國立臺灣大學管理學院資訊管理研究所

碩士論文

Graduate Institute of Information Management

College of Management

National Taiwan University

Master Thesis

考量不完全資訊情況下多階段防禦資源分配以及防禦訊息策略選擇演算法以最大化網路存活度

Maximization of Multi-Round Network Survivability under Considerations of Defensive Messaging Strategies and Incomplete Information for Both the Attacker and the Defender

施怡如

I-Ju Shih

指導教授：林永松 博士

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

中華民國 101 年 7 月

July 2012

國立臺灣大學碩士學位論文
口試委員會審定書

考量不完全資訊情況下多階段防禦資源分配以及防禦訊息策略選擇演算法以最大化網路存活度

本論文係施怡如君（學號 R99725003）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 101 年 7 月 25 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	
鍾惠平	

所　　長：

致謝

轉眼之間，兩年的碩士生涯即將結束，這兩年來要感謝的人很多，因為有你們，我才能完成這篇論文。感謝我的父親-施欽章先生和母親曹秀玉女士，因為有您們無怨無悔的付出與支持，我才能無憂無慮的成長至今。

在就讀碩士學位的這兩年裡，最感謝的是我的老師-林永松博士。在學術研究上，老師總是能夠指出我們的盲點，並給予建議，真的很感謝老師這兩年的教誨，因為有您，我才能順利完成這篇論文。另外，還要感謝輔仁大學資工系的呂俊賢教授、高雄第一科技大學行銷與流通管理系的傅新彬教授、台北大學資工系的莊東穎教授以及台灣科技大學電機系的鍾順平教授，感謝您們在口試時提出許多寶貴的建議，相信將會使此篇論文更為完善，並更具學術意義。

此外，還要感謝實驗室的明宗學長、霈語學姐與猷順學長，每當我遇到問題時，您們總是會幫助我，也謝謝您們給予我許多關於論文撰寫上的建議。同窗好友-瀅如、蕙宇、育溥以及榮翔和學弟妹-佳玲、聿軒與端駿，謝謝你們幫助我解決許多的困難，也謝謝你們陪我度過這一段美好的時光。

施怡如　謹識

民國一〇一年八月

于台灣大學資訊管理研究所

論文摘要

論文題目：考量不完全資訊情況下多階段防禦資源分配以及防禦訊息策略選擇演算法以最大化網路存活度

作者：施怡如

指導教授： 林永松 博士

隨著網際網路的快速發展，我們隨時隨地都可以連上網路，網路帶來了許多商機，但也讓企業面對許多的挑戰。企業為了 24 小時都能服務顧客，它必須保持不間斷的系統服務，但是隨著網路攻擊工具包的取得越來越容易，網路攻擊不再是駭客的專利，讓企業面臨許多資訊安全的問題。因此，如何分配防禦資源以有效的減少攻擊者所帶來的傷害，以及如何評估系統存活度以幫助企業保持營運就成為了重要的議題。

在我們的攻防情境中，我們考慮攻防雙方並不完全了解對方擁有的資訊，也就是考慮不完全資訊，並建立一個最佳化資源配置目標之數學模型，且利用一個網路存活度的指標平均網路分割度(Average Degree of Disconnectivity)來衡量在多階段攻防情境下的網路存活度，以提供網路營運者預測攻防雙方可能採取的資源分配策略。在此情境的每一個階段裡，防禦者需要分配資源在不同的節點上，透過重新分配或回收資源做更好的防禦資源利用，使用防禦資源修復已被攻克的節點，以及修補漏洞或是利用滲透測試修補漏洞，另外防禦者還可以選擇是否要釋放訊息，其訊息可能為真實、欺騙或是保密的訊息來混淆攻擊者，藉此達到更好的防禦效率;而攻擊者則會利用資源對網路中的節點進行攻擊。在求解的過程中，我們採用「梯度法」與「賽局」技巧來協助找出攻防雙方最佳的資源分配策略。

關鍵字：平均網路分割度、梯度法、賽局理論、不完全資訊、存活度、最佳化、資源分配、多階段、網路修復、滲透測試

THESIS ABSTRACT

THESIS TITLE： Maximization of Multi-Round Network Survivability under Considerations of Defensive Messaging Strategies and Incomplete Information for Both the Attacker and the Defender

NAME：I-Ju Shih

ADVISOR：Yeong-Sung Lin, Ph.D.

With Internet rapidly expanding, we can connect to Internet at anytime in anywhere. Internet brings many businesses for enterprises, but Internet also lets enterprises face many challenges. In order to serve their customers at all day, enterprises should keep operation continuously. With attack toolkits become easily to obtain, cyber attacks are not hackers' specialization. So, enterprises face many challenges of cyber security. Therefore, how to efficiently allocate defensive resources to reduce damages which was caused by cyber attackers and how to evaluate system survivability to help enterprises keeping operate became important issues.

In this multi-round attack-defense model, both cyber attacker and network defender without completely understanding the information about each other is considered. In other words, incomplete information in this model is considered and we

conduct a mathematical model for this problem. Besides, we use Average DOD to evaluate damage degree of network to help network operators to predict all possible strategies which both cyber attacker and network defender would take. In each round, network defender could allocate resources on each node, reallocate or recycle resources for better use. And network defender could also repair compromised nodes, patch system vulnerabilities or use penetration test to patch system vulnerabilities. Moreover, network defender could release message which might be doing nothing at all, truth, secrecy or deception to confuse cyber attacker to achieve better defense efficiency. In each round, cyber attacker would allocate resources to attack nodes of the network. In the process of problem solving, the "gradient method" and "game theory" would be used to obtain the optimal resource allocation strategies for both cyber attacker and network defender.

Keyword: Average Degree of Disconnectivity, Average DOD, Gradient Method, Game Theory, Incomplete Information, Survivability, Optimization, Resource Allocation, Multi-round, Network Recovery, Penetration Test

Table of Contents

List of Figures

List of Tables

Chapter 1 Introduction

1.1 Background

In recent years, the Internet becomes a part of our lives with the applications of Internet expanding rapidly and universally. No matter what devices (e.g., computers, PDAs, smart phones, etc.) we use to connect to the Internet, we can browse websites any time. This makes enterprises integrating many applications in one platform to provide more convenient and faster services. However, the functions and complexity of these applications increase continuously. Enterprises face many challenges with more and more potential system vulnerabilities and threats.

Cyber attacks are not always launched by hackers, because it is easy to get attack toolkit from Internet. According to Symantec report on attack kits and malicious websites [1], the Web-based threat activity detected by Symantec during this reporting period, 61 percent is specific to attack kits (Figure 1-1). Attack kits let cyber attackers do not having a lot of professional knowledge, which decreases the threshold of cyber attacks. Moreover, the generality of Internet allows cyber attackers to launch attacks easily in the whole world. Therefore, a person could launch large-scale attack crime

even if he was not a professional hacker.

