牌坊煙囪傾倒。
6	烈震	250~400	搖晃劇烈以致站立困難。	部分建築物受損，重傢俱翻倒，門窗扭曲變形。	汽車駕駛人開車困難，出現噴沙噴泥現象。
7	劇震	400 以上	搖晃劇烈以致無法依意志行動。	部分建築物受損嚴重或倒塌，幾乎所有傢俱都大幅移位或摔落地面。	山崩地裂，鐵軌彎曲，地下管線破壞。

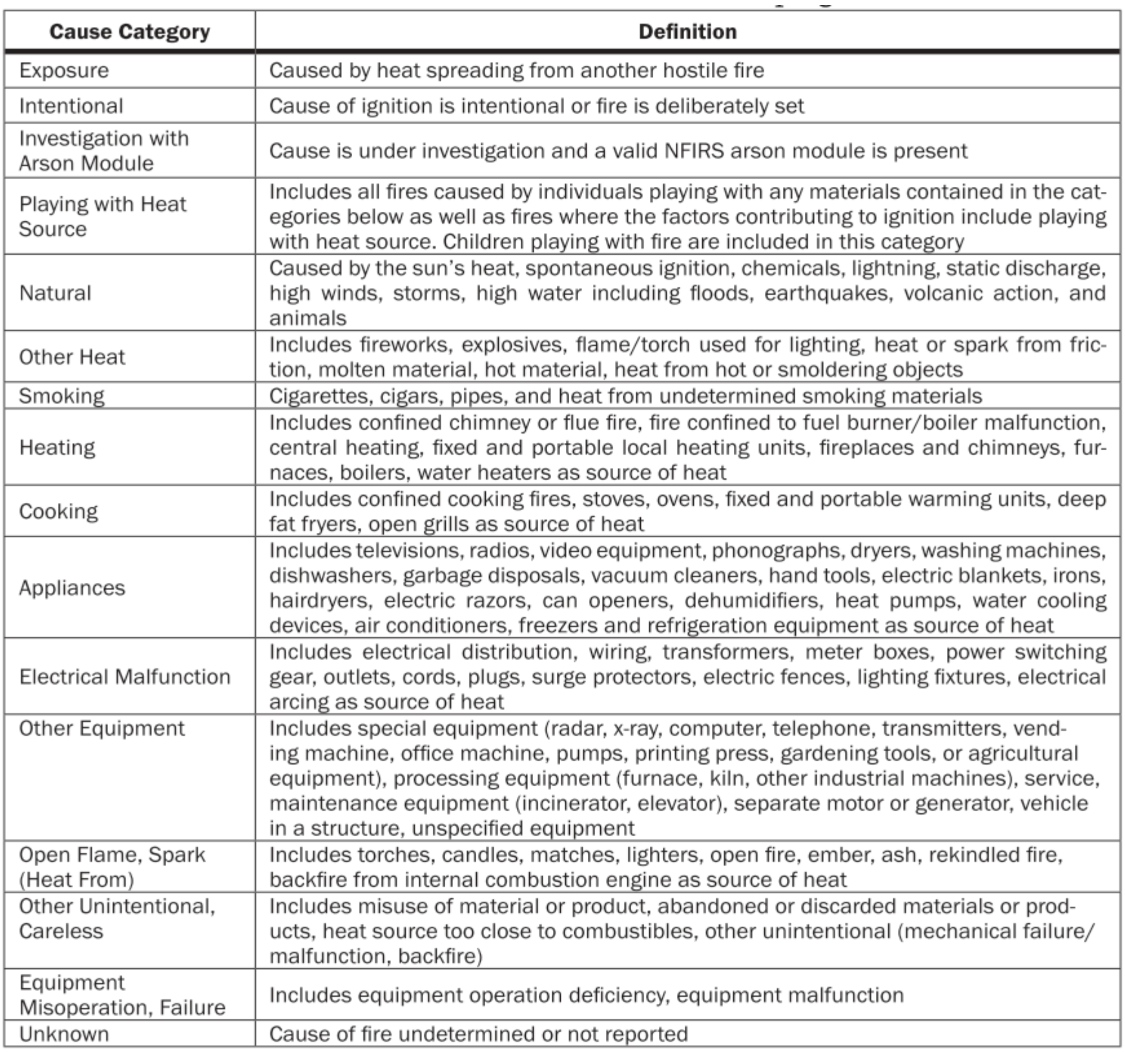
Figure 2-1: peak ground acceleration and damage comparison table [45]

Fire

U.S Fire Administration classify the cause of fires: exposure, intentional , investigation with arson module, playing with heat source, natural, other heat, smoking, heating, cooking, appliance, electrical malfunction, other equipment, open flame, other unintentional careless, equipment misoperation and unknown as Table 2-1.

The frequency sequence of the cause of fire is: cooking, heating and electrical malfunction [29]. Even though natural disaster is unpredictable, but still has some rules to follow. Like heating may cause by machine doesn’t has cold function or the machine’s loading is overwhelming plus in company engine room there are full of machines which is more likely to heating and cause fire. Engine room also often cause fire because there are many circuit lines twining together which may makes lines becoming fragile and leads fire happened. Providing significant service's server may has heavy loading to deal with, so the probability of getting fire is relatively higher. Therefore, we decide to classify fire as three types: heating, electrical malfunction and others.

Table 2-1: Fire source category [29]



Cause Category	Definition
Exposure	Caused by heat spreading from another hostile fire
Intentional	Cause of ignition is intentional or fire is deliberately set
Investigation with Arson Module	Cause is under investigation and a valid NFIRS arson module is present
Playing with Heat Source	Includes all fires caused by individuals playing with any materials contained in the categories below as well as fires where the factors contributing to ignition include playing with heat source. Children playing with fire are included in this category
Natural	Caused by the sun's heat, spontaneous ignition, chemicals, lightning, static discharge, high winds, storms, high water including floods, earthquakes, volcanic action, and animals
Other Heat	Includes fireworks, explosives, flame/torch used for lighting, heat or spark from friction, molten material, hot material, heat from hot or smoldering objects
Smoking	Cigarettes, cigars, pipes, and heat from undetermined smoking materials
Heating	Includes confined chimney or flue fire, fire confined to fuel burner/boiler malfunction, central heating, fixed and portable local heating units, fireplaces and chimneys, furnaces, boilers, water heaters as source of heat
Cooking	Includes confined cooking fires, stoves, ovens, fixed and portable warming units, deep fat fryers, open grills as source of heat
Appliances	Includes televisions, radios, video equipment, phonographs, dryers, washing machines, dishwashers, garbage disposals, vacuum cleaners, hand tools, electric blankets, irons, hairdryers, electric razors, can openers, dehumidifiers, heat pumps, water cooling devices, air conditioners, freezers and refrigeration equipment as source of heat
Electrical Malfunction	Includes electrical distribution, wiring, transformers, meter boxes, power switching gear, outlets, cords, plugs, surge protectors, electric fences, lighting fixtures, electrical arcing as source of heat
Other Equipment	Includes special equipment (radar, x-ray, computer, telephone, transmitters, vending machine, office machine, pumps, printing press, gardening tools, or agricultural equipment), processing equipment (furnace, kiln, other industrial machines), service, maintenance equipment (incinerator, elevator), separate motor or generator, vehicle in a structure, unspecified equipment
Open Flame, Spark (Heat From)	Includes torches, candles, matches, lighters, open fire, ember, ash, rekindled fire, backfire from internal combustion engine as source of heat
Other Unintentional, Careless	Includes misuse of material or product, abandoned or discarded materials or products, heat source too close to combustibles, other unintentional (mechanical failure/malfunction, backfire)
Equipment Misoperation, Failure	Includes equipment operation deficiency, equipment malfunction
Unknown	Cause of fire undetermined or not reported

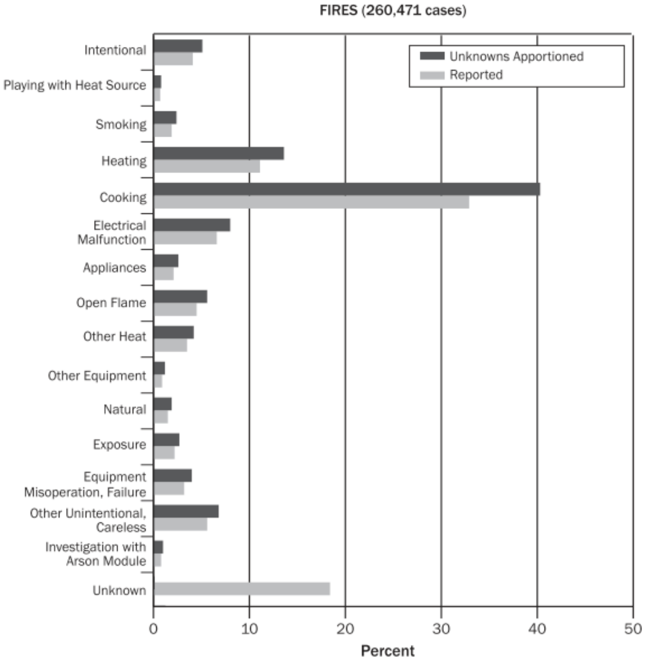
Source: USFA.

Different types of fire also have different probability of occurrence. We adopt real data to determine their probability. We use data released by U.S Fire Administration as

Table 2-2 which provides each types of fire's probability of occurrence [34]. For example, type heating, its probability of occurrence is $(0.111 + 0.184 * 0.136) = 0.136$. So, there is 13.6 percentages that this time will happened fire by heating.

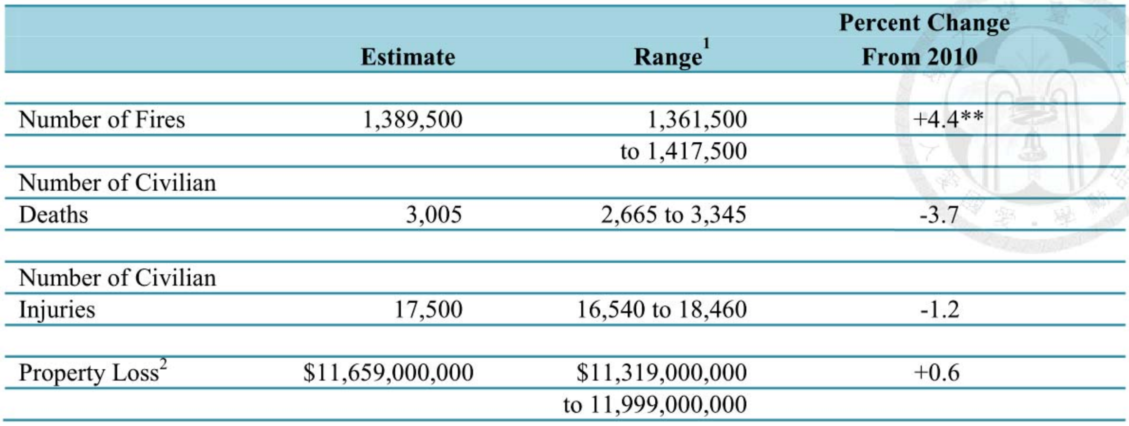
The fire influence range we reference real data released by National Fire Protection Association as we can see in Table 2-3 [35]. We use five years' data to compute the average fire influence range and using other attribute to create fire influence range distribution curve following by normal distribution. By this distribution to determine every fire influence range.

Table 2-2: Each category's probability of occurrence [34]



Cause	Reported	Unknowns Apportioned
Intentional	4.1	5.1
Playing with Heat Source	0.7	0.8
Smoking	1.9	2.4
Heating	11.1	13.6
Cooking	32.9	40.3
Electrical Malfunction	6.6	8.0
Appliances	2.1	2.6
Open Flame	4.5	5.6
Other Heat	3.5	4.2
Other Equipment	0.9	1.2
Natural	1.5	1.9
Exposure	2.2	2.7
Equipment Misoperation, Failure	3.2	4.0
Other Unintentional, Careless	5.6	6.8
Investigation with Arson Module	0.8	1.0
Unknown	18.4	0.0

Table 2-3: Estimates of 2011 Fires, Civilian Deaths, Civilian Injuries and Property Loss in the United States [35]



	Estimate	Range[1]	Percent Change From 2010
Number of Fires	1,389,500	1,361,500 to 1,417,500	+4.4**
Number of Civilian Deaths	3,005	2,665 to 3,345	-3.7
Number of Civilian Injuries	17,500	16,540 to 18,460	-1.2
Property Loss[2]	$11,659,000,000	$11,319,000,000 to 11,999,000,000	+0.6

2.1.2 Commander Perspective

In this paper, we consider noncollaborative attack (one attacker attack one target) and collaborative attack (two or more attackers attack one target). Because large-scale systems often have strong protection and facing that situation, commander can choose using collaborative attack which can use less resource and reach more harmful damage. Therefore, if commander want to attack critical point, they can adopt collaborative attack and remaining time can user noncollaborative attack. Using which attack type is made by commander. Commander can direct attackers belong to commander and make all kinds of attacker event. As we mentioned before, commander can choose to attack many target one time and using different attack type (noncollaborative or collaborative). Next, we will introduce commander and attacker’s attributes in order to understand attack operation.

- Goal:

We need to know the goal and then we can follow the goal to plan how to attack.

There are two goals which commander wants to attain.

(1) Service Disruption:

This goal is let defender cannot satisfy legitimate user’ QoS. Attacker can attack core nodes which provide services and let core node cannot provide service to users. Or they can attack the whole network such as interrupting connection path or blocking traffic which can also let defender cannot provide good enough service in such way they can achieve the goal.

(2) Steal Confidential Information:

Some nodes in network contain confidential information like each core nodes’ location, allocating how much defense resource, etc. If attacker obtains those confidential information, it may give attacker advantage to compromised the network and defender become more dangerous to deal with it.

- Attack group

Each attack group is composed of some attackers and lead by a commander. Each attacker group has different number of attackers which follows normal distribution. Commander can direct attacks to do noncollaborative attack or commander can separate attackers to some sets and launch each set to do collaborative attack. The member number of set will decide the attack power. There will be more powerful if there has more attackers in the set. It is because synergy as we mentioned at chapter 1.

If there is multiple attackers attack, there will have synergy effect. In our thesis, we adopt Cobb-Douglas function to evaluate synergy effect. Cobb-Douglas function is developed and verifies by Charles Cobb and Paul Douglas and is used to show the relationship with output and two inputs. The function is showed as below [36]:

$$\mathrm{Y} = \mathrm{A}L^{\alpha}K^{\beta}$$

Where:

Y = total production (the monetary value of all goods produced in a year)

L = labor input (total number of person-hours in a year)

K = capital input (the monetary worth of all machines, equipment, buildings, etc)

A = total factor productivity

α and β are the output effects of labor and capital.

- If $\alpha + \beta = 1$, then the production function is directly proportional to scale; in other word, if investing double capital K and labor L will return double output Y.
- If $\alpha + \beta < 1$, it represents investing equal capital and labor won't return sum output; the condition of decreasing returns to scale of production
- If $\alpha + \beta > 1$, it represents investing more capital and labor will return more output.

We apply Cobb-Douglas function and combined to evaluate the synergy value as follow:

$$\text{Attack Effect} = \mathrm{A} \times \prod_{i=1}^{N} x_i^{a_i}$$

where

$\sum_{i=1}^{N} a_i = m$

N: *N* is the number of attackers

a_i: a_i is the synergy effect of attack i.

x_i: x_i is the budget which attacker i spend

A: *A* is a constant variable

m: *m* is contest intensity

We also consider negative synergy. The entire attack set's detection probability by defender is decide by the worst member of the set. In other word, it's a worst case; the other members will be dragged by the weakest member. This is the negative synergy caused by collaborative attack.

- Budget

Commander's budget adopts normal distribution to distribute. Commander needs to user limited resource to achieve their goal.

The whole attack process can divide into preparing phase and attacking phase. In the preparing phase, the most important thing is getting attack tools and they needs to spend part of budget on it. There are three methods to get attack tool: by buying off-the-shelf tools, reorganizing the tools based on the existing tool and building brand new one by themselves. In the attacking phase, they use remaining budget to compromise nodes. Commander needs to use resource effectively. The probability of success is higher if commander invests more resource to attack. But when attack's time up or budget used up, in that time if commander doesn't achieve the goal then that means they are failed. So how to allocation resource effectively and pick up next victim node are very important decision variables.

- Aggressiveness:

Commander will evaluate each nodes and to choose the next victim nodes. They will use traffic throughput, resource invested by defender and attacker and failure time that attacker used to attack to evaluate each node's degree of importance. In other words, it is means how much commander wants to compromise that node. Aggressiveness values will decide the compromised success rate and if commander thinks that node is important then aggressiveness usually will much higher. That means if commander wants to compromises the critical node, wants to have higher success rate then they needs to invest more resource to attack the node.

- Attacker:

Every attacker has their own attributes like different capability or energy and it will influence the attack process.

(1) Capability:

Every attacker has different capability which will influence attacker using attacking tools. That is means even though using the same attacking tool; different attackers have different capabilities which will makes executing result differently. Attacker who has better capability will be able to maximize the effectiveness of the attacking tool and cause maximum destruction. Each attacker’s capability use normal distribution to distribute their capability.

(2) Energy:

Every attacker has their own energy which we can see as physical power. Every attack event will consume some energy and if attacker keeps attacking then energy will keep diminishing. Energy level high or low will affect attacking result. If attacker has more energy, then compromised probability will much higher compare to lower one. So, commander cannot let attacker keeps attacking which may make their energy level become too low and on the contrary will let attacking ineffective. Attackers need to take a break to make energy recovery and to do so will make compromised probability rises.

- Time:

Attacker has limited time to attack. The time constraint contains two parts. First, there is a total attacking time’s constraint. From the beginning to the end of attack, the total attacking time cannot exceed the total time limit (given). If exceeds this time constraint, even though attacker compromises the system, it still counts fails in this time. Second, attacking each node also has time constraint. If exceeds this time, all attack event should stop and regarded as fail. Commander needs to restart attacking that node or reselect other victim node.

2.1.3 Defender Perspective

Defender needs to use limited resource to defend malicious attack brings damage and in the meantime they also needs to adopt some measures to prevent damage caused by natural disaster. Defender's goal is using limited budget against attacker and still can maintain their service level which cannot lower than user's QoS request. Defender can only adopt passive defense and cannot active adopt attack event.

When the end of the attacking time and still cannot compromise the system or commander runs out of budget, then defender achieves their goals, defense successfully. In the following, we will introduce some defense strategies that defender can adopt in detail. It can divide into two parts: proactive defense and reactive defense.

2.1.3.1 Proactive defense

Before attacker started attack, defender can adopt some mechanism such as deploying firewall, Intrusion Detection System (IDS), Intrusion Protection System (IPS), anti-virus software, etc. Those mechanisms can enhance node’s defense intensity which may let attacker needs to spend more time and budget to compromise it or even let attacker cannot compromise the node. Or by using these mechanisms, defender may detect abnormal traffic, attack or source and try to eliminate in advance.

2.1.3.2 Reactive defense

When attacker starts attacking, defender can adopt other defense strategies called reactive defense. Reactive defense is when some event happened then defender will make some reaction to enhance their defense or make some recovery. There are three reactive defenses that defender can adopt.

- Redundancy:

Redundancy is an effective method to prevent service interruption and common using in industries. When nodes damage or temporary shutdown, then they can activate redundancy in real time which can prevent service interrupted. Natural disasters often cause large-scale destruction and the degree of impairment is more serious and need more time to recover. In the meantime, defender can start remote redundancy and provide service during recovery.

Redundancy can divide into several categories. According to the distance, it can be divided into local redundancy and geographical redundancy or geo-redundancy [37].

Companies can put critical system’s backup in a geographically separate location. The advantage is if natural disaster or man-made force majeure (disaster) events which result in site destruction, unavailability or inaccessibility, in that time geo-redundancy can take over to ensure business continuity and security [37]. In this case, if companies adopt local redundancy then it is high probability that local redundancy will also be destroyed because systems are in the same region. If facing malicious attack, local redundancy still can work because attacker still needs to invest budget to attack redundancy node.

According to the switch time, it can divide into hot standby redundancy and cold standby redundancy. Hot-standby units always power on and are ready for takeover in any time. When a fault is detected, then redundancy can take over immediately and automatically. Cold-standby redundancy will need some time to take over. Cold-standby redundancy remains unpowered in the usual and it will turn on until on-line unit fails [31] [38]. Defender can base on their limited budget to choose proper redundancy.

If the system need several servers can maintain their system, at this time defender will better also install many redundancies in order to handle legitimate users’ request. If today two servers destroyed by natural disaster, only one redundancy can activate, it may not satisfy every legitimate users and let QoS decrease. Defender can base on their budget and each service’s importance to decide which type they should adopt and how many redundancy they should install.

- Virtual machine monitor

Virtualization can create many independent virtual machines (VMs) and each of them can have their own operation system, memory, service, etc. Virtual Machines will share the same underlying physical hardware resource, but upper operation is independent to each other. Virtual Machine Monitor (VMM) is used to control the underlying virtual machines. VMM is between physical layer (hardware) and virtual machines. Each VM wants to access physical's resource need to go through VMM which means VMM is the only access entrance and VMM can control VMs by this. Hence, we can set Intrusion Prevention System (IPS) in VMM to detect abnormal behavior then the underlying VMs will all be protected. When an attack or intrusion being detected, VMM will activate local defense to enhance defense intensity. But using local defense has some drawback, VMM-IPS will enhance filtering threshold in order to strengthen protection and that may let legitimate user's flow also being block and cause QoS decrease brings negative effect. Also, VMM-IPS cannot filter the malicious event 100%; defender still has a chance being attack by attackers.