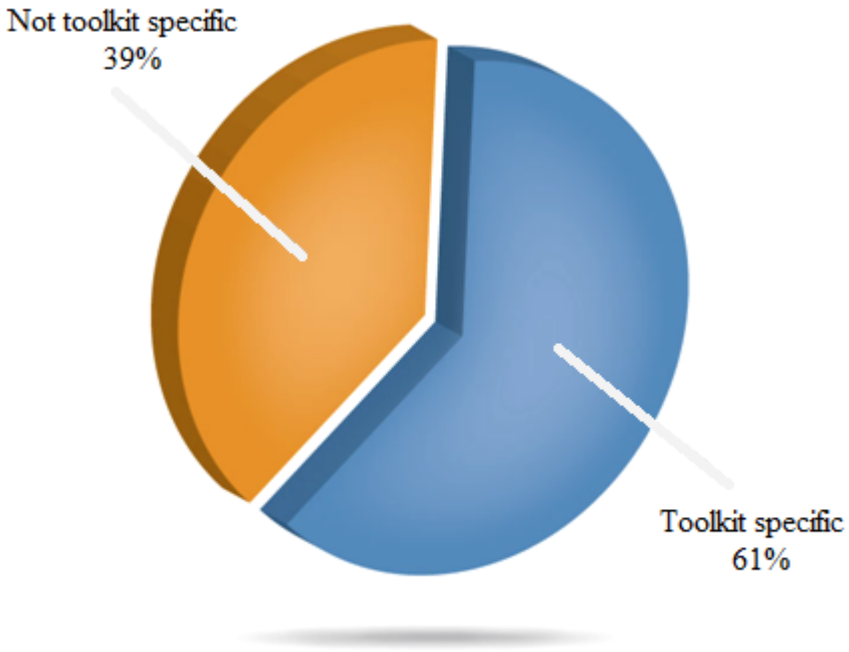


Figure 1-1 : Percentage of threat activity on malicious websites, by toolkit specificity [1]

According to 2010 / 2011 CSI (Computer Security Institute) computer crime and security survey [2], the most three common attacks were malware infection (67.1%), phishing fraud (38.9%) and laptop or mobile device theft (33.5%). Moreover, we can also find that there are increasing rapidly in malware infection, phishing fraud and bots on network, as shown in Figure 1-2. Table 1-1 shows more details.

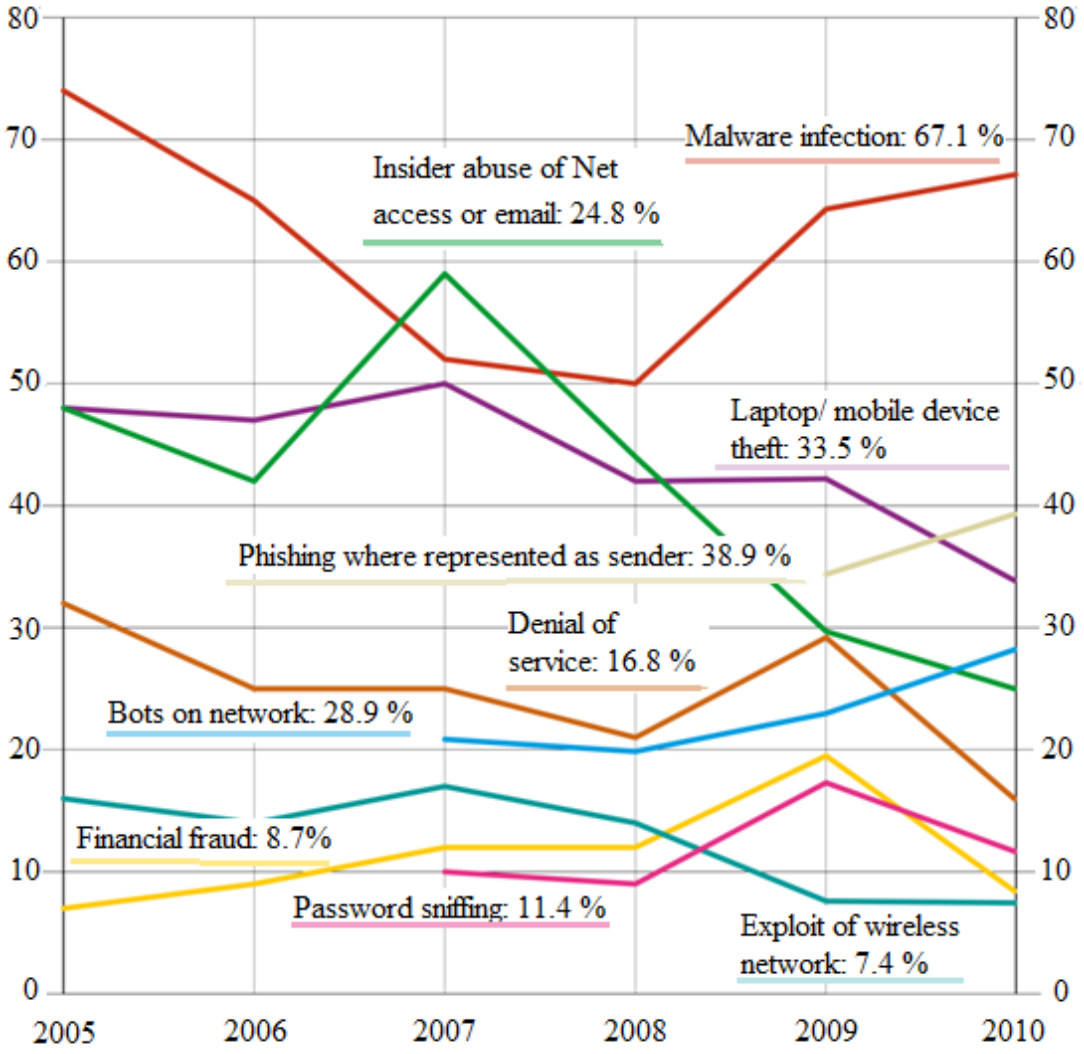


Figure 1-2 : Types of attacks experienced by percent of respondents [2]

Table 1-1 : Types of attacks experienced by percent of respondents [2]

Type of attack	2005	2006	2007	2008	2009	2010
Malware infection	74%	65%	52%	50%	**64%**	**67%**
Bots / zombies within the organization	added in 2007		21%	20%	**23%**	**29%**
Being fraudulently represented as sender of	added in		26%	31%	**34%**	**39%**

phishing messages	2007					
Password sniffing	added in 2007		10%	9%	**17%**	**12%**
Financial fraud	7%	9%	12%	12%	**20%**	**9%**
Denial of service	32%	25%	25%	21%	**29%**	**17%**
Extortion or blackmail associated with threat of attack or release of stolen data	option added in 2009				**3%**	**1%**
Web site defacement	5%	6%	10%	6%	**14%**	**7%**
Other exploit of public-facing Web site	option altered in 2009				**6%**	**7%**
Exploit of wireless network	16%	14%	17%	14%	**8%**	**7%**
Exploit of DNS server	added in 2007		6%	8%	**7%**	**2%**
Exploit of client Web browser	option added in 2009				**11%**	**10%**
Exploit of user's social network profile	option added in 2009				**7%**	**5%**
Instant messaging abuse	added in 2007		25%	21%	**8%**	**5%**
Insider abuse of Internet access or e-mail (i.e. pornography, pirated software, etc.)	48%	42%	59%	44%	**30%**	**25%**
Unauthorized access or privilege escalation by insider	option altered in 2009				**15%**	**13%**
System penetration by outsider	option altered in 2009				**14%**	**11%**
Laptop or mobile hardware theft or loss	48%	47%	50%	42%	**42%**	**34%**
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss	option added in 2008			8%	**6%**	**5%**

Theft of or unauthorized access to intellectual property due to mobile device theft/loss	option added in 2008	4%	**6%**	**5%**
Theft of or unauthorized access to PII or PHI due to all other causes	option added in 2008	8%	**10%**	**11%**
Theft of or unauthorized access to intellectual property due to all other causes	option added in 2008	5%	**8%**	**5%**
2010 CSI Computer Crime and Security Survey			**2010: 149 Respondents**	

According to Symantec internet security threat report trends for 2010 [3], the report indicated that the volume of web-based attacks per day increased gradually in 2010 compared with 2009, as shown in Figure 1-3.