Because all of underlying VMs is control by VMM, every VM has any situation VMM will know. If VM is being compromised, VMM can attain this attacking information which may help in the following attacking event. However, if VMM is being compromised, then underlying VMs will fail in the same time.

- Honeypot

Honeypot's main function is to induce and confuse the attackers. There are two kinds of honeypot that defender can adopt.

(1) False target:

False target's main purpose is to confuse attacker and let attacker think false target is the genuine node, so when commander pick victim node and they might choose false target to attack. Thus, false target can consume commander's budget, time and decrease the probability that real node being attack. Furthermore, false target can add some error information to confuse attacker.

But attacker has a certain probability which can discover false target. Because false target cannot quite perfect and has no difference with core node and base on false target's level will have different being detected rate. Higher level false target can stimulate more service type and being detected rate is much lower. Defender needs to evaluate their budget and decide to deploy cheaper one or expensive one.

(2) Fake traffic:

When defender found the situation is critical that attacker almost find out core node's location, in that time defender can activate fake traffic honeypot to send fake traffic in order to mislead attacker. Fake traffic honeypot will send flow which contains imitative information and when attacker read that information, they might be misleading to “core node’s location” which is not real. Fake traffic honeypot’s purpose is to change attacker’s original direction to far away from core node. Fake traffic honeypot also has different level. High level fake traffic honeypot which is more expensive can stimulate higher throughput.

There is another kind of honeypot: dual function. Dual function honeypot has both fake traffic and false target’s function and it’s cheaper than deploy one fake traffic honeypot and one false target honeypot.

- Cloud Security Service:

In this thesis, we detect nodes by using traffic inspection and deploy the cloud security service agents on the node. During the attack，defender can redirect the traffic to the cloud security service via the agents when detecting the uncommon data traffic. The cloud security service is provided by cloud service provider and it can filter the malicious traffic and return the neat traffic. Moreover, the cloud security service has different security which provided different ability of filtering the traffic. Because of the budget and QoS consideration, defender can choose the different level cloud security service to deploy on the nodes. In sum, under the consideration of budget and QoS, defender should find the optimal strategy on deploy the cloud security service on the nodes.

- Risk level

We use risk level to as an index to decide whether activate some reactive defense or not. Risk level is like degree of danger, when risk level is too high then defender will need to do something to prevent core node being compromised. We use three factors which are the node which is detected suffering attack to core node's distance, core node's link degree and defense resource provisioning on the shortest path from attacked node (which is being detected) to core node. We use these three factors to evaluate risk level. The computing formulation is as follow:

$$Risk_{kl} = w_1 \times \frac{\min\{HopsToCoreNode_{kl}\}}{\max Hops\ ToCoreNode} + w_2 \times \frac{\min\{pathDefenseResource_{kl}\}}{\max pathDefenseeResource} + w_3 \times \frac{\max LinkDegree - linkDegree_{kl}}{\max LinkDegree}$$

- k is the node which is detected being attacked and is the nearest node to core node
- $\min\{HopsToCoreNode_{kl}\}$ means the number of hops from node k to core node l.
- $\max Hops\ ToCoreNode$ means the maximum number of hops from attack terminal node to core node.
- $\min\{pathDefenseResource_{kl}\}$ means total defense resource provisioning on shortest path from node k to core node.

- $\max pathDefenseResource$ means the maximal defense resource deploying to one path form attacker's position to core node.
- $\max LinkDegree - linkDegree_{kl}$ means maximal link degrees of all core nodes minus core node *l*'s link degree.
- $w_1, w_2\ and\ w_3$ are weights.

We will use $Risk_{kl}$ to see if core node *l* needs to activate some reactive defense or not. For example, as we mentioned before, when risk level is too high then we will activate fake traffic to lead commander attacking wrong direction.

2.2 Attack-defense Scenarios

In this section, we will use an example to introduce our attack-defense scenarios and its operation in detail.

2.2.1 Contest Success Function:

In our thesis, we adopt [40] proposed economic theory "contest Success Function (CSF "to evaluate the attack success or not. Contest success function provides every player has a chance to win the competition and the result of the competition will evaluate by all player's effort. If you pay more effort, resource, it will more likely to win the competition but not absolutely. It can use in different applications of contest note just in economy. In [41] [42] research, they use contest success function to model defender’s vulnerability (destruction probability). In our attack-defense scenario we also use CSF to measure the winning probability of defender and attacker. In [43] research, they use underlying formula to model contest success function between attacker and defender.

$$v = \frac{T^m}{T^m + t^m}$$

T and *t* are the effort that attacker and defender invest in the node and m is a parameter that describes the intensity of the contest. Different m’s value will influence the result dramatically. It can divide into several intervals to discuss [41].

1. When m=0, T and t won’t influence the result. The vulnerability of the element is 50%.
2. When 0 < m < 1, T and t have a little influence to the result. But investment and return is disproportionate. Return rate is lower than the investing rate.
3. When m=1, the investment and return have proportional impact on the result.
4. When m>1, investment and return is disproportionate, too. But this time, invest more resource will obtain greater result and it will show as exponential growth.
5. When $m = \infty$, who invest one more unit resource will win the competition.

In the entire attack-defense process we will use contest success function to compute the winning probability. Also, we will use different m value to see the result, every attributes’ variation.

2.2.2 Attack-defense Scenario

In the following, we will use a scenario to show the whole attack and defense process to make it more easily to understand. Table 2-4 is some assumptions that we set.

Table 2-4: Problem Assumption

Assumption:

1. There is more than one core node providing service in the network.
2. Each core node only provides one kind of service.
3. Only nodes equipped with VMM-IPS can activate local defense function.
4. The fake traffic honeypot must be equipped with fake traffic generating function.
5. Every attacker subordinates in only one attack group and each attack group launches one attack
6. All attack events are atomic operations.
7. Evaluate whether the attack is success or not is determined by the Contest Success Function (CSF).
8. If earthquake’s level above 5, then it will definitely trigger secondary disaster-fire.
9. Epicenter must happen in the seismic zone.
10. Each fire may have different intensity which will decide influence range.
11. The same kind of natural disaster can only happened once in the same time. But different types of natural disaster can happened in the same time.

12. Only disasters happened at the physical location of VMM has influences on all VMs.

Figure 2-2 is the icon to represent all kinds of component such as node, defense strategy, natural disaster, etc.

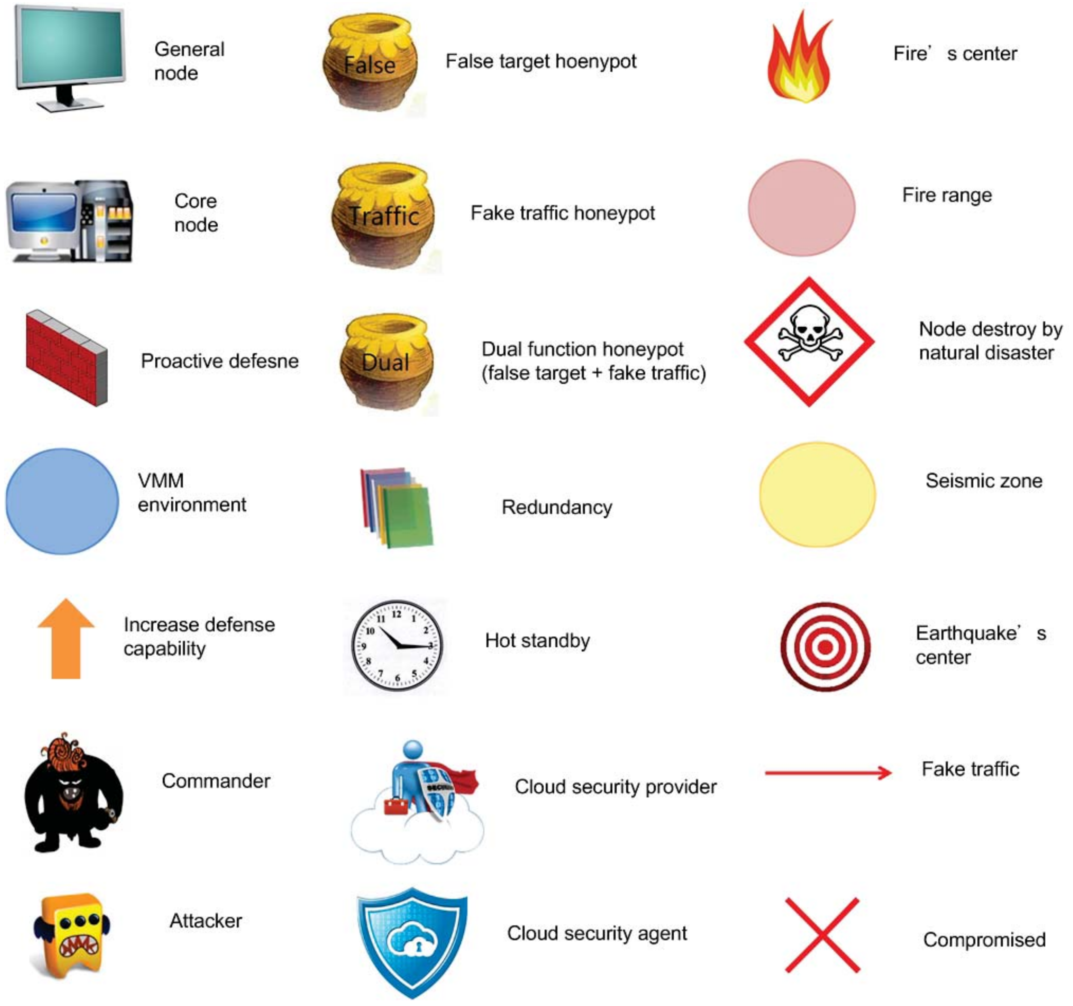


Figure 2-2: Explanation of Components

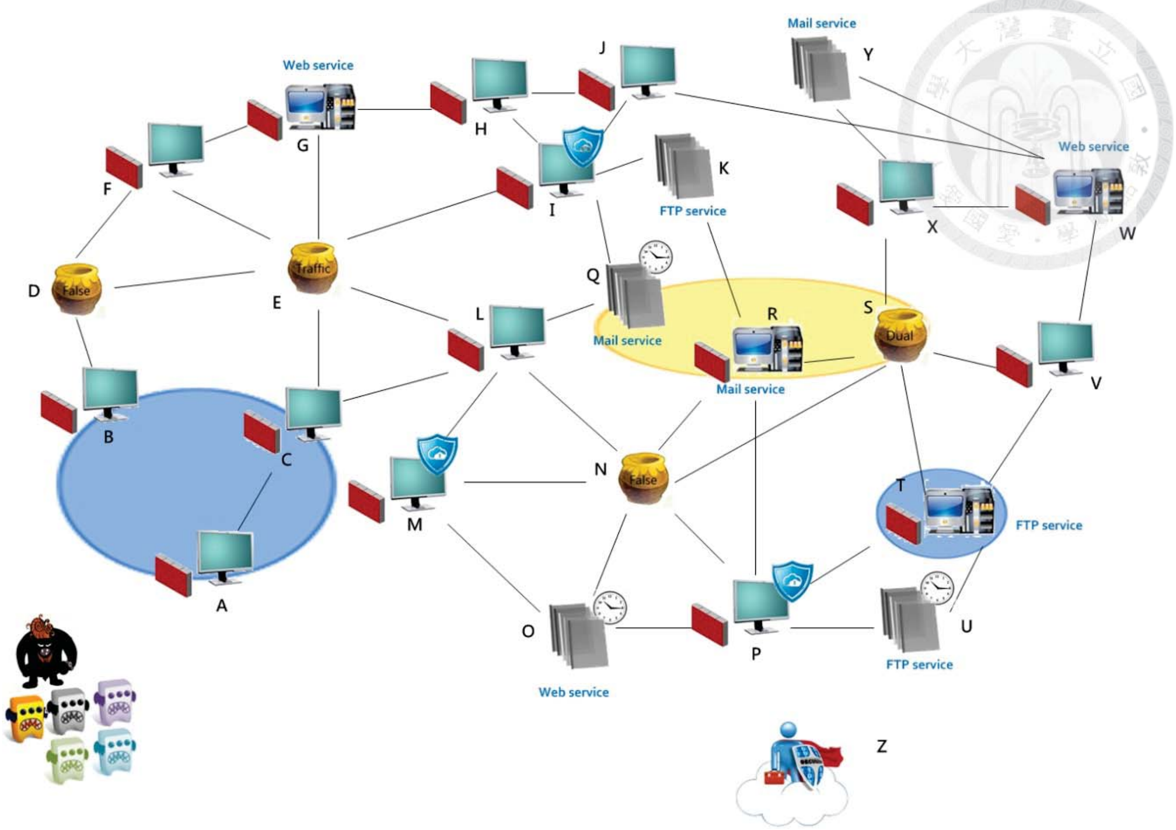


Figure 2-3: Initial Network Topology

Figure 2-3 is a network topology which defender construct. There are three kinds of services: web service, FTP service and mail service. G and W provide web service and have a full-copy redundancy with hot standby which is not been activated and just looks like normal node. T provides FTP service and has two different level of redundancy node K and U. R provides mail service and has toe different level of redundancy node Q and Y. There is a VMMs and has four VMs which is A, B, C and T. Z is cloud security provider and I, M and P deploy cloud agents which can use this service. D, E, N and S are honeypots which have different function. The yellow area contains Q, R and S is seismic zone which epicenter may happen in this area. Commander leads the attack group which is composed by five attackers and starting to attack.

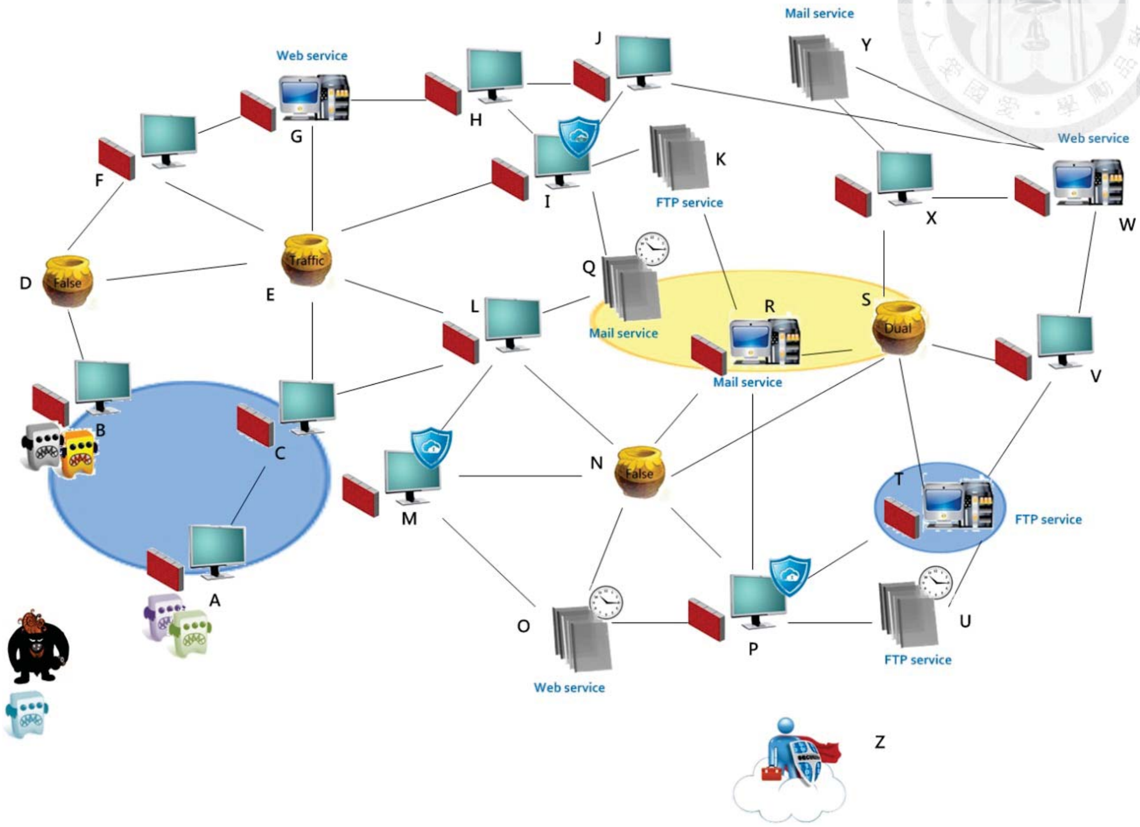


Figure 2-4: start to attack

Attacker side starts to attack. Since A and B are the terminal node which attacker can see and start attacking from, commander decides to send two attackers to attack node A and other two attackers to attack node B (Figure 2-4).

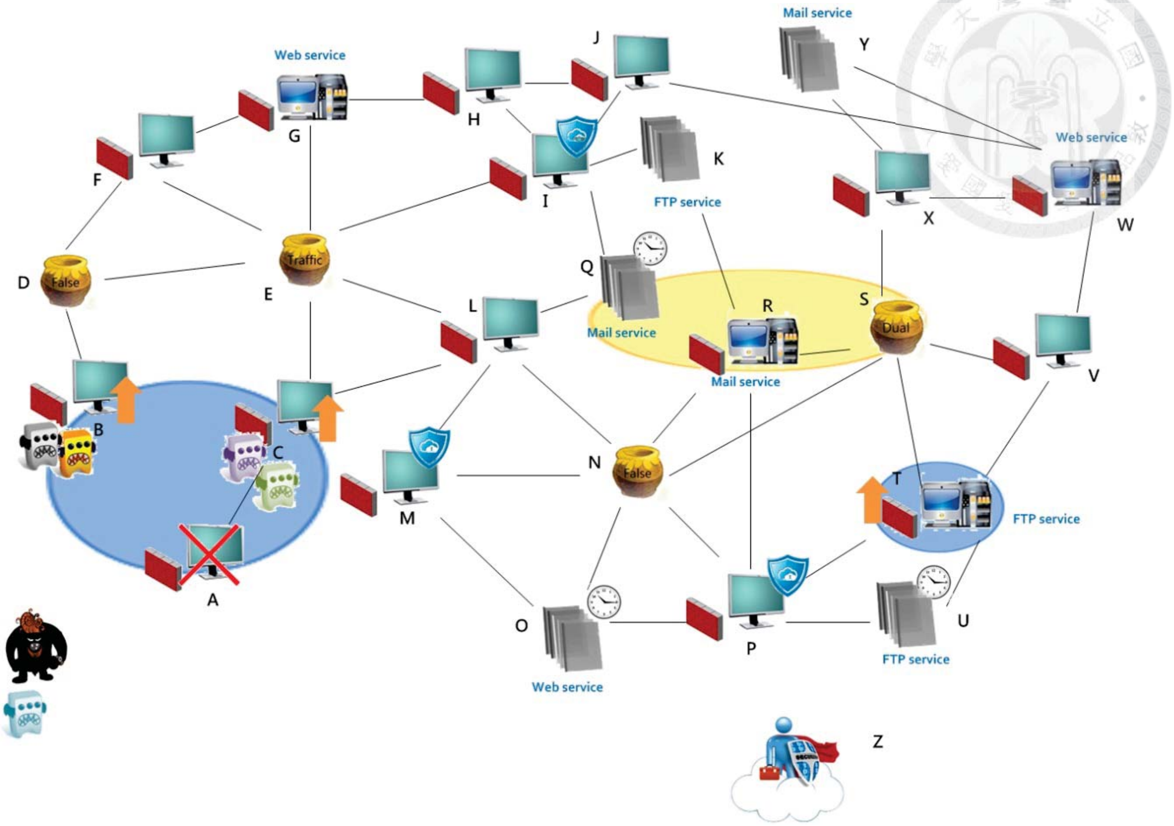


Figure 2-5: Local Defense

After attacking for a while, Figure 2-5 shows the result. Two attackers compromised A successfully and commander decide to keep attack node C. Because A, B, C and T are in the same virtualization environment, when A being compromised VMM can know that. Therefore, VMM-IPS turns on local defense to protect the system. Node B, C and T all increase their defense intensity. Attackers keep attacking node B and C.