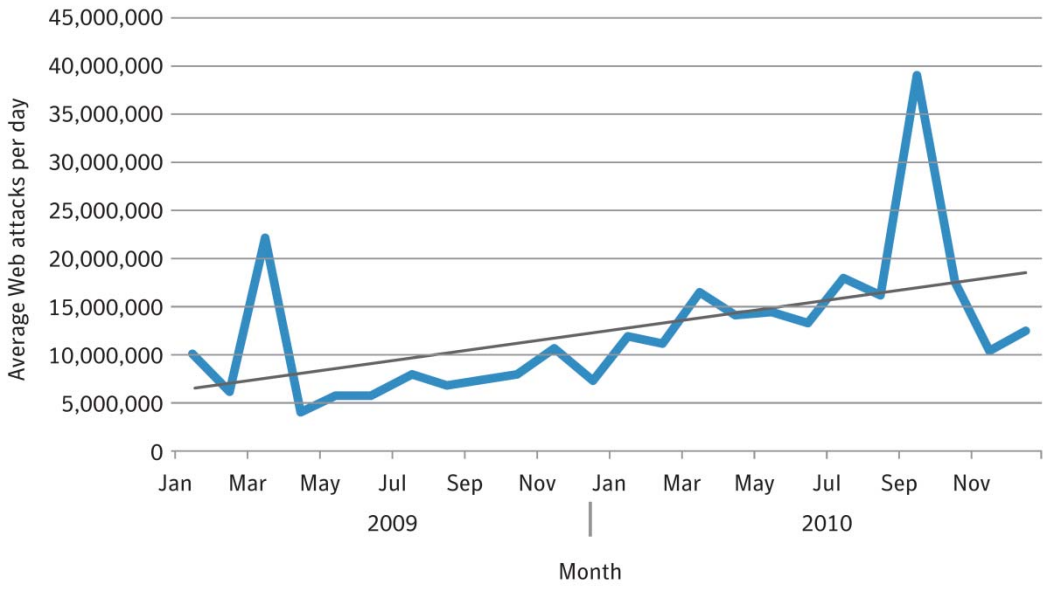


Figure 1-3 : Average web-based attacks per day, by month, 2009–2010 [3]

Though businesses today face more challenges about cyber attacks, they are also

concern about a variety of threats, including criminal activity, natural disasters and terrorism. However, according to 2011 Symantec state of security survey [4], businesses are most concern about the threat which was brought by cyber attackers, as shown in Figure 1-4.

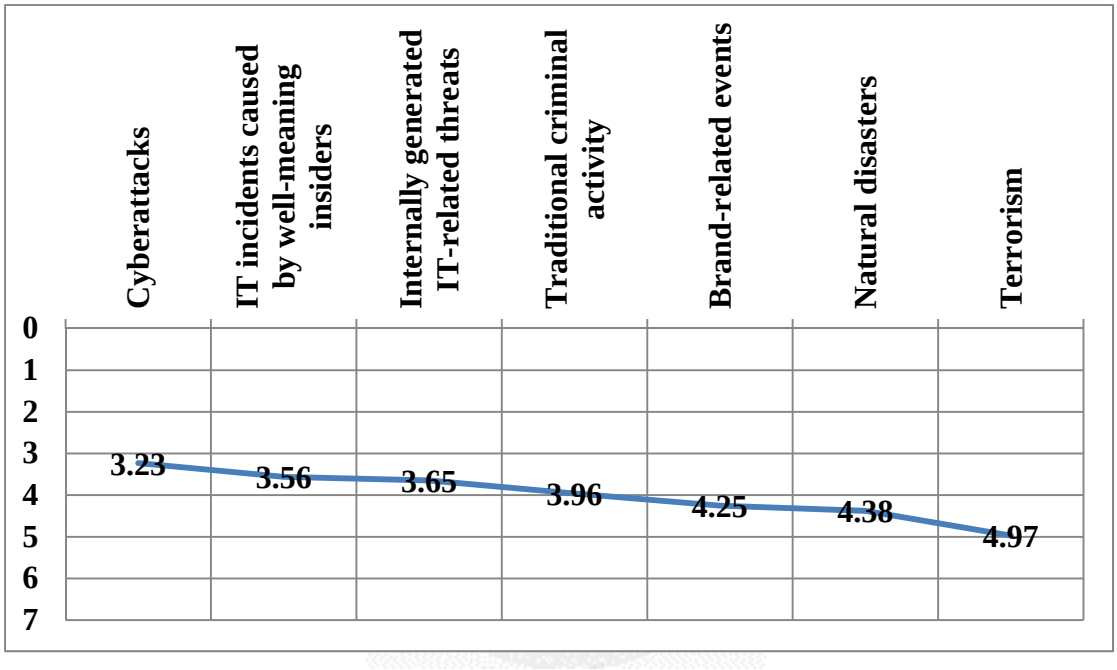


Figure 1-4 : The average ranks of business risks (1 being most significant, 7 being least significant) [4]

From the above statistics, we could observe that the Internet was full of many kinds of threats. The cyber attacks could let businesses suffer direct losses or indirect losses. The direct losses might be the drop in productivity or revenue. The indirect losses might be the loss of customer's trust or business's reputation. According to 2011

Symantec state of security survey [4], most of enterprises thought that the damage which was caused by cyber attackers was the loss of productivity and revenue, as shown in Figure 1-5.