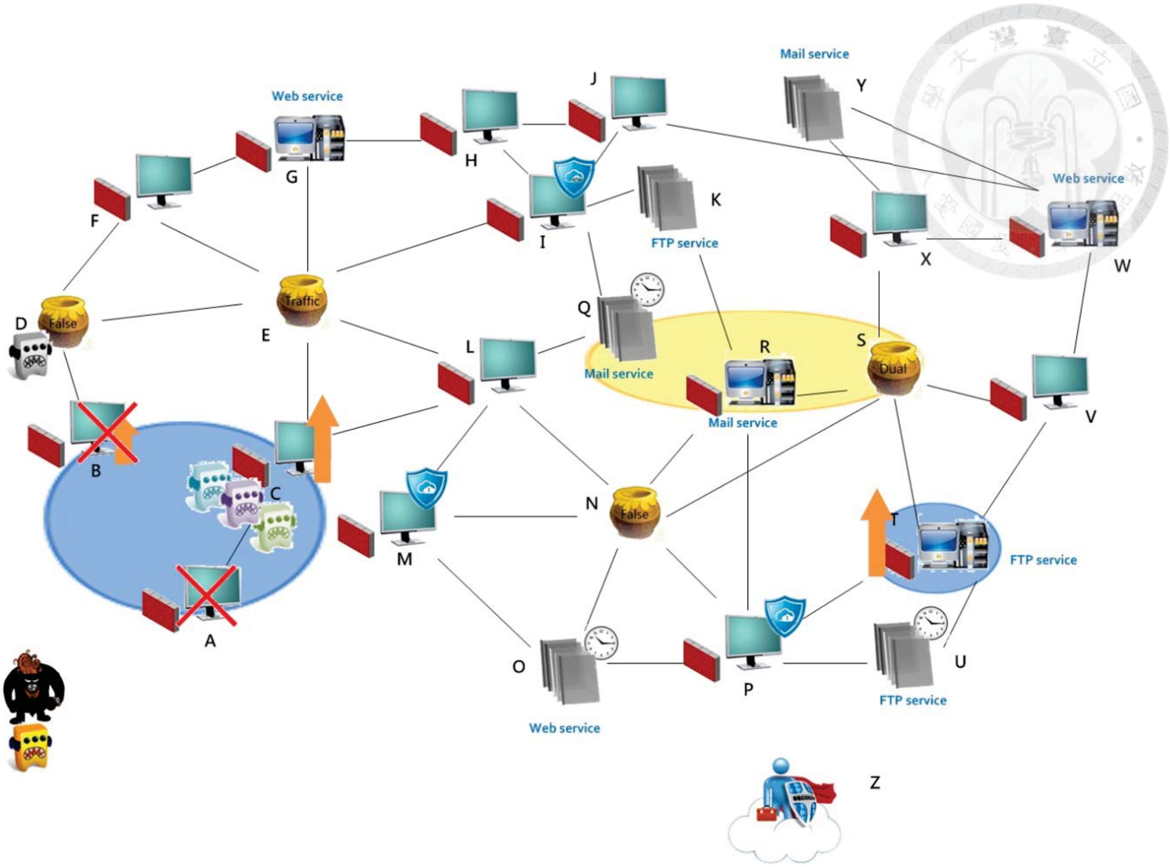


Figure 2-6: Recovery

In Figure 2-6, attacker compromised node B and decide to go forward attacking node D. Since C still cannot be compromised, commander sends one more attacker to help attacking node C. In the meantime, after compromised node B, an attacker went out of energy and need to recover for a while, so commander direct the attacker to take a break until energy's level come back. Because node B being compromised, node C and T increase their defense intensity again.

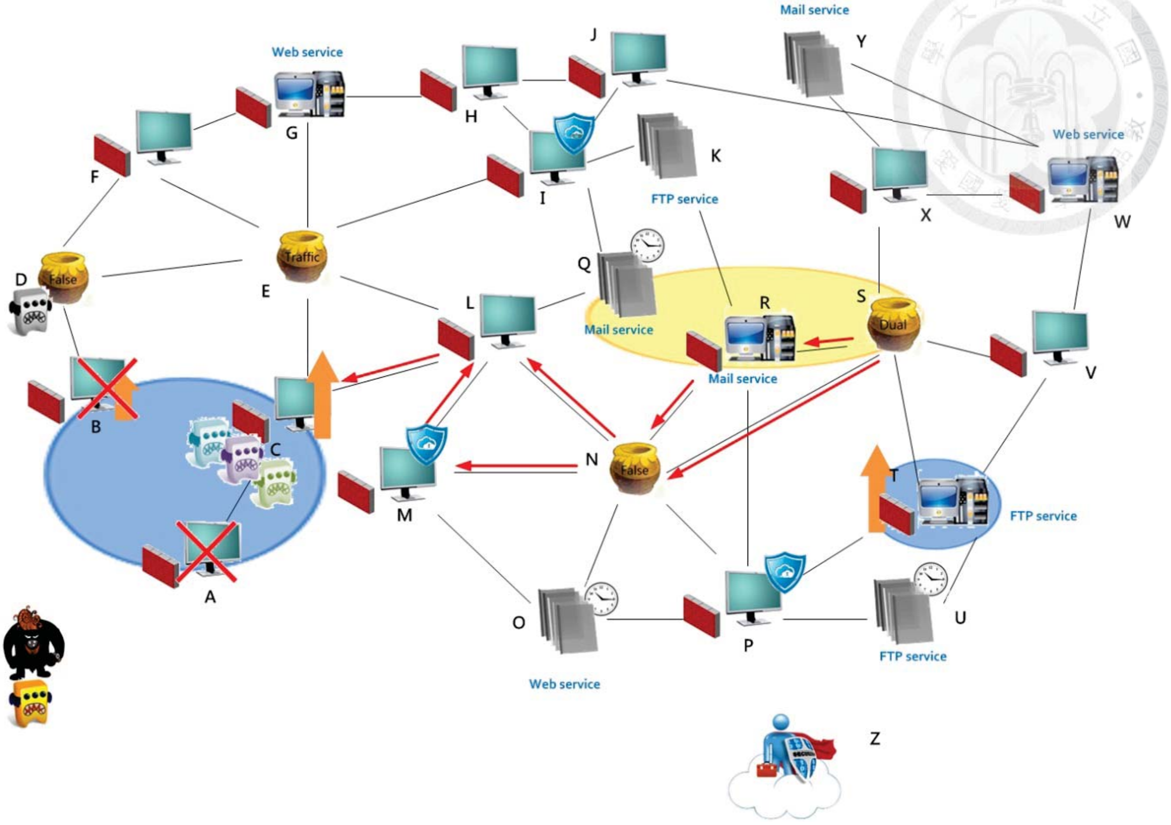


Figure 2-7: Fake traffic

When attackers keep attacking, core node G finds the situation is a little dangerous (risk level is reach a certain level), only two more hops attackers will reach it. Hence, core node G selects dual function honeypot S which can send fake traffic to guide attackers to the wrong direction in that way, core node G might not being attacked. Just like Figure 2-7, S sends fake traffic which contains some imitational information in order to make it like real traffic and induct attackers to change attacking direction toward S.

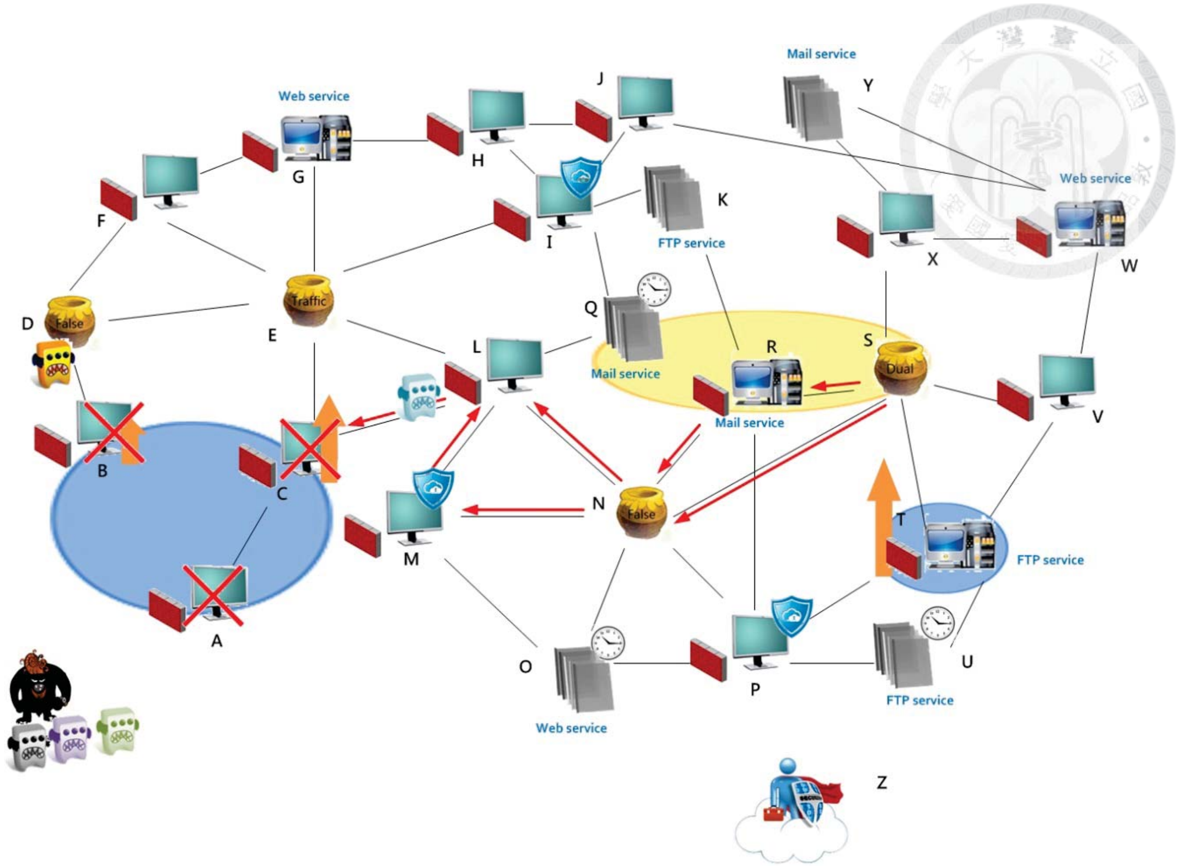


Figure 2-8: Fake traffic successfully attracts attackers

Three attackers attack node C finally compromised node C. Commander needs to decide next victim node. Commander sees many flows are from node L, so commander guesses there must has important service from that direction. Hence, commander orders attacker to attack node L like Figure 2-8. As we mention before, if attackers energy level is too low, commander will let attackers take a break for a while. Since node C being compromised, node T increases its defense intensity again. Attackers keep attacking node D and node L.

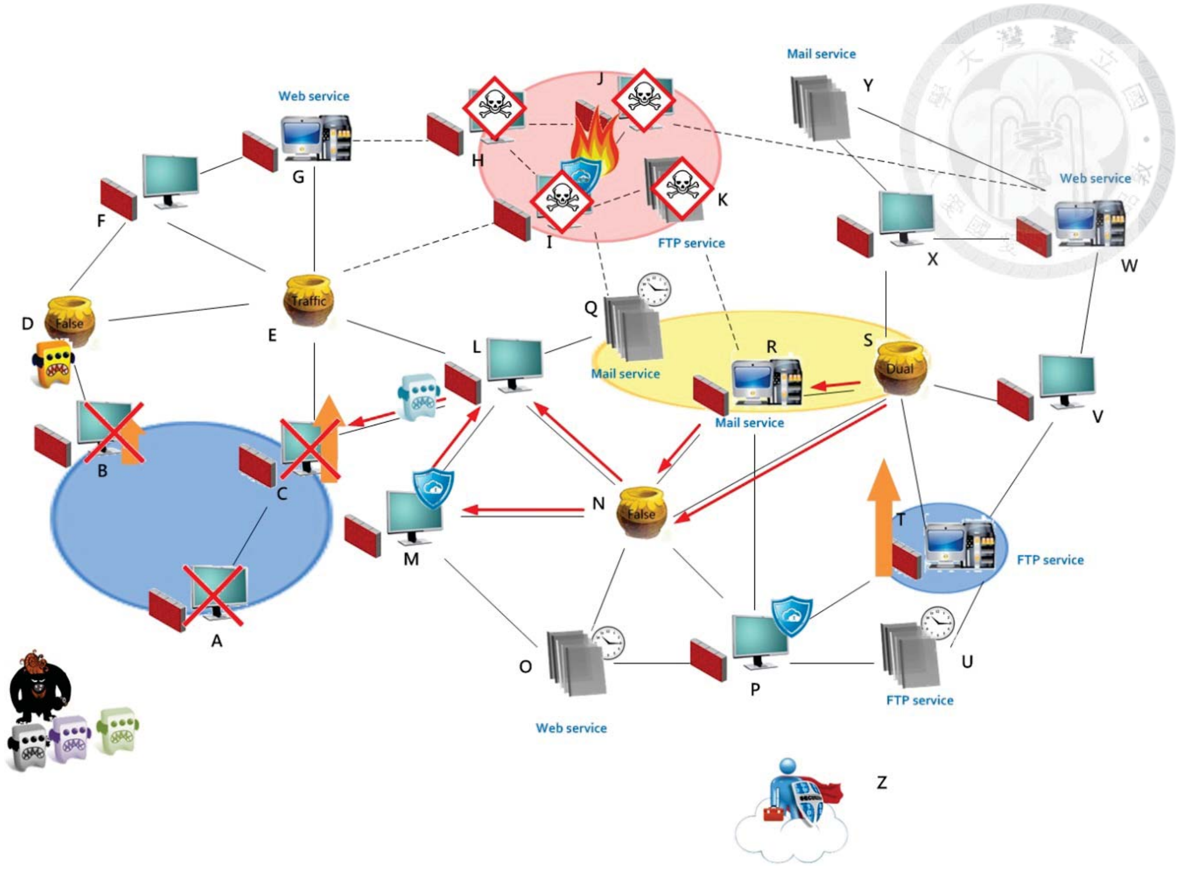


Figure 2-9: Fire

In the meantime, near node I's area happened fire (Figure 2-9). It spread to node H, I, J and K. All of nodes and link in fire range were destroyed. Both legitimate users and attackers cannot connect to those links and nodes.

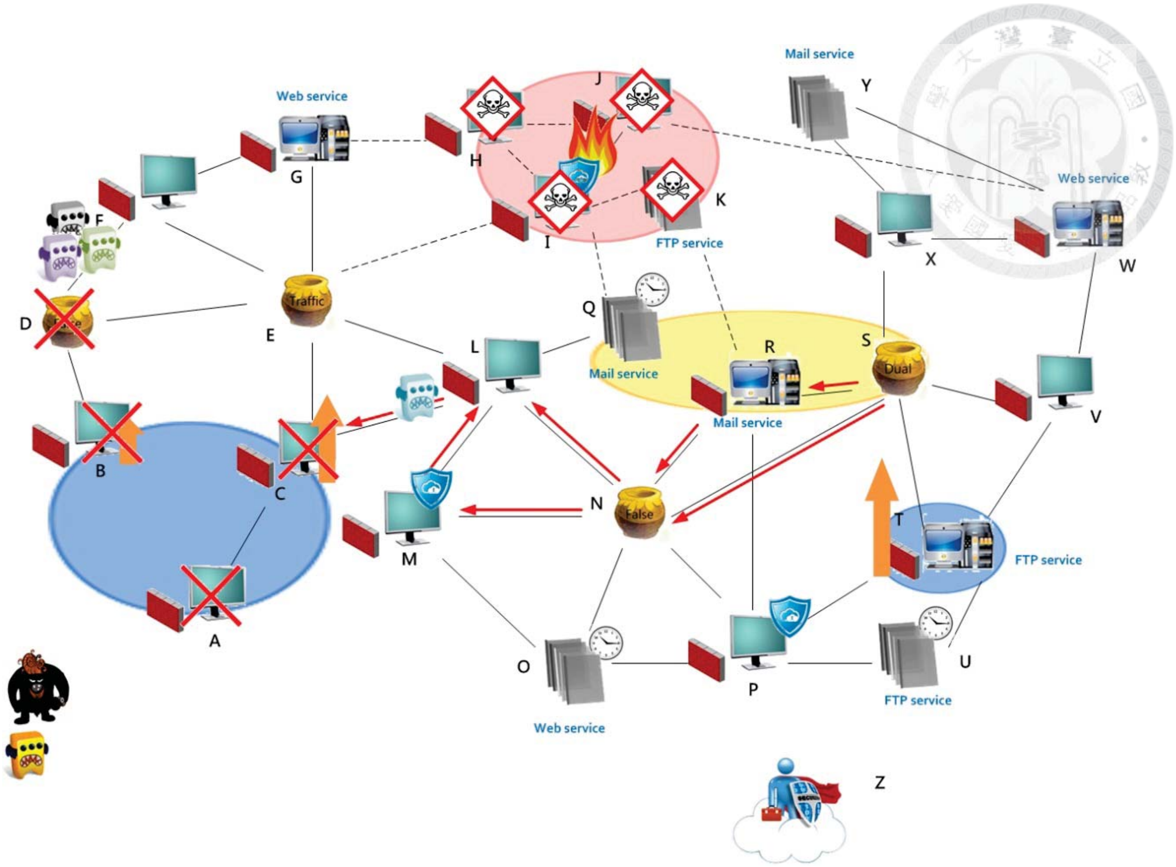


Figure 2-10: False target

After attacking for a while, attackers compromised false target D which contain some fake information and commander will read the content after compromised false target which will have a chance to believe false target node D is the core node they want and stop attacking (Figure 2-10). But since false target isn't perfect will have the probability being detected by commander, this time commander detected that node D is a false target and keep going forward attacking node F. After a while, attackers have been compromised node F and chooses node G as next victim node as you can see in Figure 2-11. After couple hours, attackers compromised node L and based on the flow's source decided to target node N as next victim node (Figure 2-12).

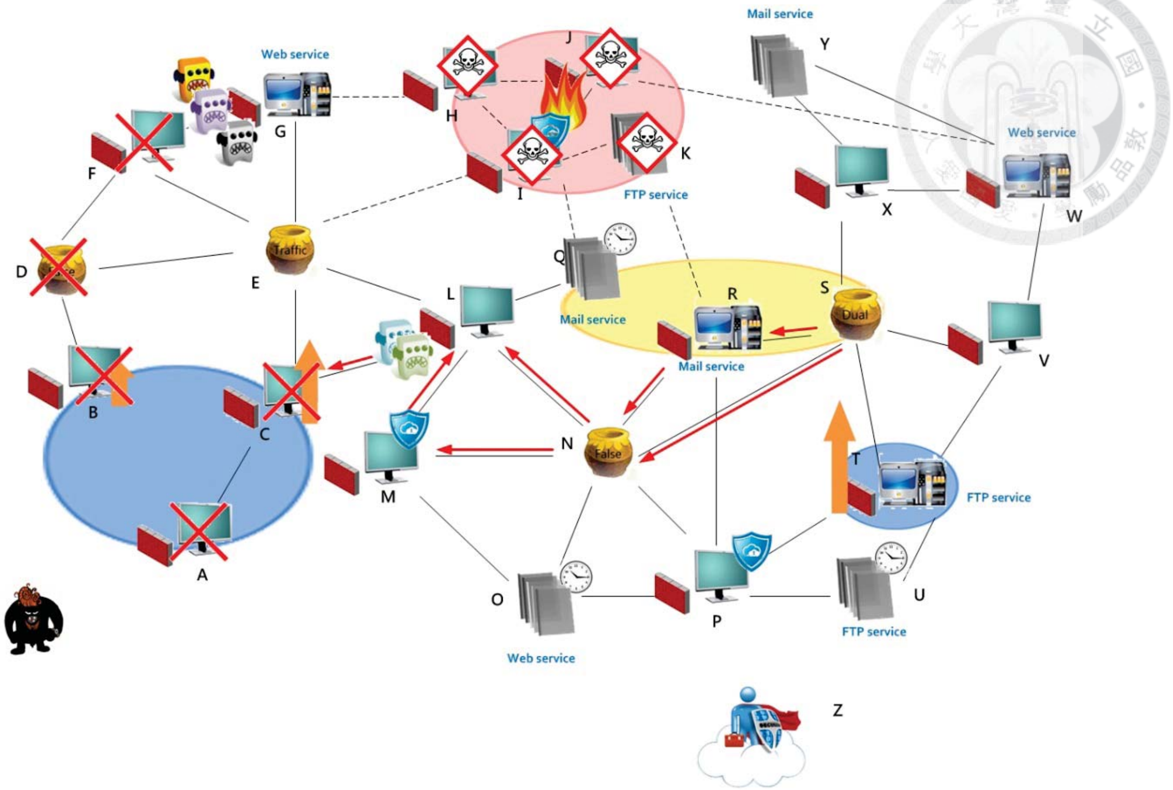


Figure 2-11: Node F being compromised

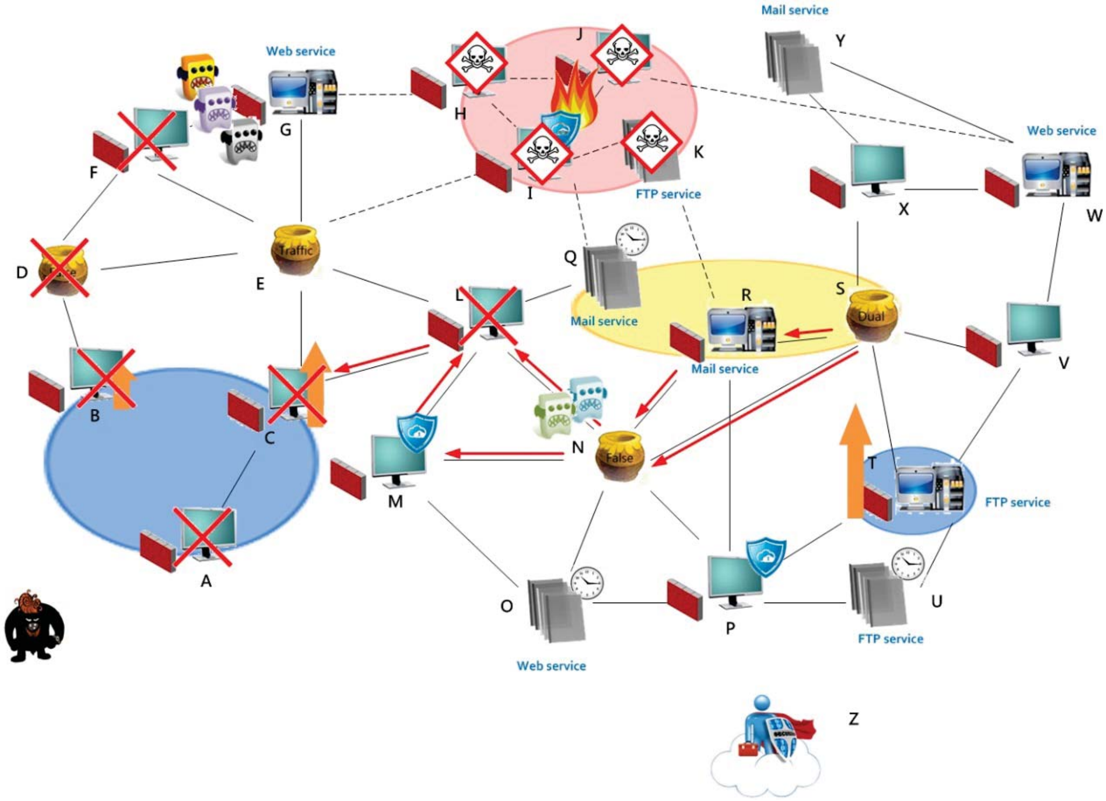


Figure 2-12: Node L being compromised

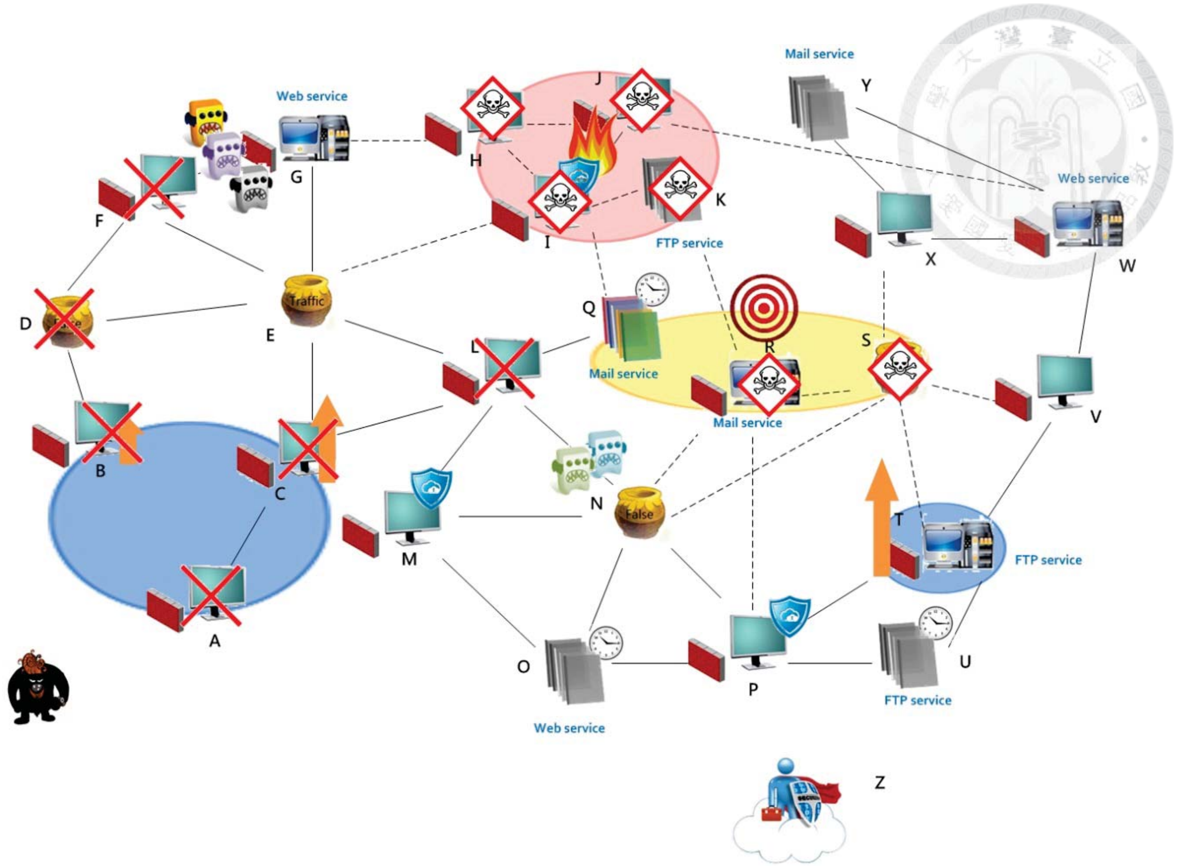


Figure 2-13: Earthquake

When attackers still attack the network, suddenly the earthquake happened and the epicenter is near node R just like Figure 2-13. Each earthquake has different intensity and we adopt Richter scale to evaluate the earthquake's strength. Different level has different energy, impact range and damage degree to the node. We will dependent on earthquake's intensity level, its energy and each node to epicenter's distance to decide node will be destroyed or not. In this case, node R and S were destroyed by earthquake and all of connecting link will be destroyed, too. Because node S being destroyed, the fake traffic honeypot stopped sending flows. Node Q is mail service redundancy with hot standby function which will automatically switch over when the core node failed in order to maintain service continuity.

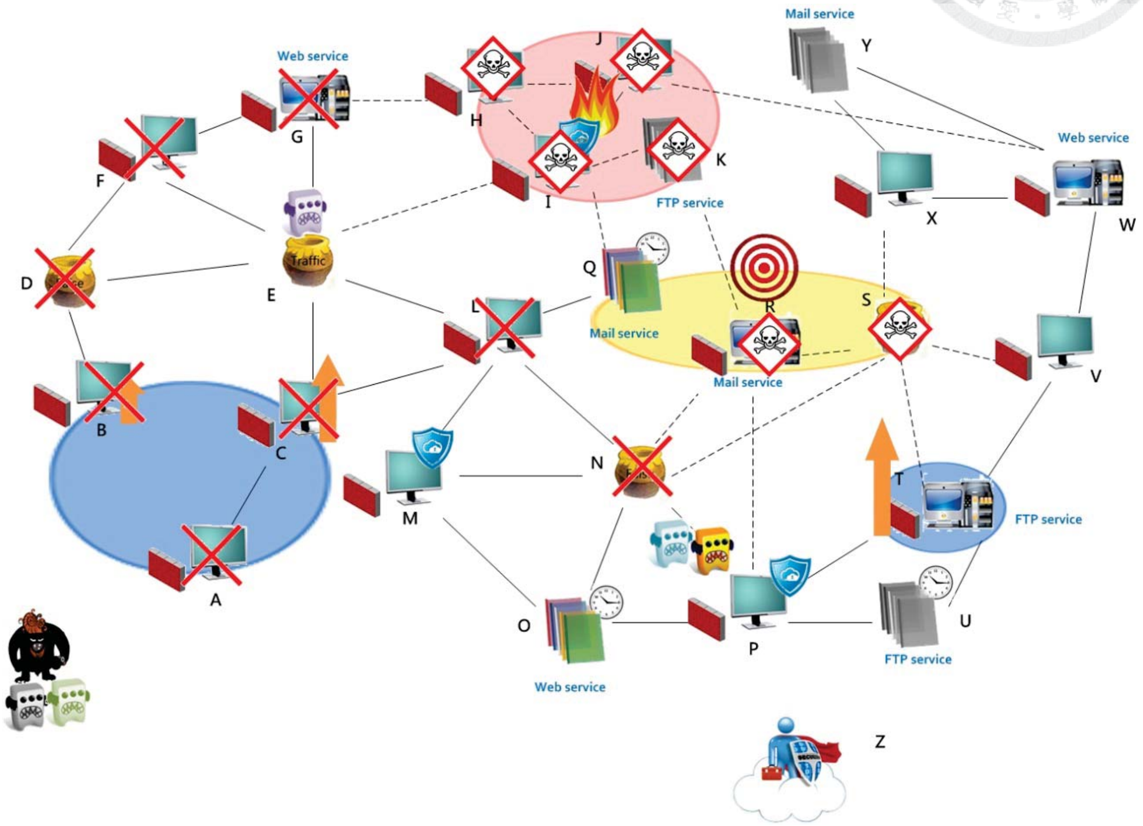


Figure 2-14: node N and core node G being compromised

Attackers successfully compromised node N (Figure 2-14) and because there is no fake traffic’s interference, commander decides to attack node P next time. In that time, attackers compromised core node G and node O detected core node failed, so node O immediately take over and keep providing web service.

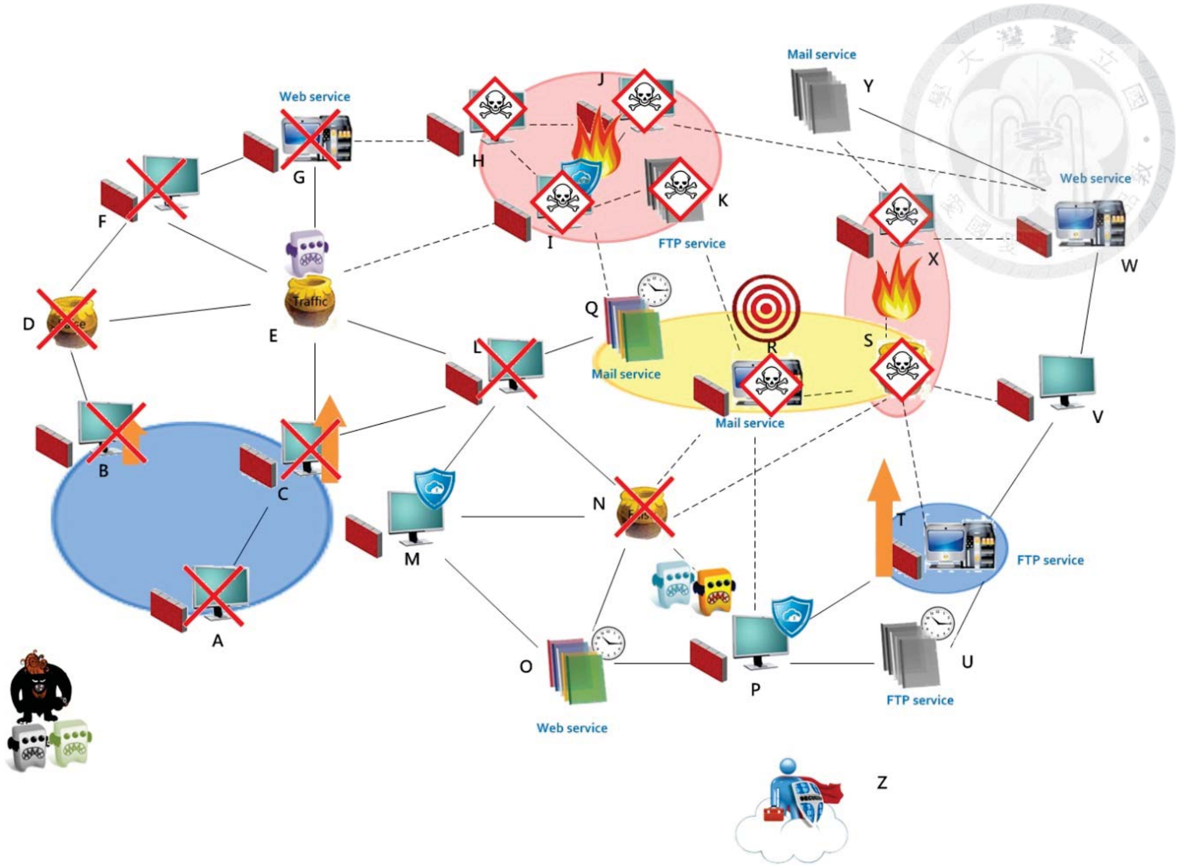


Figure 2-15: Secondary disaster – fire

After earthquake happened, there has a big chance to occur secondary disaster such as fire in our scenario and sometime damage caused by secondary disaster might be bigger than primary disaster. In Figure 2-15, after earthquake happened for a while which trigger secondary disaster fire happened in near node S area and the fire spread to node X caused node X and its link all broken.

Defender detected node P might be attacked. Since node P has deployed cloud security agent on it, defender decides to redirect the traffic to cloud security provider (Figure 2-16). Could security provider then eliminates the malicious traffic and sends the clean traffic back. Attackers still try to compromised node P and E, but commander is out of budget which means defender successfully guard the network this time using limit budget and face natural disaster and malicious attack still providing good quality of service to legitimate users.

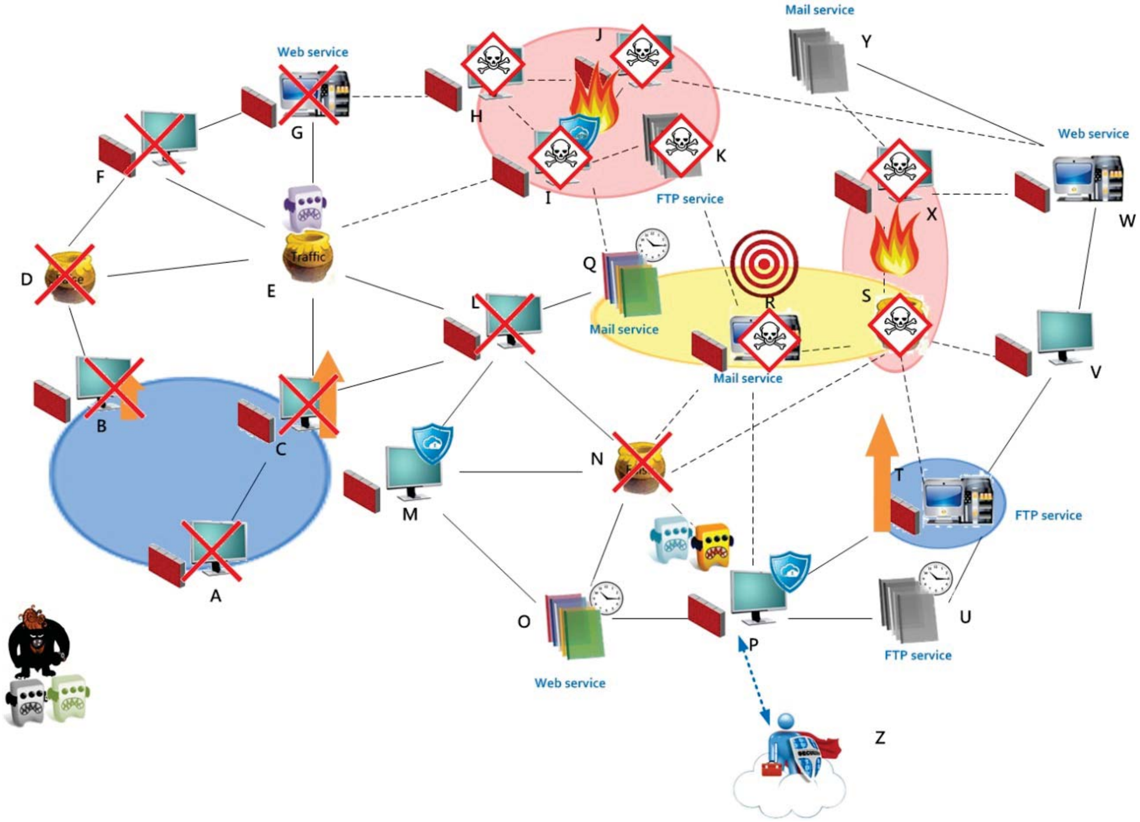


Figure 2-16: Cloud security service

Table 2-5 is our paper’s problem description.

Table 2-5: Problem Description

◆ Objective:

➢ To minimize maximized service compromise probability

◆ Given:

➢ All possible defense configurations, including defense resource allocations and defense strategies

- ➢ All possible attacker categories, including compromising commander attributes, attacker attributes and attack strategies.
- ➢ QoS threshold

◆ Subject to:

- ➢ Defender’s and commander’s total budget
- ➢ Maximize attacking time to compromise the netwrok

◆ To be determined:

- ➢ Attack and defense strategy
- ➢ Resource allocation in every defense strategy

2.3 Mathematical Formulation

In this section, we’ll introduce our mathematical formulation including given parameters, decision variable, verbal variable (in Table 2-6, Table 2-7 and Table 2-7) , objective function and its constraints.

Table 2-6: Given parameters:

Given parameters	
Notation	Description
N	The index set of all nodes
C	The index set of all core nodes
L	The index set of all links
M	The index set of all level of virtual machine monitors (VMMs)

S	The index set of all kinds of services
H	The index set of all types of honeypots
P	The index set of candidate nodes equipped with false target function
Q	The index set of candidate nodes equipped with fake traffic generating function
R	The index set of candidate nodes equipped with false target and fake traffic generating function
U	The index set of all level of cloud security services
V	The index set of all candidate nodes equipped with cloud security agent
Λ	The index set of all kinds of nature disasters considered
Γ	The index set of all types of redundant systems
B	The defender’s total budget
w	The cost of constructing one intermediate node
o	The cost of constructing one core node
p	The cost of each virtual machine (VM)
c	The cost of setting a cloud security agent to one node
E	All possible defense configurations, including defense resources and defending strategies
Z	All possible attacker categories, including attacker attributes, corresponding strategies and transition rules
F_i	The total attacking times on i^{th} service for all attackers, where $i \in S$
α_i	The weight of i^{th} service, where $i \in S$
K_p	The maximum number of virtual machines on VMM level p, where $P \in M$
d	The ratio of defense strengthen on VMs and VMM when local defense is activated
r_q	The ratio of defense strengthen using cloud security services level q, where $q \in U$
u_{ij}	The number of attackers subordinates in the attack group launching j attack, where $i \in S$, $1 \le j \le F_i$

$W_{threshold}$	The predefined threshold about QoS
$S_k^{priority_i}$	The priority of service i provided by core node k divided by the maximum service priority among core nodes in the topology, where $i \in S$, $k \in C$
$\beta_k^{threshold}$	The risk threshold of core node k, where $k \in C$
t_{fail}	Maximum time threshold to compromise network
ς_γ	The price of redundant system with level γ, where $\gamma \in \Gamma$
μ_λ	The intensity of nature disaster λ occurred, where $\lambda \in \Lambda$
$\Phi_\lambda(\mu_\lambda)$	The probability of nature disaster λ with intensity μ_λ occurred, where $\lambda \in \Lambda$
$\iota_\lambda(\mu_\lambda)$	The lower bound of range regarding disaster λ with intensity μ_λ occurred, where $\lambda \in \Lambda$
$\phi_\lambda(\mu_\lambda)$	The upper bound of range regarding disaster λ with intensity μ_λ occurred, where $\lambda \in \Lambda$
$\psi(\iota_\lambda(\mu_\lambda),\phi_\lambda(\mu_\lambda))$	The actual range of disaster λ with intensity μ_λ occurred, where $\lambda \in \Lambda$

Table 2-7: Decision Variables

Decision Variables	
Notation	Description
$\vartheta_{ks\gamma}$	1 if node *k* is equipped with redundant system level *γ* regarding service *s*, 0 otherwise, where $k \in \mathrm{N}$, $s \in S$ and $\gamma \in \Gamma$
$\overrightarrow{D_i}$	A defense configuration, including defense resource allocation and defending strategies on i^{th} service, where $i \in S$
$\overrightarrow{A_{ij}}\left(u_{ij}\right)$	A instance of attack configuration, including attacker's attributes, commander's strategies and transition rules of

	the commander ules of the commander j^{th} attack on i^{th} service, where $i \in S$, $1 \le j \le F_i$
$T_{ij}\left(\overline{D_i}, \overline{A_{ij}}\left(u_{ij}\right)\right)$	1 if the commander achieve his goal successfully, and 0 otherwise, where $i \in S$, $1 \le j \le F_i$
t_{fail}^{k}	Maximum time threshold to compromise node k, where $k \in N$
n_k	The non-deception based defense resource allocated to node k, where $k \in N$
e	The total number of intermediate nodes
l_p	The number of VMs level p VMM purchases, where $p \in M$
$v(l_p)$	The cost of VMM level p with l_p VMs, where $p \in M$
x_k	1 if node k is equipped with false target function, and 0 otherwise, $k \in N$
y_k	1 if node k is equipped with fake traffic function, and 0 otherwise, $k \in N$
z_k	1 if node k is equipped with cloud security agent, 0 otherwise, where $k \in N$
q_{kl}	The capability of direct link between node k and l, where $k \in N$, $l \in N$
$g(q_{hl})$	The cost of constructing a link from node k to node l with capability q_{kl}, where $k \in N$, $l \in N$
$B_{nodelink}$	The budget spent on constructing nodes and links.
$B_{general}$	The budget spent on allocating general defense resource
$B_{virtualization}$	The budget spent on virtualization
$B_{cloudagent}$	The budget spent on deploying cloud agents
$B_{specail}$	The budget spent on deploying special defense resource