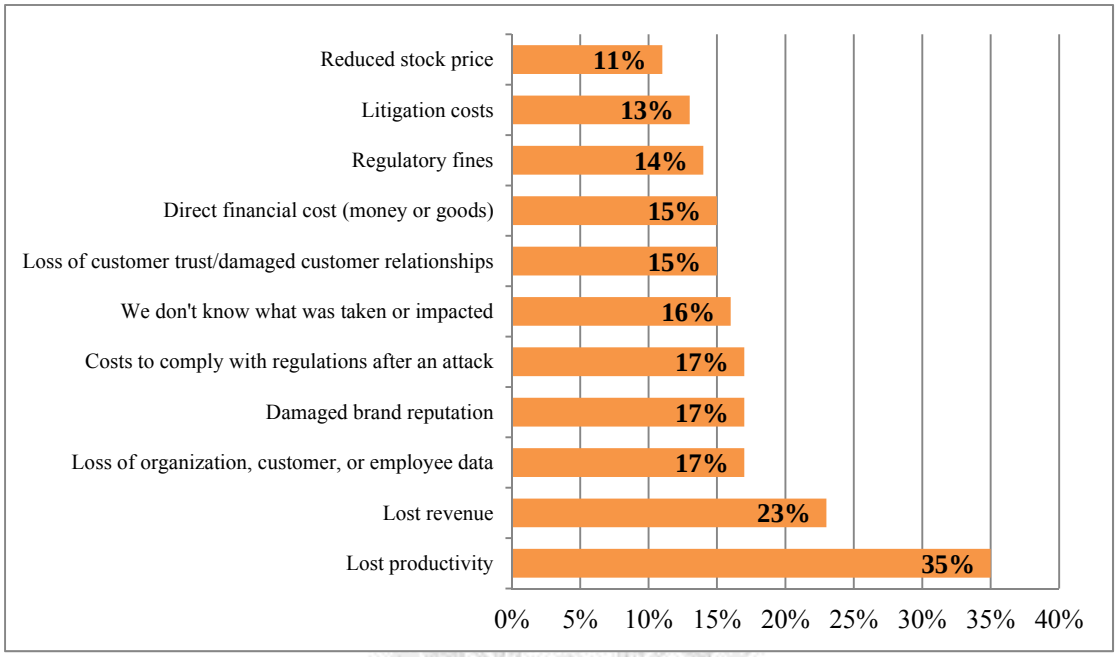


Figure 1-5 : Costs of cyber attacks [4]

Nowadays, globalization makes many enterprises have to serve their customers at all day. However, there are many attackers in the world which might attack enterprise's system resulting in unpredictable damage. In order to decrease the damage which was brought by cyber attackers, many enterprises are using business continuity management which could provide a framework to ensure the resilience of enterprises to any eventuality. Moreover, business continuity management could help enterprises ensure continuity of service to customers and the protection of reputation. In short,

business continuity management could provide a basis for planning to ensure enterprises the ability to continue operating following a disruptive event.

For example, in the terrorist attacks of September 11 both Twin Towers of the World Trade Center in New York City collapsed within two hours. After the attacks there were approximately 400 companies starting business continuity plan quickly. Morgan Stanley Company was one of these enterprises and it recovered all of its businesses within only 4 days. According to [5], this paper indicated that only 6 percent of companies suffering from a catastrophic data loss survive, while 43 percent never reopened and 51 percent closed within two years. From the instance of Morgan Stanley Company and [5] we could find that business continuity management was very important. Enterprises should normally use some metrics of survivability to help evaluate system in order to avoid attackers breaking down their operations. Therefore, there were more and more researchers studying the issue of how to optimally allocate resources to reduce damage which brought by attackers.

1.2 Motivation

Businesses believe that keeping their networks and information secure is the vital importance to their operations. When most of businesses maintain their systems, they

often hope that some existing approaches or models could help them to optimally allocate resources or effectively allocate resources. And these approaches or models could allow their system keeping operating when the attackers launched attacks.

In the past, most literatures of resource allocation considered the cyber attacker knowing complete information about the defender. Therefore, the results of these literatures recommended that the defender should truthfully disclose his defense to the attacker [6] [7] [8]. These literatures considered that defensive strategy disclosure could deter the attacker to attack or shift attacks to less valuable targets.

In reality, the attacker owns information which is often limited. It is impossible for the attacker to know the whole information about the defender. When the defender has private information, he can manipulate his private information to use some tricks. Hence, there are some researchers studying the situation with incomplete information [9].

The strategic interaction between cyber attacker and the defender should not be only one-round. In general, cyber attacker and the defender interact repeatedly. So, the interactions must be multi-round. For example, the attacker might probe the system before he attacked the system. Therefore, how to optimally allocate limited resources in multiple rounds becomes an important issue.

Because there are many attackers in the world and the interactions between attackers and defenders are repeated. In order to achieve business continuity, enterprises should use some metrics of survivability to help evaluate system robustness. So, how to evaluate the network survivability was important thing for network security professionals. The concept of the network survivability is gradually applied to evaluate the degree of the network security. Network survivability could be used to describe the ability of providing service when the system suffered attacks. In [10], this paper considered a model which is the attacker using the smallest cost to minimize the network survivability and the attacker could accumulate experiences. Therefore, the defender how to allocate resources to achieve maximal network survivability became an important issue.

Most models in past literature only considered simple system configuration, such as series or parallel [11], [12]. With the progression of technology everyone could use the Internet anytime. E-commerce became a part of businesses' operation, so businesses had to keep their e-commerce service running. In order to keep service not stopping, businesses would conduct high availability system for equipment. High availability system could ensure the service which would not be interrupted and could increase system survivability.

Motivated by above-mentioned literatures, a defender having private information in an attack-defense model is considered. The defender's objective is minimizing network survivability. Moreover, the model is a multi-round resource allocation problem. Resources reallocation, resources recycle, node recovery and vulnerabilities patches problem would also be considered in each round. More details would be further discussed in chapter 2.

1.3 Literature Survey

In this section, the definition of incomplete information would be introduced in the first part. And then the concept of multi-round and high availability would also be discussed in the second and third part, respectively. Finally, the conception of metric of the network survivability which was called the Average Degree of Disconnectivity (ADOD) would also be introduced in the final section.

1.3.1 Incomplete Information

Incomplete information meant that the information between competitors under the same competition was not always symmetric, that is, there possibly occurring asymmetry of information in a competition. For example, assuming a defender has private information, and the more details are shown in Figure 1-6. Figure 1-6 represent

the defender-owned information including the defender's private information which the attacker doesn't know, common knowledge which is known to both, and the defender unknowing information. The solid double arrow represents the defender's understanding information and the dashed double arrow represents an attacker's understanding information. As shown in Figure 1-6, the attacker does not know the defender's private information. But the attacker may know some information the defender does not know (e.g., system vulnerabilities, etc.). So, we can find that the information between the attacker and the defender in the same contest in Figure 1-6 is not symmetric and the contest is an incomplete information contest.

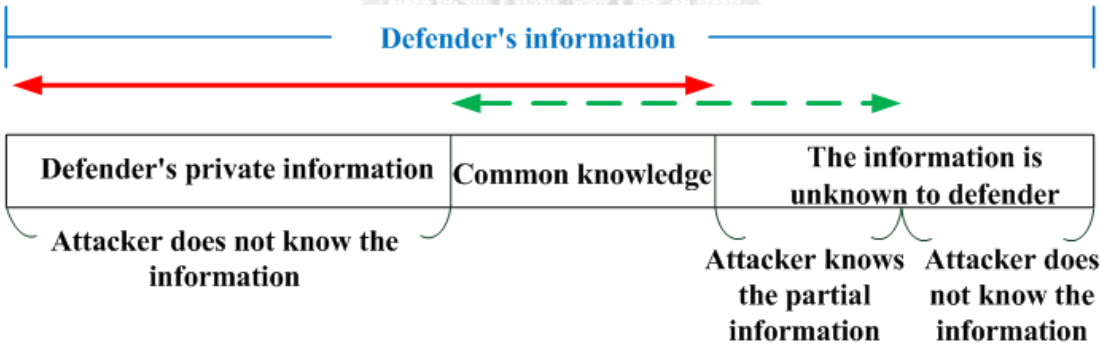


Figure 1-6 : An example of a defender's information

In the past, most literatures indicated that truthful disclosure of defense should often be preferred to secrecy [6] [7] [8]. Because publicizing defensive information could deter attackers to launch attacks. Moreover, most literature indicated that truthful disclosure could shift attacks to less valuable targets or allow the defender to have

first-mover advantage [13].