$B_{honeypot}$	The budget of honeypots
$B_{redundancy}$	The budget spent on constructing redundant systems
δ_o	The number of services that honeypot o can simulate, where $o \in H$
ε_o	The interactive capability of false target honeypot o, where $o \in P$
θ_o	The maximum throughput of fake traffic that fake traffic generator honeypot o can achieve, where $o \in Q$
$h(\delta_o, \theta_o)$	The cost of constructing a false target honeypot with the number of simulating services and the interactive capability, where $o \in P$
$f(\delta_o, \theta_o)$	The cost of constructing a fake traffic generator honeypot with the number of simulating services and the maximum achievable throughput of fake traffic, where $o \in Q$
$t(\delta_o, \varepsilon_o, \theta_o)$	The cost of constructing a honeypot equipped with false target and fake traffic generating functions with the number of simulating services, the interactive capability and the maximum achievable throughput of fake traffic, where $o \in R$

Table 2-8: Verbal Notation

Verbal Notation	
Notation	Description
Y	The total compromise events
G_{core_k}	Loading of each core node k, where $k \in C$
U_{link_m}	Link utilization of each link m, where $m \in L$
K_{effect}	Negative effect caused by applying fake traffic adjustment
I_{effect}	Negative effect caused by fallacious diagnosis of cloud security service
J_{effect}	Negative effect caused by false positive while applying local defense

O_{tocore}	The number of hops legitimate users experienced from one boundary node to core nodes
W_{final}	The QoS level at the end of attack
$W(\cdot)$	The value of QoS determined by G_{core_k}, U_{link_m}, K_{effect}, I_{effect} and O_{tocore}, where $k \in C$, $m \in L$
$\omega_k^{\deg ree}$	The link degree of core node k divided by the maximum link degree among all nodes in the topology, where $k \in C$
$\rho_k^{\deg ree}$	The defense resource of the shortest path from detected attacked nodes to core node k divided by total defense resource, where $k \in C$
τ_k^{hops}	The minimum number of hops from detected attacked nodes to core node k divided by the maximum number of hops from attacker's starting position to one core node, where $k \in C$
$\beta_k(\cdot)$	The risk status of core node k which is the aggregation of $\rho_k^{\deg ree}$, τ_k^{hops}, $\omega_k^{\deg ree}$ and $S_k^{priority_i}$, where $k \in C$
D_{unsupply}	Unsupplied demand caused by partial redundant system

Objective function:

$$\min_{\overrightarrow{D_i}} \max_{\overrightarrow{A_{ij}}\left(u_{ij}, v_{ij}\right)} \frac{\sum_{i \in S}\left[\alpha_i \times \sum_{j=1}^{F_i} T_{ij}\left(\overrightarrow{D_i}, \overrightarrow{A_{ij}}\left(u_{ij}\right), t_{fail}, \Phi_q(\mu_q), \psi(\iota_q(\mu_q), \phi_q(\mu_q))\right)\right]}{\sum_{i \in S}\left(\alpha_i \times F_i\right)}$$

(IP 1)

Constraint:

$\overrightarrow{D_i} \in E$ $\forall i \in S$ (IP 1.1)

$\overrightarrow{A_{ij}}(u_{ij}) \in Z$ $\forall i \in S, 1 \le j \le F_i$ (IP 1.2)

$B_{nodelink} \ge 0$ (IP 1.3)

$B_{general} \ge 0$ (IP 1.4)

$B_{specail} \ge 0$ (IP 1.5)

$q_{kl} \ge 0$ $\forall k, l \in N$ (IP 1.6)

$g(q_{hl}) \ge 0$ $\forall k, l \in N$ (IP 1.7)

$w \times e \ge 0$ (IP 1.8)

$$w \times e + o \times \left\| C \right\| + \frac{\sum_{k \in N} \sum_{l \in N} g(q_{kl})}{2} \le B_{nodelink} \qquad \text{(IP 1.9)}$$

$n_k \ge 0$ $\forall k \in N$ (IP 1.10)

$\sum_{k \in N} n_k \le B_{general}$ (IP 1.11)

$x_k + y_0 \ge 1$ $\forall o \in H$ (IP 1.12)

$x_k = 0$ or 1 $\forall k \in N$ (IP 1.13)

$y_k = 0$ or 1 $\forall k \in N$ (IP 1.14)

$z_k = 0$ or 1 $\forall k \in N$ (IP 1.15)

$\sum_{k \in N} z_k \times c \le B_{cloudagent}$ (IP 1.16)

$v(l_p) \ge 0$ $\forall p \in M$ (IP 1.17)

$0 \le l_p \le k_p$ $\forall p \in M$ (IP 1.18)

$$\sum_{p\in M} v(l_p) + p \times \sum_{p\in M} l_p \le B_{virtualization} \qquad \text{(IP 1.19)}$$

$$\sum_{i\in P} x_i \times h\left(\delta_i, \varepsilon_i\right) + \sum_{j\in Q} y_i \times f\left(\delta_j, \theta_j\right) + \sum_{i\in N}\sum_{j\in N} x_i \times y_j \times t\left(\delta_i, \varepsilon_i, \theta_j\right) \le B_{honeypot} \qquad \text{(IP 1.20)}$$

$$\sum_{k\in N}\sum_{s\in S}\sum_{\gamma\in\Gamma} \vartheta_{ks\gamma}\varsigma_{\gamma} \le B_{redundancy} \qquad \text{(IP 1.21)}$$

$$B_{virtualization} + B_{cloudagent} + B_{honeypot} + B_{redundancy} \le B_{special} \qquad \text{(IP 1.22)}$$

$$B_{nodelink} + B_{general} + B_{special} \le B \qquad \text{(IP 1.23)}$$

$$\sum_{k\in N} t_{fail}^{k} \le t_{fail} \qquad \text{(IP 1.24)}$$

$$h(\delta_0, \varepsilon_0) \ge 0 \qquad \forall o \in P \; \text{(IP 1.25)}$$

$$f\left(\delta_o, \varepsilon_o\right) \ge 0 \qquad \forall o \in Q \; \text{(IP 1.26)}$$

$$t(\delta_o, \varepsilon_o, \theta_o) \ge 0 \qquad \forall o \in N \; \text{(IP 1.27)}$$

Table 2-9: Verbal constraint:

Verbal Constraints	
$\frac{\int_{y=1}^{Y}[w_i(G_{core_k}, U_{link_m}, K_{effect}, I_{effect}, J_{effect}, O_{tcore}, D_{\text{unsupply}})]dy}{Y} \ge W_{threshold}$, where $i \in S, k \in C, m \in L$	(IP 1.28)
The performance reduction cause by compromised core nodes, local defense, cloud security or applying partial-copy redundancy should not make legitimate users' QoS satisfaction violate (IP 1.28)	(IP 1.29)
At the end of attack, final QoS constraint must be satisfied. $W_{final} \ge W_{threshold}$	(IP 1.30)

All the defense strategies are adopted only if the risk levels are lower than a predefined threshold. $\beta(\rho_{defense}, \tau_{hops}, \varpi_{degree}, s_{priority_i}) \leq \beta_{threshold}$, where $i \in S$	(IP 1.31)

Explanation of the objective function:

- Objective function: Our problem is a bi-level MinMax problem like in (IP 1). Commander would adjust their attack strategies first in order to maximize the success probability. Second, defender then figure out their best corresponding defense strategy to minimum these maximum probability.
- (IP 1.1) and (IP 1.2): these two constraints show all possible solution of attacking and defending strategies.
- (IP 1.3) ~ (IP 1.5): these three constraints are defender’s budget distribution constraints, all of them cannot be zero.
- (IP 1.6): the capacity of all links cannot lower than zero.
- (IP 1.7): the cost of constructing a link cannot lower than zero.
- (IP 1.8): the cost of deploying intermediate nodes cannot lower than zero.
- (IP 1.9): the sum of constructing core nodes, intermediate nodes and links cannot exceeds the constructing topology’s budget.
- (IP 1.10): the cost of deploying proactive defense resource on each node cannot

lower than zero.

- (IP 1.11): the total cost of proactive defense resource cannot exceed the budget distributing to proactive defense.
- (IP 1.12): honeypot should at least be equipped with one function.
- (IP 1.13) ~ (IP 1.15): these three constraints are binary restrictions on decision variables.
- (IP 1.16): total cost of constructing cloud security agent cannot exceed its budget.
- (IP 1.17): cost of constructing all VMMs cannot less than zero.
- (IP 1.18): the number of VM on VMM cannot greater than the maximum number of VMs in level *p*.
- (IP 1.19): the total cost of virtualization cannot exceed the budget of deploying virtualization.
- (IP 1.20): the total cost of honeypot cannot exceed the budget of deploying honeypots.
- (IP 1.21): the total cost of constructing redundancy cannot exceed budget of deploying redundancy.
- (IP 1.22): the total budget of all kinds of reactive defense cannot exceed the budget of reactive defense resource.
- (IP 1.23): the budget of all purposes cannot exceed defender’s budget.

- (IP 1.24): the sum of compromise time cannot greater than the time threshold that compromising the network.
- (IP 1.25) ~ (IP 1.27): the cost each types of reactive defense cannot lower than zero.
- (IP 1.28) ~ (IP 1.30): the average QoS cannot lower than threshold that legitimate users request during the attack process.
- (IP 1.31): defender can only activate reactive defense mechanism when the risk status is dangerous higher than expected value.

Chapter 3 Solution Approach

3.1 Mathematical Programming

Mathematical programming is a popular method to solve the optimal problem. Mathematical programming is the selection of a best element (with regard to some criteria) from some set of available alternatives. Hence, it is very suitable to use mathematical programming to solve our problem because our problem is also want to select the best solution in all kinds of defense strategies in order to maximize system survivability.

There are three ways to evaluate performance: best case, average case and worst case. Using best case to evaluate performance will be too optimistic since best case is seldom happened. If using best case to evaluate situation, it may cause decision-makers make wrong decision facing the problem. Worst case is also an extreme processing method because it is seldom happened, too. If using worst case to solve the problem means attackers has complete information about the network topology which will help them easily compromised network and it is unusual in the real world. Therefore, we use average case to evaluate performance. Commander only has incomplete information about the network topology and they need to base on this information to make decision.

3.2 Monte Carlo Simulation

Because we assume that commander only has incomplete information, it will lead defender needs to face all kinds of attack strategies with different attackers group. Worst of all, different commander will make different decision based on all kinds of attributes and various of situations which will make the problem more complicate. It is difficult to only use simple mathematical model to handle average case. Hence, we need to combine another approach called Monte Carlo simulation to help us solve the problem [44].

Monte Carlo simulation can use in many domain; it use to deal with problem which is unfeasible or impossible to compute with a deterministic algorithm. Monte Carlo simulation can solve complex, non-linear, involving many uncertain’ s problem by repeating random sampling to compute the results and execute more experiments may have higher probability to get the result closing to real situation. Even though it needs more time to compute to get the final result since it needs to execute thousands of times, it still a good manner to solve those non-deterministic problem. Since our problem has a lot of uncertainty of both attack and defense strategies, we adopt Monte Carlo simulation to simulate attack-defense scenarios.

3.3 Problem Evaluation Process

As we mentioned before, we combine mathematical programming and Monte Carlo Simulation to solve the problem and use Monte Carlo simulation to evaluate the network survivability. In the execute process, it will also collect some useful information which can help us find out the effective defense strategy and resource allocation dealing with different kinds of situation. The following we will introduce evaluation process.

- Evaluation Process:

First, defender would determine a defense configuration randomly. Defender needs to decide topology configuration and all kinds of resource allocation. Second, we need to know the performance of the initial configuration afterward we can enhance to configuration. Therefore, we evaluation this initial configuration by running *M* times of simulations with different commanders. Monte Carlo Simulations needs to execute certain times which will make the result more close to the average case. We decide to rum M times experiment. We will also base on the relationship between success attack times and total evaluation times to adjust value *M* to find out the ideal number of total evaluation time. After running *M* times evaluations, we will use average service compromise probability as the standard to compare with the result after enhancement.

Third, we will adjust attack and defense configuration by enhancement process which we will introduce in 3.4 and it will come up with a new configuration. Fourth, we then use this new defense configuration evaluate its performance again by running M times simulations. The third and fourth steps will repeat several times until reach the terminal condition. Defender who will choose an expected number of enhancement times in advance. When reaching that times, it will end enhancement process. Another situation is that enhancement process cannot help quality getting better then after certain times we will terminate simulation. Fifth, we will get a result from enhancement process, and then we can use it to compare with the initial one. We can see the whole evaluation process in Figure 3-1.

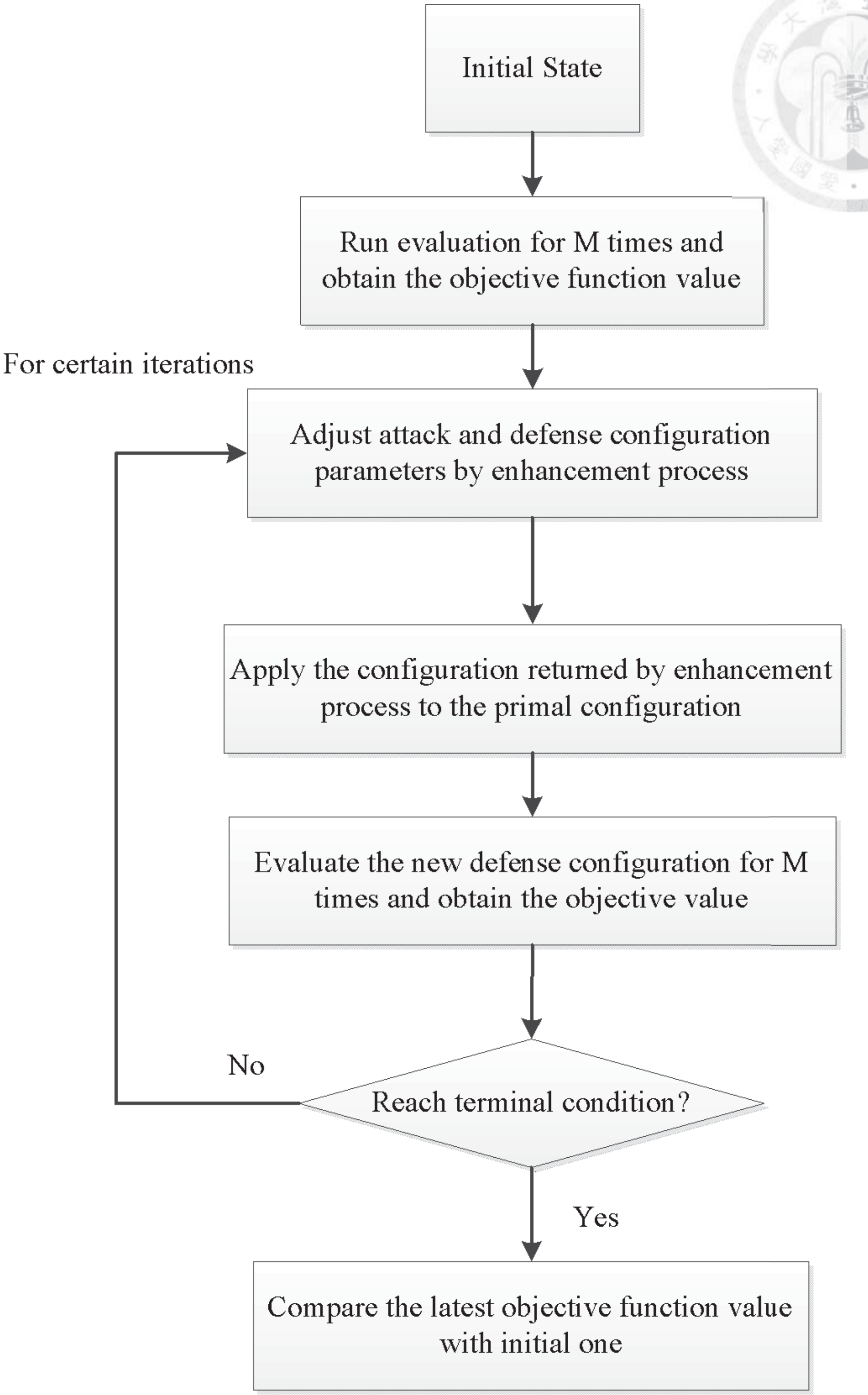

Initial State
Run evaluation for M times and obtain the objective function value
For certain iterations
Adjust attack and defense configuration parameters by enhancement process
Apply the configuration returned by enhancement process to the primal configuration
Evaluate the new defense configuration for M times and obtain the objective value
No
Reach terminal condition?
Yes
Compare the latest objective function value with initial one

Figure 3-1: Flow Chart of Enhancement Process

3.4 Policy Enhancement

In this section, we will introduce the enhancement process that we mentioned before. Both commander and defender will enhance their strategies and resource allocation in order to reach their goal. Commander would want to maximize their compromising success probability and defender would want to minimize the value in other word is want to maximize network's survivability. We will introduce both commander and defender's enhancement in the following.

3.4.1 Commander Enhancement

There are three kinds of attacking strategies to compromise the node which are collaborative attack, non-collaborative attack and pretend to attack. The commander enhancement is to choose the best strategies in order to increase the chance of compromising the network.

Collaborative attack is attacking by several attackers to compromise a node. Non-collaborative is attacking by single attacker to attack the victim node. Pretend to attack is like the literally means. Commander would send an attacker with low energy and capability to attack. Commander will score the victim node by considering traffic, proactive defense resource and the failure time of attacking this node and it will give divide a score between 0-1. Commander will base on this score to decide which attacking strategy they want to use. This score is represent commander how badly wants to compromise this node. Hence, if this score is high represent commander wants to compromise this node badly and commander will adopt collaborative attack and the following are non-collaborative attack and pretend to attack.

We will enhance the attacking strategies by adjust the score’s threshold of three attacking strategies. We will use exhaustive search to see all possibility and its related success probability to find out the best boundaries. The score’s threshold will adjust 0.1 once a time.

3.4.2 Defender Enhancement

Initial defense configuration is according to heuristic method to evaluate. We will use hops from node to core node and node’s link degree to estimate each node’s importance. Node which is close to core node (numbers of hop is lees) and link degree is higher is more important. After evaluation process, we will collect useful information from initial defense configuration. Defender then can use this information to adjust their configuration and resource allocation in order to enhance their survivability.

In the following, we will introduce two defender enhancement approaches: “Definition of Gradient” and “Local Information Estimation”.

(1) Enhancement by local information estimate

The whole idea of local information estimation is too decrease the unnecessary expense and add more resource to useful defense strategies. Therefore, if one strategy or node is useless then we might consider removing it and if one defense strategy shows good effect we may consider adding more. We will base on previous information and some rules to make decisions. The process will relax budget constraint first; we can add more resource on defense strategies or nodes which we think effective. Second, since defender still only have limited budget, we need to remove some relative useless defense strategies or nodes by using expected value to evaluate.

In the enhancement process, first we will evaluate the topology status and see where should add some nodes or links and then evaluate the new topology's performance. Second, we then base on this new topology to increase each node's proactive defense resource; then use the new topology and new proactive defense resource allocation to evaluate the performance. Third, we will use the new configuration to increase reactive defense by node and then also evaluate the performance. In the whole increasing process, we will base on the information getting from evaluation process and heuristic rule.

But we need to get primal feasible by dropping some resource that is relative useless since defender has limited budget we cannot just increase resource. We will use expected value to evaluate useless resource allocation and decrease until budget fit with the constraint. Different defense strategies will use different formulation computing a expected value and choose the smallest one to decrease. Keep choosing and decrease until fit the budget constraint. Finally, we will get the final solution which is fitting the budget constraint and use this result to compare with the initial one to see the enhance result is better or not. The process is like Figure 3-2 as below.