The results of above-mentioned literatures were all recommending a defender to disclose his defensive information, because these literatures' models were assumed having complete information. However, this assumption was not reasonable in reality. It is impossible for a defender to know all information about cyber attacker such as the number of the attacker's resources or attack efficiency. Similarly, it is impossible for an attacker to know all information about a defender such as the defender's defense or defense efficiency.

Intuitively, publicizing defensive information might decrease the efficiency of defense. For example, the disclosure of defense could attract more attacks to attack or increase attack success probability. Because the disclosure could let an attacker easily avoid or overcome the defense.

Traditionally, security-related information such as defensive resource allocations was often keeping secret. Using secret technique could avoid attackers getting more information about a defender, and let the defender feeling more security than disclosure. Moreover, deceptive technique was often used in military field. Therefore, there are more and more researchers to start studying the issue of incomplete information of interactions between attackers and defenders.

In [14], this paper demonstrated that secrecy or deception was preferred to truthful disclosure for the defender with private information. Though this model considered incomplete information, the defender only had one asset. It was not reasonable in reality. In fact, there were many assets such as web servers, email servers, file servers or database in enterprises.

Besides, there are some papers considering incomplete information between the attacker and the defender [15] [16] [17]. But these papers only considered one-round. Actually, the defender and the attacker interacted repeatedly until one of the both gave up.

According to above-mentioned literatures, considering a model with incomplete information would be more general. Moreover, in [18], this paper examined the opportunities for deceptions in defense of computer systems from cyber attacks including honeypots, fake information, false delay, false error messages, and identity deception. In [19], this paper proposed a taxonomy of deception which was feasible for defense from cyber attacks. And [18] revised assessments of suitability on a scale of 1 (unsuitable) to 10 (suitable) in [19] as shown in Table 1-2. In this taxonomy, some deception methods were considered suitable for defense in cyberspace. Therefore, we thought using deception for defense in network would be reasonable and would reach

better defense efficiency.

Table 1-2 : A taxonomy of deception in network [18]

Deception method	Suitability in network	Example
Agent	4	Pretend to be a naïve user to entrap identity thieves
Object	7	Camouflage key targets or make them look unimportant, or disguise software as different software
Instrument	1	Do something in an unexpected way
Accompaniment	4	Induce attacker to download a Trojan horse
Experiencer	8	Secretly monitor attacker's activities
Direction	3	Transfer Trojan horses back to attacker
Location-from	2	Try to frighten attacker with false messages from authorities
Location-to	6	Transfer attack to a safer machines, like a honeypot
Frequency	7	Swamp attacker with messages or requests
Time-at	2	Associate false times with files
Time-from	1	Falsify file-creation times
Time-to	1	Falsify file-modification times
Time-through	8	Delay in processing commands
Cause	7	Lie that you cannot do something, or do something not asked for

Effect	9	Lie that a command succeeded
Purpose	8	Lie about reasons for asking for authorization data, like a password
Content	9	Plant disinformation, redefine executables, or give false file-type information
Material	3	"Emulate" hardware of a machine in software for increased safety
Measure	6	Send data too large or requests too hard back to the attacker
Value	7	Systematically misunderstand attacker commands
Supertype	5	Be a decoy site for the real site
Whole	2	Ask questions that include a few attacker-locating ones
Precondition	10	Give false excuses for being unable to do the attacker commands
Ability	6	Pretend to be an inept defender or have easy-to-subvert software

1.3.2 Multi-round

In the past, most literatures often considered the interaction between an attacker and a defender only one-round [20] [21].

In fact, an attacker and a defender would interact repeatedly. An attacker would collect information about a defender or probe systems before he launched attacks.

In [22] and [23], these papers considered a multi-round model, but [22] did not consider a situation which a defender could recover node in his network or patch vulnerabilities and [23] only considered one target.

Therefore, a multi-round model of attack and defense would more usual. In addition, most literature in economics and political science had applied game theory to multi-round interactions. The game theory could address multi-period problems where multiple players with different objective compete and interact with each other on the same system [24]. So, applying game theory to describe the interactions between an attacker and a defender was reasonable.

1.3.3 High Availability

Most past literatures considered models in which the nodes in the network topology were only one single point [11] [12]. In fact, most enterprises have to conduct backup for important nodes to provide against a rainy day. If a model only considered nodes with a single point, that would insufficient for real businesses.

Since the Internet has become essential to business operations, numbers of trades are accomplished through computer network. Customers want their systems, for example hospitals, airplanes or computers, to be ready to serve them at all times. Much

important data is usually stored in computers or other equipment. Moreover, enterprises may have web servers, email servers, file servers, FTP servers and database, etc. Therefore, protecting these data and systems to ensure regular operation is a critical issue for enterprises.

High availability (HA) is a system design approach and associated service implementation that ensure a prearranged level of operational performance would be met. High availability (HA) clusters operated by harnessing redundant computers or components in groups or clusters that provided continued service when system components failed. Moreover, using high availability (HA) clusters could increase system survivability. High availability (HA) clusters could sometimes be categorized into active/active and active/passive. Active/active means that two components operated together and distributed workload across these two components. For example, node *i* in Figure 1-7 has 6 servers and the workload is distributed across these six servers. When one server of node *i* failed, node *i* could still operate normally. Active/passive means that only one component operates and the other is redundancy when the active component failed the redundancy would take over. For example, node *j* in Figure 1-7 has 2 databases and one is a backup database. When the active database of node *j* failed, node *j* could still operate normally by the backup database. Generally

speaking, high availability (HA) cluster implementations attempted to build redundancy into a cluster to eliminate single point of failure.

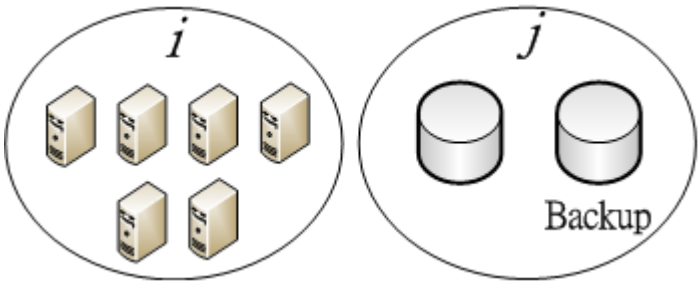


Figure 1-7 : High availability examples

In [25], targets could be in parallel, series, combined series-parallel, complex, k-out-of-n redundancy. In [26], this paper studied a model in which security investment decision-making was established (e.g., weakest-link, best-shot) and allowed expenditures in self-protection (e.g., patching system vulnerabilities) versus self-insurance (e.g., having good backups) technologies. However, these papers only considered the situation of one-round which was lack of reality.

Therefore, considering a high availability designed approach would be more general. Here, only the vital node of the topology would be applied the high availability designed.

1.3.4 Average Degree of Disconnectivity (ADOD)

In the past, the security state of systems or infrastructures was classified in terms of

two states: safe or compromised [27]. However, the network often faces many situations such as natural disasters, malicious attacks, and random error conditions which could result in different outcomes. Network security professionals must ensure the available and continuous services. Therefore, the binary concept is insufficient to describe a system's state. As a result, more and more researchers focus the issue of network survivability.

In [28], this paper proposed a new metric of the network survivability which was called the Degree of Disconnectivity (DOD). The DOD metric could be used to evaluate the damage degree of network. When the number of the DOD value was larger, the damage degree of network was bigger. The definition of the DOD was as below:

$$DOD = \frac{\sum \text{No. of broken nodes on the shortest path of each O-D pair}}{\text{No. of all OD pairs of a network}}$$

The calculated DOD value could be explained as measuring the average numbers of broken nodes in any O-D pair of network. Therefore, the DOD value could be effectively represented the damage degree of network. However, there was a disadvantage to this

metric. The DOD metric had assumed that the attacker would launch the attack either successfully or unsuccessfully. This assumption was limited, since the attack might not be 100% successful or unsuccessful.

In [29], the author proposed a new metric of the network survivability which was called average DOD. Average DOD combined the concept of probability calculated by the contest success function [30] with the DOD metric. The definition of contest success function was showed in the Table 1-3.

Table 1-3 : The Definition of Contest Success Function

Definition	***Notation***
$S_i(T_i, t_i) = \frac{{T_i}^m}{{T_i}^m + {t_i}^m} = \frac{1}{1 + \left(\frac{t_i}{T_i}\right)^m}$	$S_i(T_i, t_i)$：the attack success probability on node *i*
where $\frac{\partial S}{\partial T} \geq 0$, $\frac{\partial S}{\partial t} \geq 0$, $m \geq 0$	T_i ：the attack resource allocated on node *i*
	t_i ：the defensive resource allocated on node *i*

	m：contest intensity

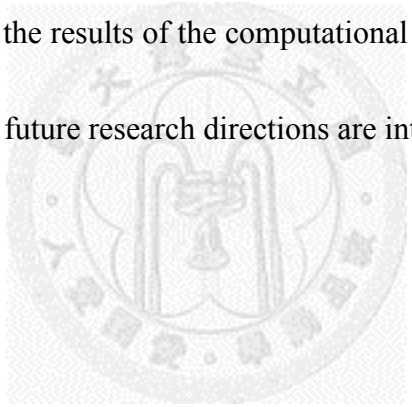
According to the definition of contest success function, if the attacker allocated more resource on a node, the more probability of the attacker could compromise the node. Similarly, if the defender allocated more resource on a node, the more probability of the defender could protect the node. Besides, m was a parameter which described the intensity of the contest [11]. When $m = 0$, no matter what sizes of T and t the attack success probability was 50%. When $0 < m < 1$, there was disproportional advantage of investing less than one's opponent. When $m = 1$, the investments had proportional impact on the success probability of attacker compromised the node. When $m > 1$, there was disproportional advantage of investing more than one's opponent. When $m > \infty$, the contest was winner-takes-all.

Average DOD used the concept of expectation value which combined the probability calculated by the contest success function [30] with the DOD value of each possible network configuration to evaluate damage degree of whole network. When the number of the ADOD value was larger, the damage degree of network was bigger. The calculated ADOD value could be explained as measuring the average damage degree of

network. Therefore, the ADOD value could be effectively represented the damage degree of network. And we would use Average DOD to help evaluating the network survivability.

1.4 Thesis Organization

The remainder of the thesis was organized as follows. In Chapter 2, the attack-defense scenario is described. In Chapter 3, solution approaches to the problem are presented. In Chapter 4, the results of the computational experiments are presented. Finally, the conclusions and future research directions are introduced in Chapter 5.



Chapter 2 Problem Formulation

2.1 Average Degree of Disconnectivity (ADOD)

The Average DOD, proposed in [29], is a metric of the network survivability which combined the concept of probability calculated by the contest success function [30] with the DOD metric. More details about the concept of Average DOD were described in the following sections.

2.1.1 Illustration

The concept of Average DOD and the method to calculate Average DOD value were introduced in this section. First, we would use some examples to show how to calculate the Average DOD value. If a network was like Figure 2-1, there were only 4 nodes in the network. Any two nodes of the network could form an O-D pair, so there were $C_2^4 = 6$ O-D pairs.

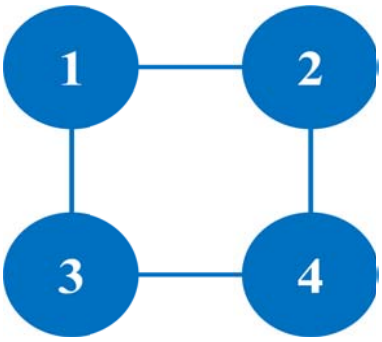


Figure 2-1 : An example of network

An attacker would allocate resources on nodes for compromising nodes, and a defender would allocate resources on nodes for defending and decreasing the damage bringing by the attacker as shown in Figure 2-2.

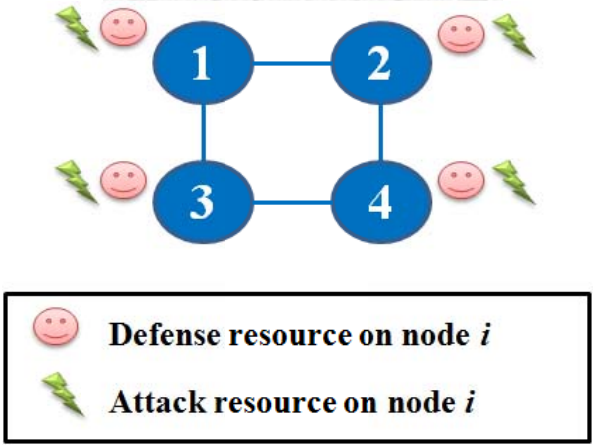


Figure 2-2 : An attacker and a defender's resource allocation on each node

According to the attacker and the defender allocating resources on nodes, we could calculate the attack success probability by contest success function for each node as shown in Figure 2-3, where S_i represented the attack success probability of node i .

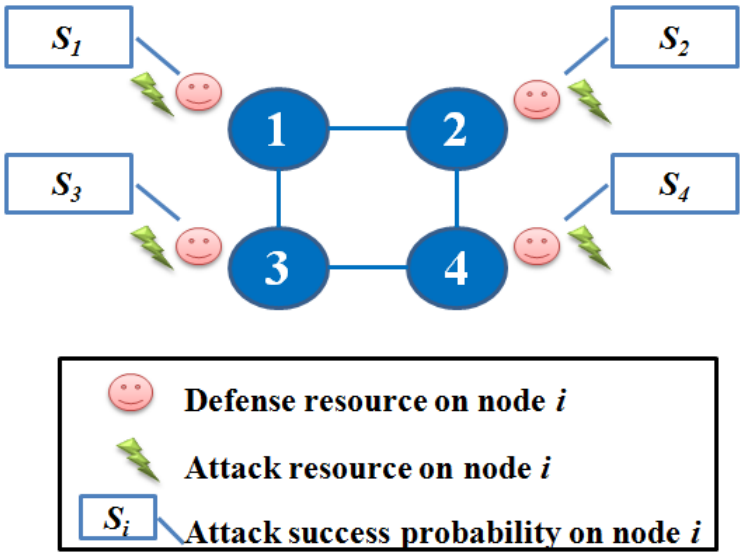


Figure 2-3 : The attack success probability of each node

The state of network configuration would be changed by the attacker if the attacker compromised nodes. Therefore, the probability of different states of network configuration was calculated by the product of the attack success or failure probability of each node. For example, in Figure 2-3 if all nodes were compromised by the attacker, the probability of the state of network configuration would be $\prod_{i=1}^{4} S_i$ (where S_i meant the attack success probability of the node *i*). If all nodes were functional, the probability of the state of network configuration would be

$\prod_{i=1}^{4}(1 - S_i)$ (where S_i meant the attack success probability of the node *i*).