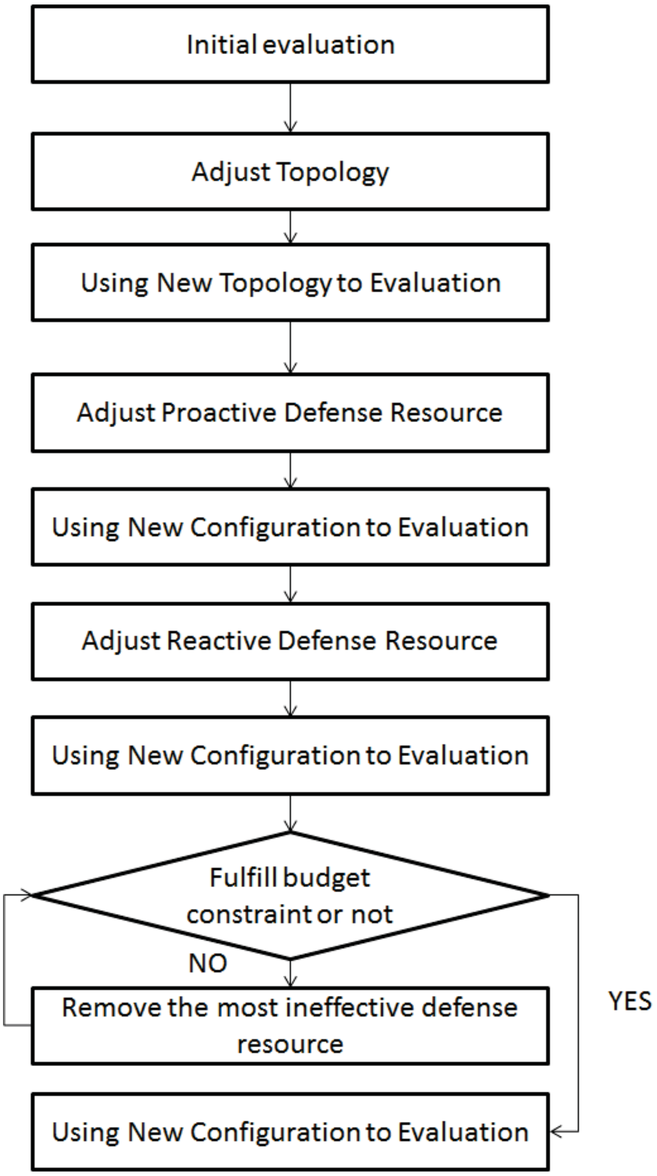

Initial evaluation
Adjust Topology
Using New Topology to Evaluation
Adjust Proactive Defense Resource
Using New Configuration to Evaluation
Adjust Reactive Defense Resource
Using New Configuration to Evaluation
Fulfill budget constraint or not
NO
Remove the most ineffective defense resource
YES
Using New Configuration to Evaluation

Figure 3-2: The process of enhancement by local information estimate

In the following, we will introduce the first three steps in detail.

- Adjust topology

Adjusting topology can separate as two parts: remove nodes and then add new nodes. Not only we need to consider malicious attack but also need to keep an eye on natural disaster.

To deal with natural disaster, we want to reduce the risk that nodes being destroy by natural disaster. Hence, we will estimate each node’s location and the frequency of being destroyed by natural disaster. If nodes are too close to the seismic zone or often destroyed by natural disaster, removing those nodes maybe can increase system’s survivability. In the same way, if we need to add new nodes, we also need to avoid installing nodes around the seismic zone.

In addition, we examine other factors in order to deal with malicious attack. We want to draw those nodes that are both used less to users and attackers. We use link capacity and the number of being attacked as the indexes to estimate each node’s degree of importance and draw the useless nodes.

The second part: adding new nodes. We want to increase the distance from edge node to core node. Therefore, we use hops to core node and being compromised rate as indexes to estimate whether adding new nodes or not. Attackers then need to spend more effort compromising the system.

- Adjust proactive defense resource and reactive defense resource

Each defense resource will use different factors to compute scores and using two methods (defense front and minimum cut) to select nodes that need to increase defense resource with different resource types. First, we will introduce two methods: defense front and minimum cut. If the node is at the defense front or minimum cut, which means it is suitable to increase that kind of defense resource. We will add that kind of defense at the node.

- Defense front:

We want to put right defense at right place. We use defense front to help us achieve this goal. We want to construct a castle like defense front. We can put more resource at the defense front. Different defense resource will have different rules to help us construct defense front. We will use grid topology and with 25 nodes to show how to construct defense front.

Take false target as example. We want to cheat attackers whose attack goal is steal confidential information. Because only that kind of attacker will being cheated by false target and stop attacking. Hence, we use times of being targeted by attackers when their goal is stealing information as index to construct defense front. Figure 3-3 is each node’s score distribution. The number is represented its score. We want to choose those nodes are frequent targeted by attackers.

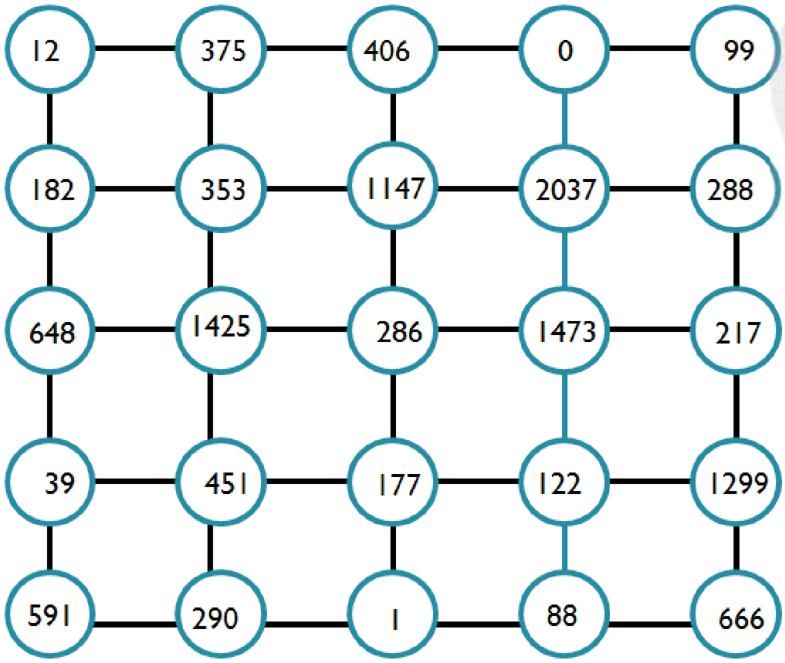


Figure 3-3: Score distribution

Therefore, these three nodes marked with red color is the top three of all 25 nodes as Figure 3-4.

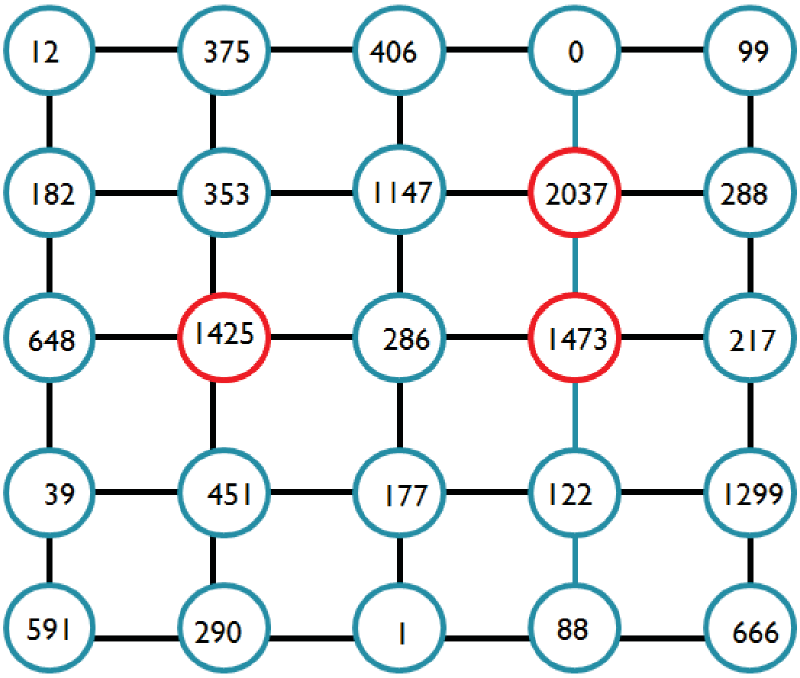


Figure 3-4: Score distribution (2)

We will use these three nodes as start point and end point. Each time choose two nodes as start point and end point to find out shortest path, but when finding shortest path we still considerate each node's score. We will choose the one whose score is better than neighbors. The result shows as below Figure 3-5. This is defense front of false target. The nodes those at the defense front are suitable for installing false target.

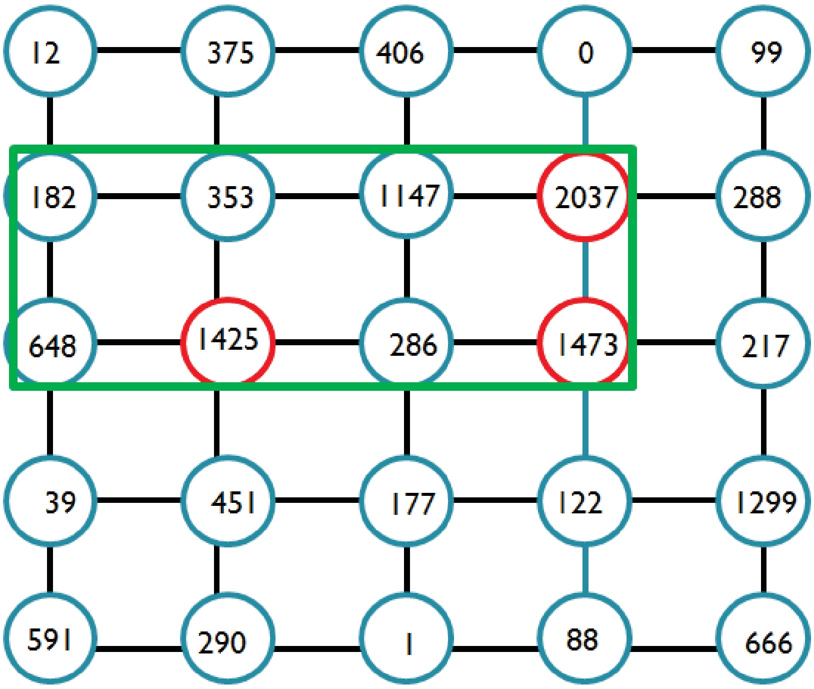


Figure 3-5: Defense front

- Minimum cut:

For many problems, it is hard to directly find out its solution. But sometimes by the mean time of solving another problem, it also finds out the primal problem's solution. Maximum flow minimum cut is a good example. By solving minimum cut, it also obtains maximum flow. Therefore, we want to use minimum cut to help us find out the right place to put defense resource. Dealing different defense resources can use different factors as the weight and find each defense resource's minimum cut. By solving minimum cut problem, we may find out the weakest part or the strongest part. Then we can put suitable defense resource on those nodes that are at minimum cut.

For example, we use the ratio of attacker's remaining budget as the index to estimate where should put more proactive defense resource. If the node's score is small which is good means even though attacker reach that node it has high probability that attacker doesn't have enough budget to compromise the node. We only need to put more money on those nodes and the compromised probability may decrease a lot. Each service will use this index to find out a minimum cut. We can select to put more proactive defense on those nodes to protect those core nodes that behind them.

We use two methods to construct minimum cut. First one is construct a virtual start point and virtual end point. We link all edge nodes to virtual start point and all core nodes to virtual end point. We then use this graph to construct minimum cut. Every service will build a minimum cut. Figure 3-6 is an example of minimum cut.

Second one is using every edge node as start point and construct minimum cut for each service. If use mini scale of topology, that would construct six minimum cuts (3 terminal nodes * 2 service type). The final result would use union set of all minimum cuts.

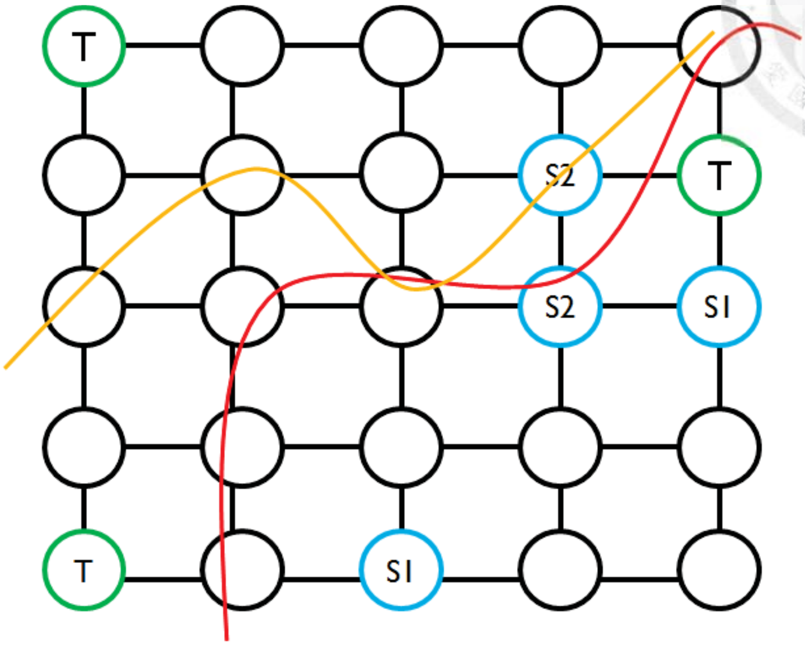


Figure 3-6: Minimum cut of proactive defense resource

The following table 3-1 shows the indicators adopted by each defense resource. We will use these indicators as input parameters to construct each defense resource's defense front or minimum cut.

Table 3-1: Indicators of each defense resource

- Proactive defense resource:

  Ratio of attacker's remaining budget.

- Virtual machine monitor:

  The number of failure attack on each node.

  The ratio of detected attacked times on each node.

- Honeypot- fake traffic:

Times of being visiting by users.

- Honeypot- false target:

  Times of being targeted by attackers when their goal is stealing information.

- Cloud security:

  Attacker’s remaining budget.

  The ratio of detected attacked times on each node.

  Distance from current node to terminal nodes.

- Redundancy:

  Total being attacked rate.

  Total being compromised rate.

  The frequency of being destroyed by earthquake.

  Distance from current node to terminal nodes.

After construct minimum cut or defense front, we still use some indicators to estimate each node at the defense front or minimum cut in order to make sure those nodes are suitable to increase more budget on them. Table 3-2 shows factors of each defense resource that we estimate.

Table 3-2: Indicators of each defense resource (2)

- Virtual machine monitor:

  The same factors as Table 3-1.

- Honeypot- fake traffic

  Hops to core node.

- Honeypot- false target

  Node’s total being compromised rate.

- Cloud security

  Using compromised probability and proactive defense resource as indexes.

- Redundancy

  The same factors as Table 3-1.

(2) Definition of Gradient

The idea is similar with local information estimation. We want to find out useful defense strategies. We adopt mathematical method Gradient to evaluate configuration’s performance. We also will relax the budget constraint first, then defender can increase more resource on every resource type. After that, we will use other rules to decrease resource in order to fit the budget constraint again.

First, we will increase the same amount Δ on topology, proactive defense resource, and each reactive defense resource. We also use defense front or minimum cut to help us find out which node should increase resource. We use the same indicators as we mentioned before.

Next step, we will compute the derivative $d_i(\nabla)$ of each resource types using the following formulate to estimate effect of each defense resource:

$$d_i = \frac{Z' - Z}{\Delta} \qquad \text{(Eq. 3.1)}$$

where

Z': Z' is service being compromised probability after increasing Δ amount resource

Z: Z is the origin configuration that being compromised probability

We use d_i to choose which defense resource is better and will actually put more resource on it. We use following formulation to compute the increase amount:

$$B_i^{k+1} = (1 + d_i) \times B_i^k \qquad \text{(Eq. 3.2)}$$

Where

k: k is which iteration

In the increasing process, we also use defense front or minimum cut to help us find suitable nodes.

After increasing process, we still need to decrease budget in order to fit the original budget constraint. We will use d_i again to find the worst defense resource and remove some budget from it and repeat until fit the budget constraint.

3.5 Initial Allocation Scheme

In the following, we will introduce our initial allocation scheme such as topology generation and defense resource allocation method.

3.5.1 Topology Generation

There are three kinds of topology that can construct in our thesis which are grid, scale-free and random. Because the amount of nodes and links will affect other defense resource due to the total budget constraint, which may influence evaluation result, we will control the amount of nodes and links in different topology type to make it more similar. We use the algorithms mentioned in [46] and [47] to construct scale-free and random topology.

3.5.2 Proactive Defense Resource Allocation

We will deploy proactive defense resource on every node and use two major factors which are hops to core node and link degrees to estimate the importance of node in order to determine the amount of proactive defense resource on every node.

If the node is close to core node, we need to avoid attacker getting through the node and reach to core node. Hence, we will put more proactive resource on the nodes that is close to core nodes. We also use node’s link degree as another indicator. Higher link degree will have higher probability that attackers will reach to the node. Thus, the node will have higher probability being attacked and need more protection. There are also some other factors that we care. For instance, terminal nodes and core nodes will need more protection than others and we also will base on different reactive defense resource to do some adjustment.

3.5.3 Reactive Defense Resource Allocation

Reactive defense resource is another strong protection against to malicious attacker and natural disaster. We need to make sure reactive defense resource indeed exert its function. The location and the amount of reactive resource will become very important. For example, if attacker compromised false target, it has a chance can let attacker believe that he has successfully stolen the confidential information. Therefore, it is good choice to allocate false target on the way to core node. Fake traffic honeypot will need to have some distance with core node because it needs time to distract attackers heading to other direction. If it is too close to core node, it will lose its original effect. Different reactive defense gave different characteristic. We need to use these characteristics to well allocate our limited budget. At initial configuration, we will equally distribute budget on every reactive defense resource since we don’t know which defense resource is better. The investing amount of reactive defense resource and each one’s location will have further adjustment by enhancement process.

Chapter 4 Computational Simulations

4.1 Experiment Environment

Our entire experiment is written in C language in Code::Blocks 10.05. The experiment is executed on our desktop with Intel Core i7-3770 CPU 3.40 GHz and with 16 G main memory and the operating system is Microsoft Windows 7. The system parameters are showed at Table 4-1 as below.

Table 4-1: System Parameters

Parameter	Value
CPU	Intel Core i7-3770K e.40GHz
Main Memory	16.0 GB
Operating System	Microsoft Windows 7
Programming Language	C
IDE	Code::Blocks 10.05
Compiler	GNU GCC

Except three kinds of topology type: grid, random and scale-free, we also construct different topology scale. Each kind of topology type has five scales. Each scale has different number of nodes, core nodes, service type and total budget. The larger scale of topology, the more budget of defender has. The detail parameters are showed as below Table 4-2.

Table 4-2: Parameters of Defender

Parameters	Value				
Topology Type	Grid, Random, Scale-free				
Topology Scale	Mini	Tiny	Small	Medium	Big
No. of Nodes	9	25	49	100	169
No. of Terminal	1	3	5	5	5
No. of Service	1	2	3	3	4
No. of Core Node	(2)	(2,2)	(2,2,4)	(2,4,7)	(2,2,4,7)
Weight of Each Service	(1)	(1,1)	(1,1,2)	(1,2,3)	(1,1,2,3)
Total Budget	500000	1,500,000	2,700,000	5,600,000	11,500,000

The parameters of commanders are showed as below Table 4-3. We use normal distribution to generate commanders' budge, the number of attackers that he led and those attackers' characteristic such as energy, capability and harmonization. Commander's attack goal can divide into two parts: steal confidential information and disruption as his goal.

Table 4-3: Parameters of Commander

Parameter	Value
Commander's total budget	2,000,000 – 4,000,000
Goal	Steal confidential information

	Service disruption
No. of attackers per group	5-14
Attacker’s energy	80-120
Capability of attacker	0.7-1.3
Harmonization of attacker	0-100

Parameters of natural disaster are showed as below Table 4-4 and Table 4-5. We will generate several seismic zones by normal distribution. Different topology scale will contain different number of seismic zone. There are total eleven Richter scales. We only deal with from four to nine scales. Because from zero to three Richter scale barely impact building and ten Richter scales is rare happened. We adopt historical statistic data which is described each scale’s probability of occurrence as we mention before. The reason of cause fire can divide into three types: heating, electrical malfunction and others. We also adopt historical static data which is described each type’s probability of occurrence as we mentioned before.

Table 4-4: Parameters of Earthquake

Parameter	Value					
Seismic zone	Tiny:3	Mini:5	Medium:8	Big:12	Big:17	
Richter scale	Only deal with 4-9					
Probability of occurrence	4	5	6	7	8	9
	0.6564	0.0864	0.0064	0.0004	0.0002	0.0001

Table 4-5: Parameters of Fire

Parameter	Value		
The reason of cause fire	heating, electrical malfunction and others		
Probability of occurrence	Heating	electrical malfunction	Others
	0.13	0.08	0.79
Impact range	2 scale		

4.2 Simulation Result

4.2.1 Convergence Evaluation Times

It is important to find out a suitable evaluation times. If the evaluation time is too small not enough, we cannot get stable result. Hence, we need to find out evaluation times first. We decide a converge experiment. We use grid topology with 25 nodes to execute the experiment. We run plenty of times simulation and compute to cumulative compromised probability. Every 1000 times, we collect the result and compute average compromised probability as a unit and the average compromised probability is P_i. Every 1000 times, we will compare cumulative compromised probability until this time with the cumulative compromised probability of previous (*n*-1) times' result. Using mathematical express is comparing $(\sum_{i=1}^{i=n} P_i)/n$ and $(\sum_{i=1}^{i=n-1} P_i)/(n-1)$. If the difference is less than 0.0001, we will count one time. It needs to accumulate to 50 times which is less than 0.0001. We will consider the result as convergence. The experiment result is showed as below in Figure 4-1. At the beginning, the compromised probability is still very unstable. By increasing the simulation times, probability becomes stable and reaches the stopped condition. We total run five times and adopt 70,000 as our simulation times.