Moreover, different states of network configuration would result in different damage degree of network. The Degree of Disconnectivity (DOD) which was

introduced in chapter 1 would be applied to measure the damage degree of network. For instance, in Figure 2-3 if all nodes were functional, the DOD value would be 0. If node 1 failed, the DOD value would be 3/6 = 1/2. Table 2-1 showed more details for calculating the DOD value when node 1 failed. The left column showed the route of different O-D pair and the numbers which were underlined represented the origin and the destination of the O-D pair. The right column showed the number of broken nodes of different O-D pair when node 1 failed. So, the DOD value would be the sum of all numbers in right column dividing by the number of O-D pairs in the network, that is, 3/6. Similarly, we could use the same way to calculate the DOD value of different states of network configuration.

Table 2-1 : The number of broken nodes for different O-D pair

(when node 1 failed)

route	number of broken nodes
1, **2**	1
1, **3**	1
1, 2, **4** (**1**, 3, **4**)	1
2, 4, **3** (**2**, 1, **3**)	0
2, **4**	0
3, **4**	0

After calculating the probability and DOD value of each possible state of network configuration, we could calculate the Average DOD value. Average DOD used the

concept of expectation value which combined the probability with the DOD value of each possible state of network configuration to evaluate damage degree of whole network. The more details about calculating Average DOD were shown in Table 2-2.

Table 2-2 : An example about calculating the average DOD value

No.	Network configuration (*i* means the node *i* is compromised)	Probability	DOD value	Probability * DOD value
1	1,2,3,4	$\prod_{i=1}^{4}(1-S_i)$	0	0
2	1,2,3,4	$S_1\prod_{i=2}^{4}(1-S_i)$	$\frac{3}{6}$	$S_1\prod_{i=2}^{4}(1-S_i)\times\frac{3}{6}$
3	1,2,3,4	$(1-S_1)S_2\prod_{i=3}^{4}(1-S_i)$	$\frac{3}{6}$	$(1-S_1)S_2\prod_{i=3}^{4}(1-S_i)\times\frac{3}{6}$

The total number of states of the network configuration was $2^4 = 16$.

16	1,2,3,4	$\prod_{i=1}^{4} S_i$	$\frac{14}{6}$	$\prod_{i=1}^{4} S_i \times \frac{14}{6}$
We could get the expectation value by calculating the sum of all values of last column (Probability*DOD value) and the expectation value was called as the **Average DOD**.				

When the number of the ADOD value was larger, the damage degree of network was bigger. Moreover, the average DOD value was affected by attack success probability which was calculated by an attacker and a defender's resource allocation. Therefore, the ADOD value could be effectively represented the damage degree of network. And we could use Average DOD to find optimal resource allocation on each node for both a defender and an attacker.

2.1.2 The Procedure of Calculating Average DOD

In preceding section, we introduced the concept of Average DOD and the method to calculate Average DOD value. Hence, this section would summarize the procedures of calculating Average DOD as blow:

Step 1. Finding out all possible states of network configuration. The total number of states would be 2 to the power of the number of nodes in the network.

Step 2. Calculating the probability of different states of network configuration. The probability of different states of network configuration was calculated by the product of the attack success or failure probability of each node.

Step 3. Using the DOD metric to evaluate the damage degree of network for each possible state of network configuration.

Step 4. Using the concept of expectation value which combined the probability with the DOD value for each possible state of network configuration to evaluate damage degree of whole network. The calculated expectation value is called the **Average DOD**.

2.2 Problem Description

In this model, there were only two players which were an attacker and a defender. We considered the defender determining strategy and choosing message which might

be truth, secrecy, deception or doing nothing at all to each node in each round. In the attack-defense scenario both a defender and an attacker have their respective objectives. Also, the defender and the attacker had to use some strategies to achieve their goals, respectively. From the defender's standpoint, the defender wanted to minimize the damage degree of network. From the attacker's standpoint, the attacker wanted to maximize the damage degree of network. Nevertheless, both the defender and the attacker were limited by finite resources. Therefore, both the defender and an attacker were concerned about the issue of how to optimally allocate resources on each node in different round. Hence, a mathematical model was developed to help both the defender and an attacker to optimally allocate resources on each node in different round.

It is impossible for a defender to know all information about cyber attacker in reality, and vice versa. So, incomplete information would be considered in this model. Moreover, the interaction between an attacker and a defender would not be only one round. Because in reality an attacker and a defender interact repeatedly such as the attacker collecting information about the defender or probing systems before the attacker launching attacks. So, we would consider multi-round in this model. Besides, nodes in the network are not always only one single point. In fact, most enterprises use the design approach of high availability to conduct redundancy for important nodes to

provide against a rainy day. So, we would consider high availability for network in this model. Furthermore, the Average DOD would be used in this model to evaluate the damage degree of network. The larger value of the Average DOD, the bigger damage degree of network would be.

Both a defender and an attacker would use some strategies to achieve their objectives. Hence, in the following section the attacker and the defender's characteristics would be introduced in the first part. And then two kinds of situations of message releasing and the defender's network topology would also be discussed in the second and third part, respectively.

2.2.1 The Attacker and the Defender's Characteristics

The defender's objective was minimizing Average DOD value, and the defender had resources constraints. The defender's resources would be used by the defender to deploy the defense budget on nodes, repair the compromised node, patch system vulnerabilities or release messages of each node. The attacker's objective was maximizing Average DOD value, and the attacker also had resources constraints. The attacker's resources would be used by the attacker to deploy the attack budget on nodes or update information of each node.