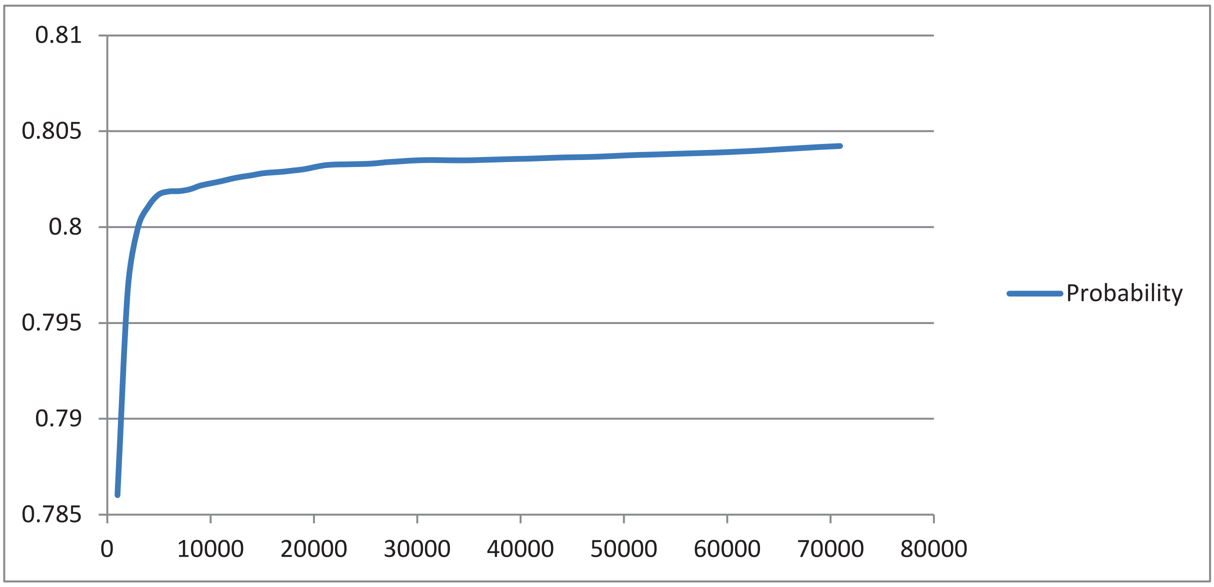


Figure 4-1: The experiment result of convergence

4.2.2 Robustness Experiment

In this section, we show the result of robustness experiment with different topology type and scale as below Figure 4-2. As we can see, using same topology scale with different topology type still retain similar trend. Compromised probability is strongly affected by topology scale. It is difficult to compromise the system when the topology scale is bigger since attacker needs to compromise more nodes to achieve their goal and also big topology scale can contain more variety of defense resource because it has more nodes to put those defenses on it. The depth of topology will also influence performance of reactive defense resource. Similarly, since grid topology has higher average hops to core node, its compromised probability is lower than other two topologies with the same topology scale.

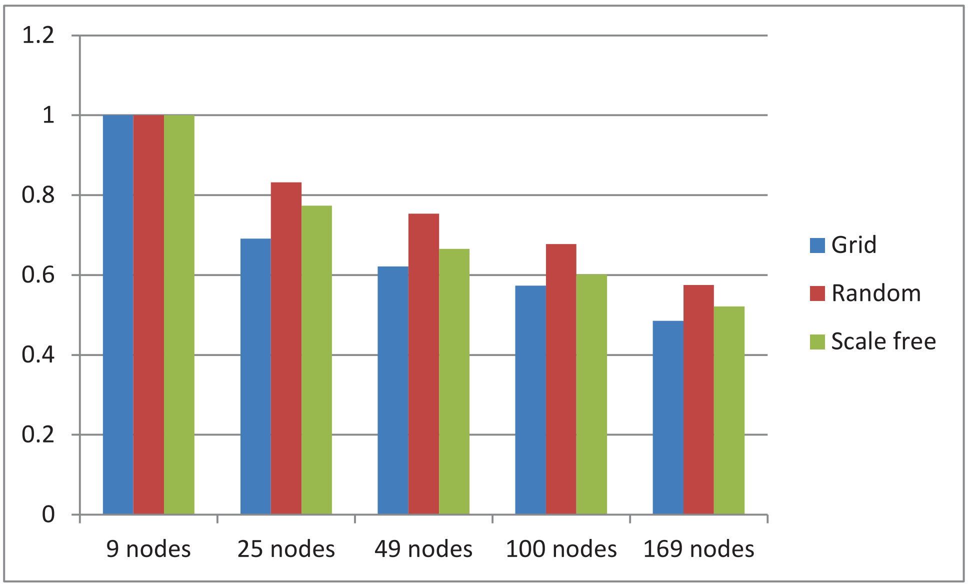


Figure 4-2: Compromised probability of different kinds of topology and scale

4.3 Enhancement Result

We want to help defender increase their survivability by adjust their defense resource allocation and topology. We will use two enhancement methods: local information estimate and definition of gradient to estimate our enhance effect. We use grid topology with 25 nodes to simulation. We use the same commander, defenders, topology and disasters as input parameters to estimate each experiment.

4.3.1 Enhancement by local information

When evaluate which node should increase defense budget, we will use two different methods defense front and minimum cut as we mentioned before to do the experiment.

- Defense front

First, we introduce the enhancement result using defense front. Compromised probability is decrease from 0.734277 to 0.41527. First we will discuss the change of topology. Figure 4-3 is the initial topology. We have two services corresponding to two core nodes and have three edge nodes. Figure 4-4 is the topology after enhancement. The skull sign is represented the seismic zone.

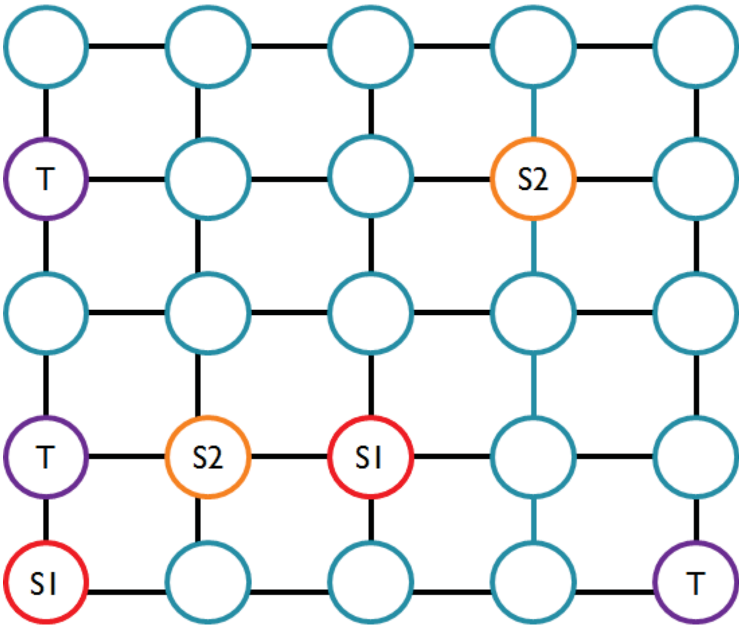


Figure 4-3: Initial topology

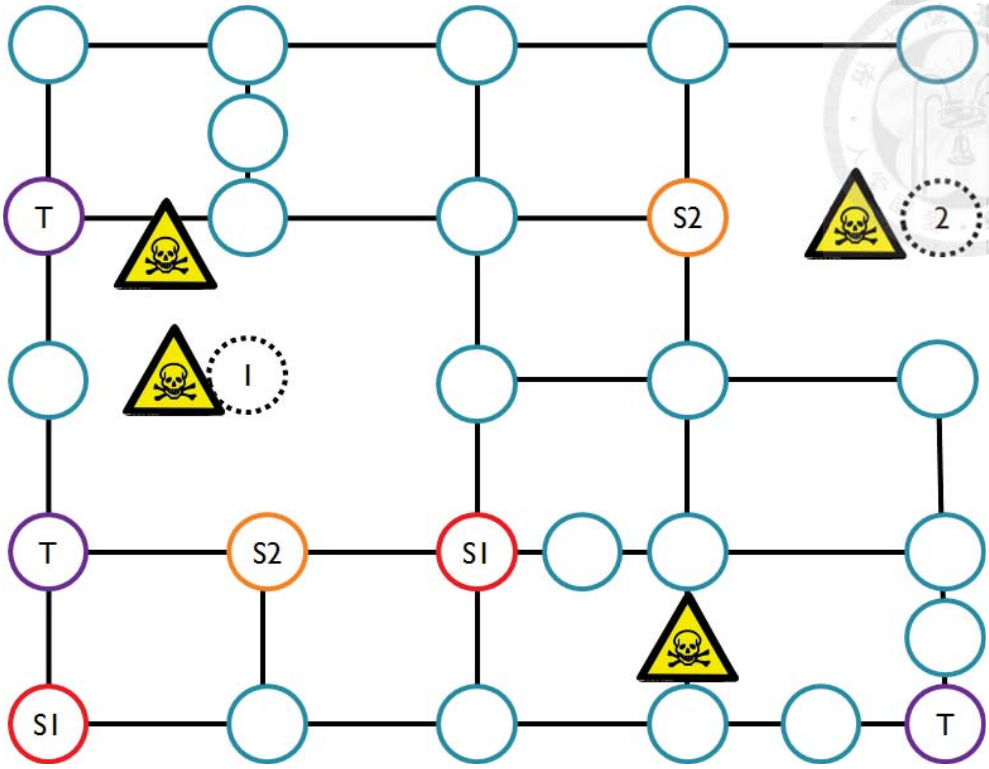


Figure 4-4: Topology after enhancement

We can see there are two nodes being removed and add four nodes at other place. The two nodes being removed are close to seismic zone. We also add new nodes on the path to core nodes. It can help defender deplete attacker’s budget and decrease compromised probability.

Figure 4-5 is the initial configuration (without proactive defense resource) and Figure 4-6 is the configuration after enhancement.

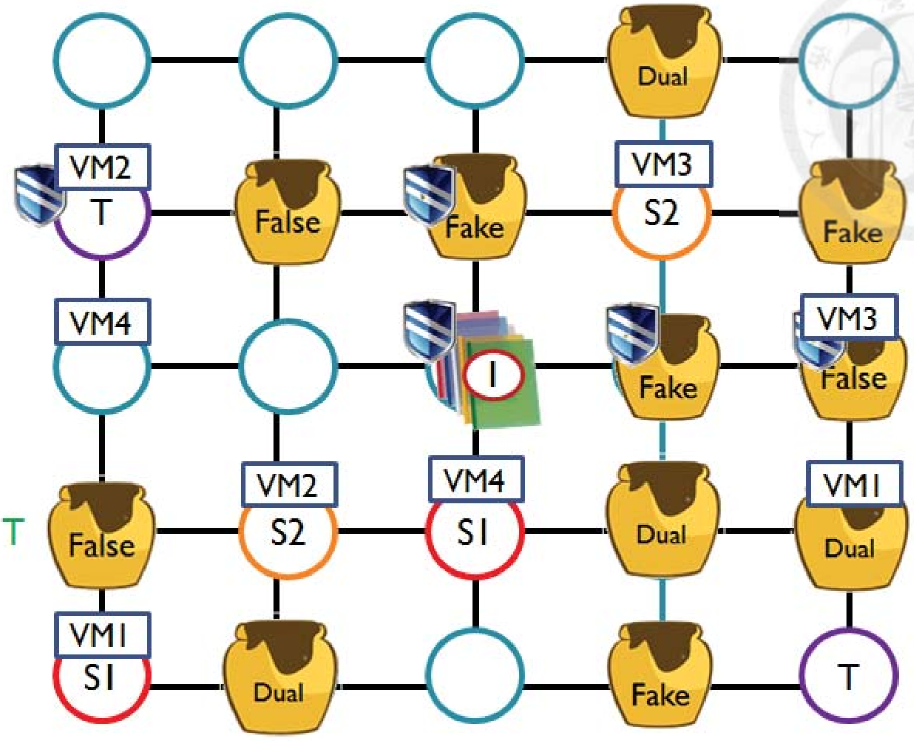


Figure 4-5: Initial configuration

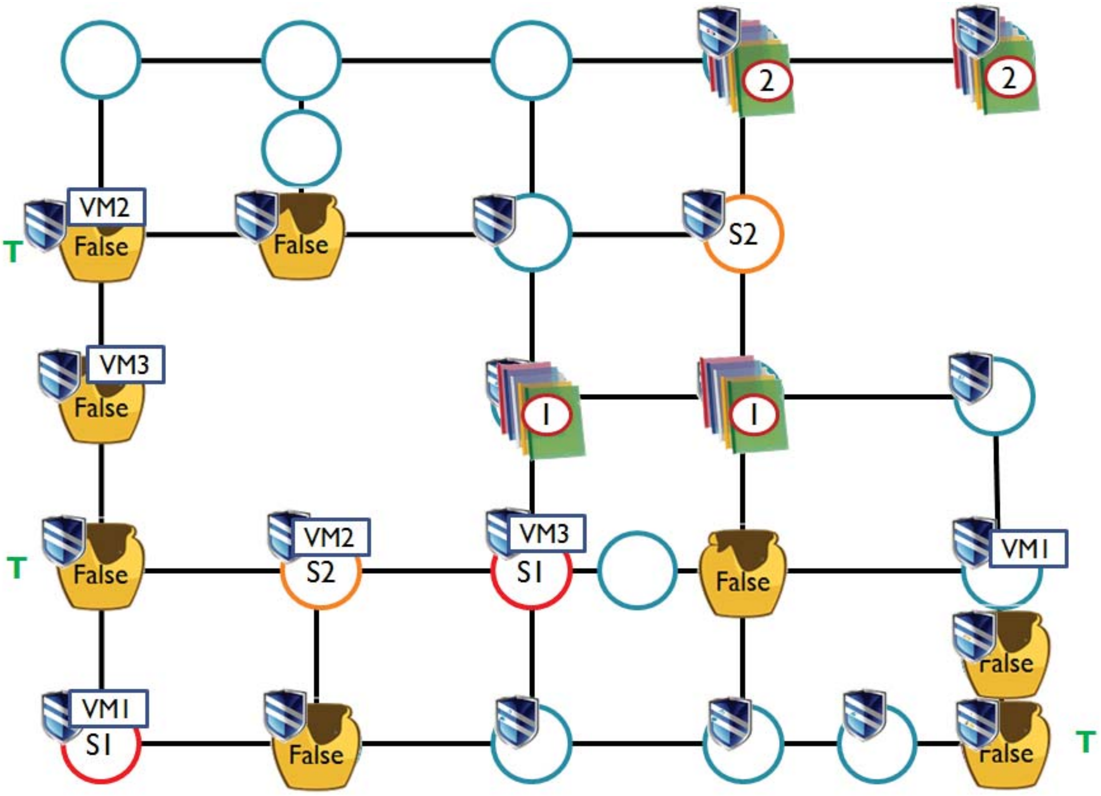


Figure 4-6: Configuration after enhancement

As you can see, those nodes that are close to edge nodes, we install false target trying to fool attacker to stop attacking. Many core nodes are install virtual machine and their group member are put close to edge node. As long as those nodes with virtual machine are not being compromised, those nodes which are in the same group can increase their defense intensity. Hence, core nodes can keep increasing intensity make them difficult to compromised. Virtual machine can collocate with cloud security. Because when activating cloud security, the node become hard to compromise and it as long as nodes not being compromised it can activate local defense and increase its defense strength. It also increases three redundancies and put those redundancies far away edge nodes. Figure 4-7 and Figure 4-8 show distribution of proactive defense resource and Table 4-6 shows some data about enhancement. The numbers means proactive defense resource on each node.

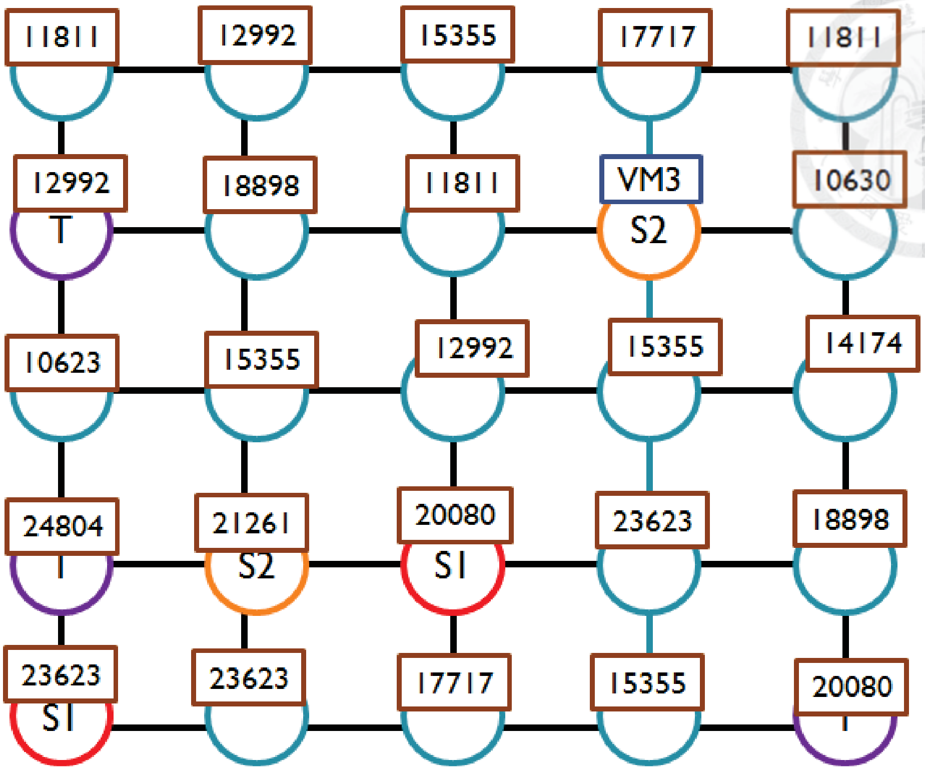


Figure 4-7: Initial proactive defense distribution

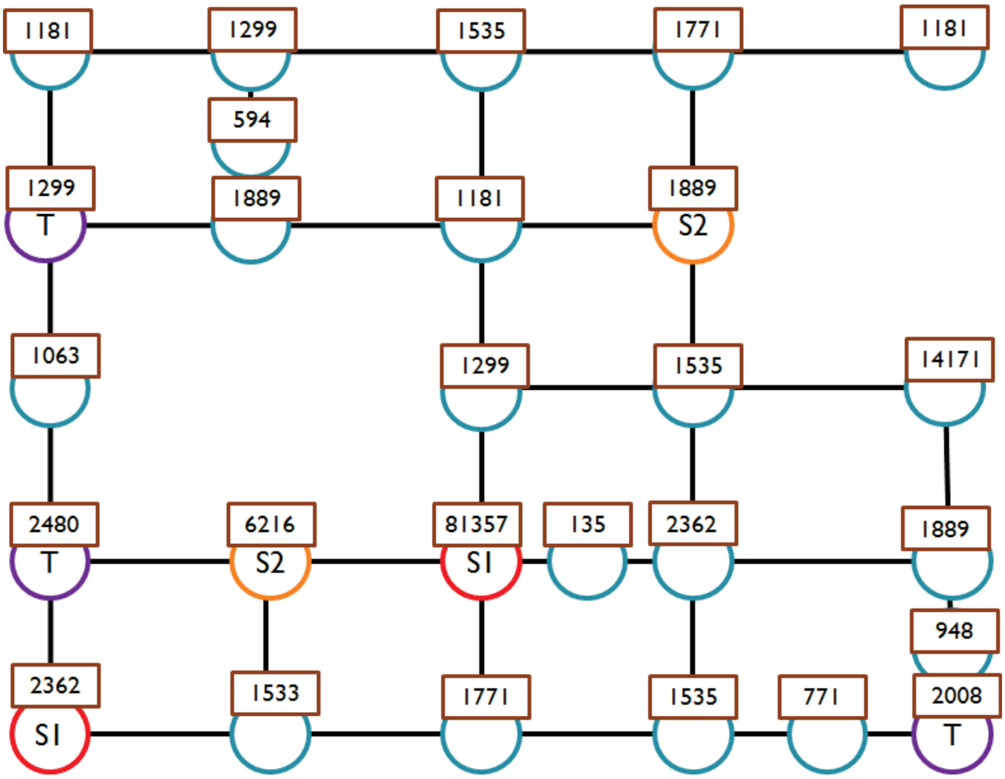


Figure 4-8: Proactive defense distribution after enhancement

Table 4-6: Experimental Data

	Before enhance	After enhance
Compromised probability	0.734277	0.41527
No of nodes	25	27
Budget of topology	450000	449000
Budget of proactive defense	415500	124500
Budget of reactive defense	214500	506500

As you can see, proactive defense resource decreases a lot. It is because cloud security and virtual machine already can provide enough protection. We don’t need to put too much budget on proactive defense resource.

- Minimum cut

Now, we use the same topology, commanders, user and defender to run enhancement test. We use minimum cut to help us find which node should increase budget. Figure 4-9 shows the configuration after enhancement using minimum cut (with virtual start and end point) and Figure 4-10 show the configuration after enhancement also using minimum cut but without virtual start and end point directly using edge node as start point. The initial configuration is like Figure 4-5. Those circles represent nodes that are in the same virtual machine monitor group. Table 4-7 shows some experiment data.

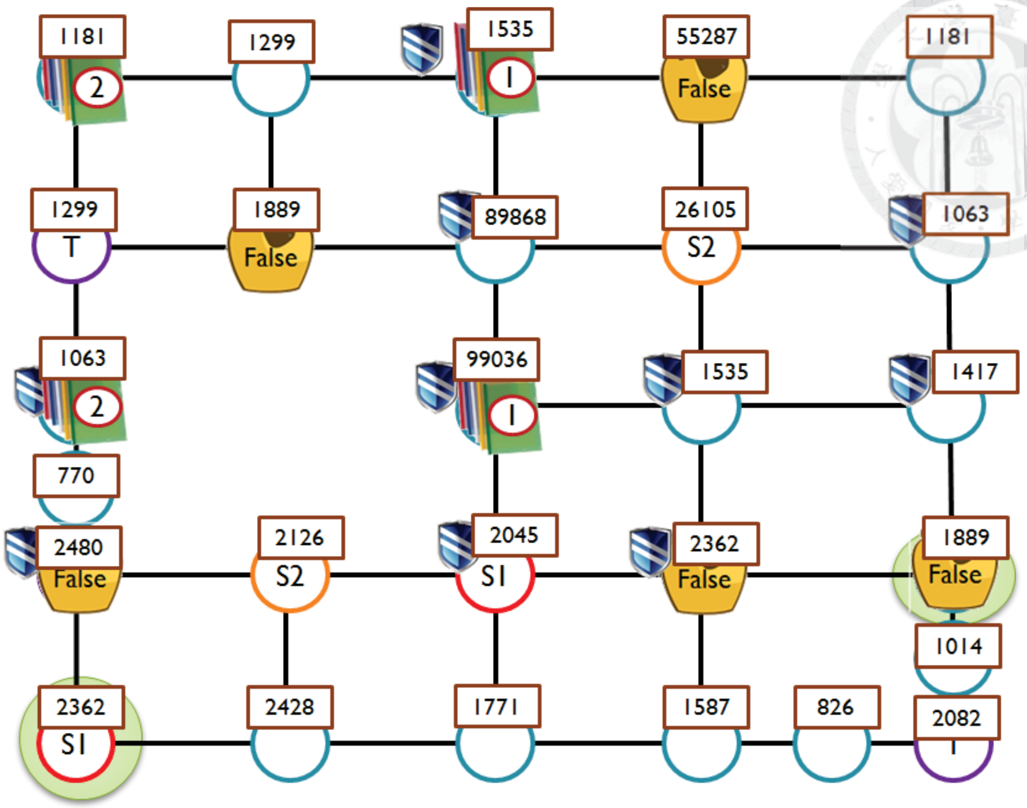


Figure 4-9: Configuration after enhancement (with virtual start and end point)

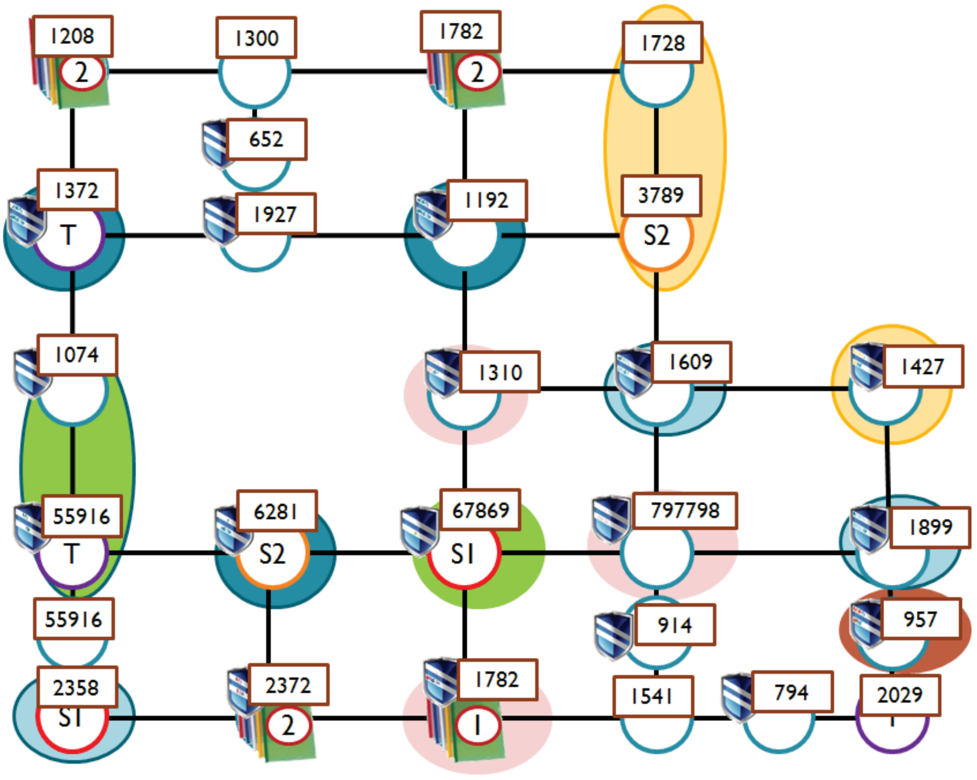


Figure 4-10: Configuration after enhancement (without virtual start and end point)

Table 4-7: Experiment data

	With virtual node	Without virtual node	Defense front
Compromised probability(before)	0.734530	0.738271	0.734277
Compromised probability(after)	0.454835	0.396389	0.41527
No of nodes	27	27	27
Budget of topology	455000	446000	449000
Budget of proactive defense	307500	245000	124500
Budget of reactive defense	317500	389000	506500
No of honeypot	5	0	8
No of virtual machine	2	16 (3,3,3,3,3,1)	6 (2,2,2)
No of redundancy	4 (2,2)	4(1,3)	4 (2,2)
No of cloud security agent	10	18	17

First, we see topology configuration. These two topologies are similar to previous one in Figure4-4. Still hold the principle of drawing the nodes that are close to seismic zone and add new nodes on the path to core nodes in order to consume attacker's budget and decrease the possibility of attacking core nodes.

The configuration of minimum cut with virtual node is similar with defense front. Both of them put some budget on deploying false target to cheat attackers. But configuration of defense front put more budget on constructing virtual machine and cloud security, using these two defense strategies to keep increase nodes' intensity. The other one choose to put more budget on proactive defense resource. But since this method (with virtual node) each service only choose one terminal node which has better performance and one core node to find minimum cut, so some place might be ignore since those nodes don't at the cut. It may be the reason why this configuration doesn't improve that much compares to defense front.

The configuration of minimum cut without virtual node totally use cloud security, virtual machine and proactive defense to strength system's intensity. Every core node belongs to one group and deploy virtual machine near edge node helping core node keep increase its intensity. It is also an efficient way to protect system.

4.3.2 Enhancement by definition of gradient

Now, we use the same commander, user, defender and topology to run the experiment of definition of gradient. We use grid topology with 25 nodes and use minimum cut without virtual node as the increasing method. Figure 4-10 shows the configuration after enhancement and Table 4-7 shows some experiment data.

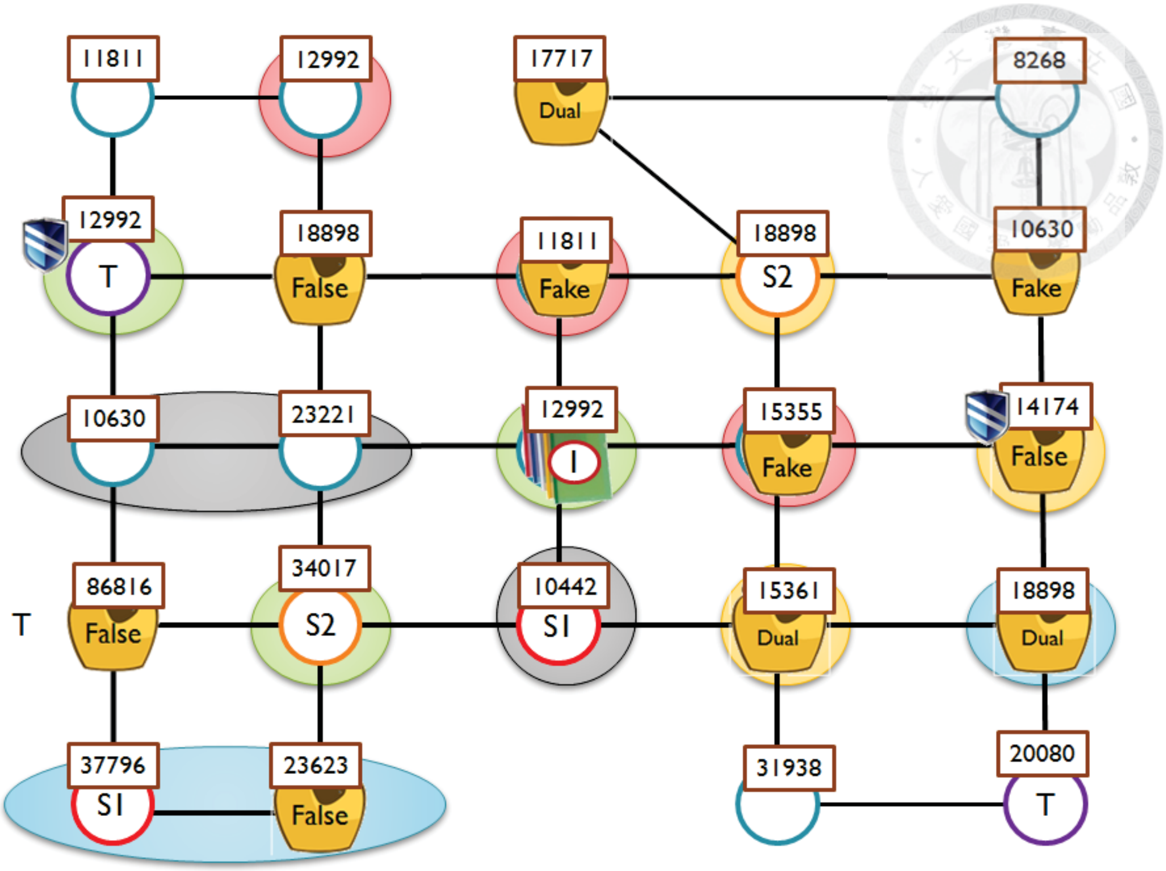


Figure 4-11: Configuration after enhancement by definition of gradient (using minimum cut and without virtual node)

Table 4-7: Experiment data (minimum cut without virtual node)

	Definition by gradient	Local information estimate
Compromised probability(before)	0.733321	0.738271
Compromised probability(after)	0.394301	0.396389
No of node	23	27
Budget of topology	412000	446000
Budget of proactive defense	479645	245000
Budget of reactive defense	185000	389000

No of honeypot	10	0
No of virtual machine	15(3,3,3,3,3)	16 (3,3,3,3,3,1)
No of redundancy	1	4(1,3)
No of cloud security agent	2	18

There are a lot of differences between two methods. They both use many virtual machines to strength their intensity. But in definition of gradient chooses to put more resource on proactive defense instead of using cloud security to strengthen the defense and use honeypot to cheat attackers in order to let attacker stop attacking. From those experiments, we can see using different method end up with different configuration and all of them all help us improve system survivability.

Chapter 5 Conclusion and Future Work

When dealing with cyber-attack and natural disaster, defender needs to strengthen their defense in order to increase system's survivability. In our scenario, we provide several defense strategies to help defender against to malicious attack and natural disaster. Our purpose is to help defender find out effective defense strategy and resource allocation to optimize survivability of network. This problem is a bi-level problem. Commander would try to maximize their compromised probability by adjusting their attack strategies and defender will try to minimize compromised probability by finding out suitable resource combination. This complex problem, we use mathematical programming combined Monte Carlo Stimulation to help us solve this problem since there are various of attack and defense strategies and full of uncertainty. Furthermore, we use two enhancement methods (Local Information Estimate and Definition by Gradient) to help us keep improving the result. In the enhancement process, we adopt two ideas to help us find out better solution which are Defense Front and Minimum Cut. From the experiments that we do can see it actually improves a lot. In addition, even though using different configuration as long as its allocation is appropriate and match properly, all of them can help defender well against attackers.

In future research, we will expand the defense mechanisms adopting new defense strategies in our scenario. Besides, we will keep trying other enhancement methods or rules in order to find out the optimal solution.

Reference

[1]Symantec, "*2011 State of Security Survey*", 2011. http://www.symantec.com/content/en/us/about/media/pdfs/symc_state_of_security_2011.pdf

[2] "*2012 Cost of Cyber Crime Study: United Kingdom*", Ponemon Institute October 2012. http://docs.media.bitpipe.com/io_10x/io_102267/item_575599/2012%20UK%20Cost%20of%20Cyber%20Crime%20Study%20FINAL%204.pdf

[3] "*PlayStation Hackers May Have Stolen Data on 75 Million Users, Sony Says*", Cliff Edwards and Pavel Alpeyev, Apr 27, 2011. http://www.bloomberg.com/news/2011-04-26/sony-says-network-hackers-may-have-stolen-users-personal-data.html

[4] "*McAfee Threats Report: First Quarter 2012*", McAfee Lab Technical report, 2011.

[5] IBM Internet Security Systems X-Force research and development team, "*IBM X-Force® 2012 Mid-Year Trend and Risk Report*", IBM, September 2012. http://public.dhe.ibm.com/common/ssi/ecm/en/wgl03014usen/WGL03014USEN.PDF

[6] "*2012 Global Security Report*", Trustwave, 2012

[7] R. Richardson, "*2010 CSI Computer Crime and Security Survey*," Computer Security Institute, December 2010

[8] UNESCAP, UNISDR "*The Asia-Pacific Disaster Report 2010*", The UN Office for Disaster Risk Reduction (UNISDR) and the UN Economic and Social Commission for Asia and the Pacific (ESCAP), October 2010

[9] UNESCAP, UNISDR "*The Asia-Pacific Disaster Report 2012*", The UN Office for Disaster Risk Reduction (UNISDR) and the UN Economic and Social Commission for Asia and the Pacific (ESCAP), October 2012

[10] S. Xu, "*Collaborative Attack vs. Collaborative Defense*," Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2009, Volume 10, Part 2, 217-228, 2009.

[11] F. Cohen, “*Managing Network Security: Attack and Defence Strategies,”* Network Security, Volume 1999, Issue 7, pp. 7-11, July 1999.

[12] R. J. Ellison, D. A. Fisher, R.C. Linger, H. F. Lipson, T. Longstaff and N. R. Mead, “*Survivable Network Systems: An Emerging Discipline*,” Technical Report CMU/SEI-97-TR-013, Novermber 1997.

[13] H.F. Lipson, N.R. Mead, and R.C. Linger, “*Requirements Definition for Survivable Network Systems*,” Proceedings of the 3rd International Conference on Requirements Engineering, pp. 14-23, April 1998.

[14] N.R. Mead, “*Panel: Issues in Software Engineering for Survivable Systems*,” ACM Proceedings of the 21st International Conference on Software Engineering, pp. 592-593, May 1999.

[15] D. Medhi and D. Tipper, “*Multi-layered Network Survivability-models, Analysis, Architecture, Framework and Implementation: An Overview*,” Proceedings of DARPA Information Survivability Conference and Exposition 2000 (DISCEX’00), Volume 1, pp. 173-186, January 2000.

[16] A.P. Moore and R.C. Linger, “*Foundations for Survivable System Development: Service Traces, Intrusion Traces, and Evaluation Models*,” Technical Report CMU/SEI-2001-TR-029, October 2001.

[17] V.R. Westmark, “*A Definition for Information System Survivability*,” Proceedings of the 37th IEEE Hawaii International Conference on System Sciences, pp. 10, January 2004.

[18] A. Snow, G. Weckman, and P. Rastogi, “*Assessing Dependability of Wireless Networks Using Neural Networks*,” IEEE Military Communications Conference, 2005 (MILCOM’05), Vol. 5, pp. 2809-2815, October 2005.

[19] D. Tipper, K. Lu, and Y. Qian, “*A Design fo Secure and Survivable Wireless Sensor Networks*,” IEEE Wireless Communications, Vol. 14, Issue 5, pp. 30-37, October 2007.

[20] A.W. Krings and Z. Ma, “*Survival Analysis Approach to Reliability, Survivability and Prognostics and Health Management (PHM)*,” IEEE Aerospace Conference 2008, pp. 1-20, March 2008.

[21] P. E. Heegaard and K. S. Trivedi, "*Network Survivability Modeling*," Computer Networks, vol. 53, pp. 1215-1234, 2009.

[22] J.Huang, J.Jiang and L. Zhang, "*A Novel Transient System Survivability Quantitative Evaluation Framework*," Computer Engineering and Applications (ICCEA), 2010 Second International Conference on, pp. 34-39, 2010.

[23] S.Braynov and M.Jadiwala, “*Representation and Analysis of Coordinated Attacks*,” Proceedings of the 2003 ACM workshop on Formal methods in security engineering, pp. 43-51, October, 2003.

[24] Debby Guha-Sapir, Femke Vos, Regina Below and Sylvain Ponserre, “A*nnual Disaster Statistical Review 2011- the numbers and trends*”, United States Agency for International Development (USAID), 2012

[25] Jiang-Hua Zhang, Jin Li, Zhi-Ping Liu, “*Multiple-resource and multiple-depot emergency response problem considering secondary disasters*”, Expert Systems with Applications An International Journal, 2012

[26] “*Developing a Physics-based Model for Post-Earthquake Ignitions*”, Proceedings of the 9th International ISCRAM Conference – Vancouver, Canada, April 2012

[27] Fire and Disaster Management Agency in Japan. http://www.fdma.go.jp/

[28] California. State Earthquake Investigation Commission, “*Lawson, Andrew C, The California Earthquake of April 18, 1906. Report of the State Earthquake Investigation Commission, Carnegie Institution of Washington，1906*”, Washington, D.C., Carnegie Institution of Washington,1910

[29] U.S. Fire Administration, “*U.S. Fire Administration Fire Estimates*”, 2010, http://www.usfa.fema.gov/statistics/estimates/index.shtm

[30] B. B.M. Shao (2005). “*Optimal Redundancy Allocation for Information Technology Disaster Recovery in the Network Economy*”. IEEE Transactions on Dependable and Secure Computing, 2(3), 262-267.

[31] O. Tannous , L. Xing, P. Rui , M. Xie, S.H, Ng, “*Redundancy Allocation for Series-Parallel Warm-Standby Systems*”, 2011 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), 6-9 Dec.2011, page 1261-1265

[32] Gutenberg, R., and C.F. Richter, (1944). "*Frequency of earthquakes in California*", Bulletin of the Seismological Society of America, 34, 185-188.

[33] Yin Myo Min Htwe, Shen WenBin, "*Gutenberg-Richter Recurrence Law to Seismicity Analysis of Southern Segment of the Sagaing Fault and Its Associate Components*", World Academy of Science, Engineering and Technology 26, 2009.

[34] U.S. Fire Administration/National Fire Data Center, "*Fire in the United States 2003-2007*", FEMA, Fifteenth Edition, October 2009

[35] Michael J. Karter, Jr., "*Fire Loss in the United States during 2011*", National Fire Protection Association Fire Analysis and Research Division, September 2012

[36] Fandel, G., et al., "*Measuring synergy effects of a Public Social Private Partnership (PSPP) project*", International Journal of Production Economics, 2012

[37] Xuemei Zhang , Hoang Pham and Carolyn R. Johnson, "*Reliability models for systems with internal and external redundancy*", International Journal of System Assurance Engineering and Management, December 2010, Volume 1, Issue 4, pp 362-369

[38] Ola Tannous, Liudong Xing and Joanne Bechta Dugan, "*Reliability Analysis of Warm Standby Systems using Sequential BDD*", 2011 Proceedings - Annual Reliability and Maintainability Symposium (RAMS), 24-27 Jan. 2011, page 1-7

[39] Jannik Laval, Simon Denier, Stéphane Ducasse, Jean-Rémy Falleri, "*Supporting simultaneous versions for software evolution assessment*", Journal of Science of Computer Programming ,2010

[40] S. Skaperdas, "*Contest success functions*," Economic Theory, vol. 7, pp. 283-290, 1996.

[41] R Peng, G Levitin, M Xie and SH Ng, "*Optimal defence of single object with imperfect false targets*", Journal of the Operational Research Society (2011), page 134 –141

[42] Rui Peng, Wenbin Wang, Fei Zhao, "*Object Defense Strategy With Imperfect False Targets and Disinformation*", 2012 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE), 15-18 June 2012, page 59-62

[43] K. Hausken and G. Levitin, "*Protection vs. false targets in series systems*", Reliability Engineering & System Safety, vol. 94, pp. 973-981, 2009.

[44] M.H. Kalos and P.A. Whitlock, “*Monte Carlo Methods,*” John Wilet & Sons Incs, ISBN 978-3-527-40760-6, November 2008.

[45] Central Weather Bureau, Taiwan, http://www.cwb.gov.tw

[46] S. Nagaraja and R. Anderson, “Dynamic Topologies for Robust Scale-Free Networks,” Bio-Inspired Computing and Communication, Volume 5151, pp. 411-426, 2008.

[47] J. Blitzstein and P. Diaconis, “A Sequential Importance Sampling Algorithm for Generating Random Graphs with Prescribed Degrees,” Internet Mathematics, Volume 6, pp. 489-522, March 2011.