First, we introduced the defender's private information. When the defender had private information, he could manipulate his private information to use some tricks to increase defense efficiency. The defender's information as shown in Figure 2-4 included common knowledge, defender's private information and the defender's other information which was unknown to the defender such as system vulnerabilities. In Figure 2-4, the solid double arrow represented the defender knowing information. In defender's information, common knowledge was known to both the defender and the attacker. The defender had private information, including each node's type and network topology. In this thesis, we considered that there were two types (lower or higher valuation) of nodes and the prior belief of each node in the first round was common knowledge. The prior belief was the probability of a node belonging to higher valuation. When the valuation of node was bigger, the importance of the node was larger. Therefore, the attacker would allocate resources on nodes according to the importance of nodes that he thought. Nodes could be different type and different type's node could be used to shift attacks to unimportant nodes such as the nodes with lower valuation imitating the nodes with higher valuation. Moreover, the attacker could update the prior belief of the node's type by Bayes' theorem after the result of each round's contest [14]. As a result, the prior belief of the node's type in next round would

be

$$P'_{(r+1)i}(\delta_{ri}, P'_{ri}) = \begin{cases} \dfrac{P'_{ri} \times f_{ri}}{P'_{ri} \times f_{ri} + (1 - P'_{ri}) \times g_{ri}} & if\ \delta_{ri} = 1 \\ \dfrac{P'_{ri} \times (1 - f_{ri})}{P'_{ri} \times (1 - f_{ri}) + (1 - P'_{ri}) \times (1 - g_{ri})} & if\ \delta_{ri} = 0 \end{cases}$$

Table 2-3 : The parameter of prior belief

Notation	***Description***
P'_{ri}	The prior belief of node *i* belongs to the type of higher valuation in round *r*
δ_{ri}	1 if node *i* is compromised by attacker in round *r*, 0 otherwise
f_{ri}	When node *i* was the type of higher valuation, the attack success probability of node *i* in round *r*
g_{ri}	When node *i* was the type of lower valuation, the attack success probability of node *i* in round *r*

However, the attacker might know a part of the defender's private information,

which the defender did not know the attacker knowing his private information. Besides, the attacker might know some system vulnerabilities which were unknown to the defender. So, the dashed double arrow represented the attacker knowing information in Figure 2-4. For example, the attacker might know a part of network topology, which was the defender's partial private information. The attacker could only attack nodes of the network which had been known to the attacker and keep collecting information about the other nodes. For instance, if a defender's network topology was like Figure 2-5, an attacker only knew node *i* at first and the attacker could only attack node *i* at first. When the attacker attacked node *i*, he could know the existence of node *j* and node *m* in the defender's network topology and in the next time he could attack node *j* and node *m*.

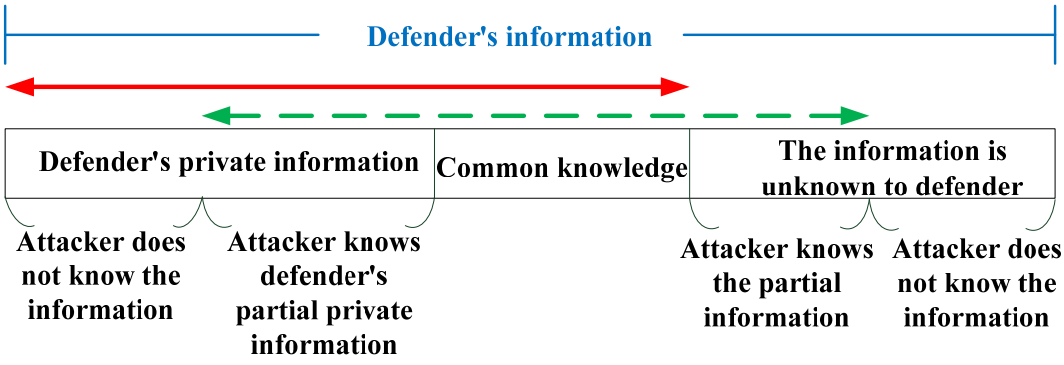


Figure 2-4 : The defender's information in this model

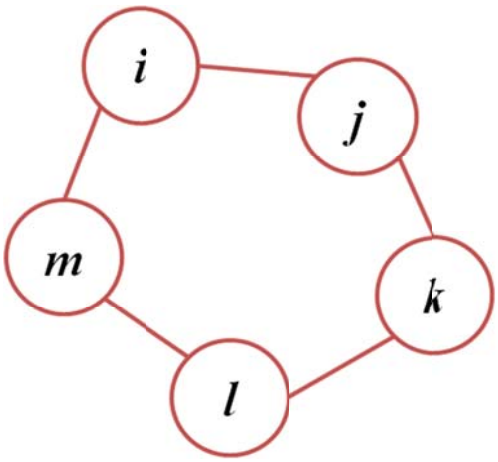


Figure 2-5 : An example of the defender's network topology

The defender could reallocate or recycle the existing resources in the network, but the cost of those reallocated or recycled resources would also be considered in this model. For example, assuming the defender invested resources to conduct firewall on a node, and then the defender could reallocate this firewall to other node or recycle this firewall. Besides, the defender could accumulate resources to decrease attack success probability to defend network nodes in next round. However, the discount factor of those accumulated resources would also be considered in this model. Hence, the total number of resources which the defender could use would be the new allocated, reallocated and recycled resources in each round and those resources could be used to repair compromised nodes, protect survival nodes in the network and release messages of each node.

The attacker also had private information including the number of his resources and some information which the defender did not know such as system vulnerabilities. Besides, the attacker could increase resources when the attacker used system vulnerabilities to compromise network nodes. When the attacker used system vulnerability which the defender did not patch it yet to compromise a node, the defensive resources on the node were received by the attacker with discount. Moreover, the attacker could also accumulate resources on each node to next round to increase attack success probability. However, the discount factor of those accumulated resources would also be considered in this model. For example, before attacking a node the attacker might invest some resources to collect information about the node in order to increase attack success probability. Hence, the total number of resources which the attacker could use would be the new allocated, and the resources from compromised nodes in each round and those resources could be used to attack important nodes in the network and update information of each node. The attacker could update information after observing the result of each round's contest. So, the information of the attacker knowing would increase as shown in Figure 2-6.

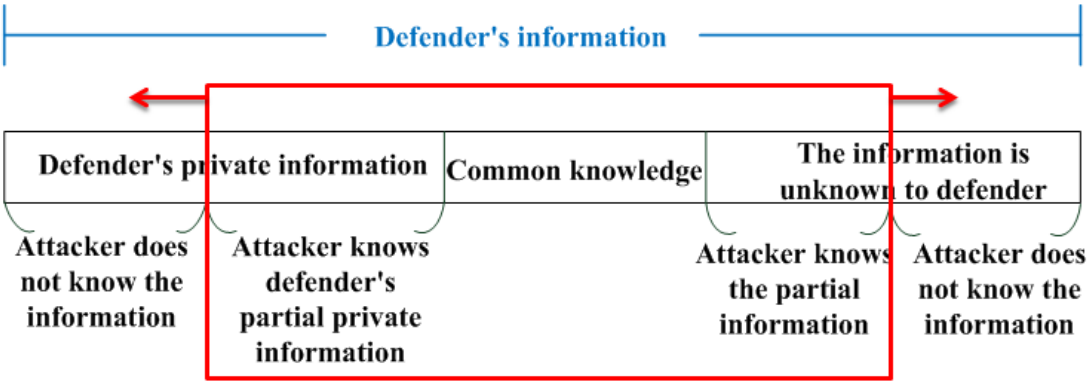


Figure 2-6 : The attacker knowing information would increase

Although the attacker knew something that the defender did not know such as system vulnerabilities, the defender could update information after observing the result of each round's contest. After the defender updated information, he had immune benefit which meant that the attacker was unable to use identical attack. Besides, the defender could use resources doing penetration test to patch system vulnerabilities. So, the information of the defender knowing would increase as shown in Figure 2-7.

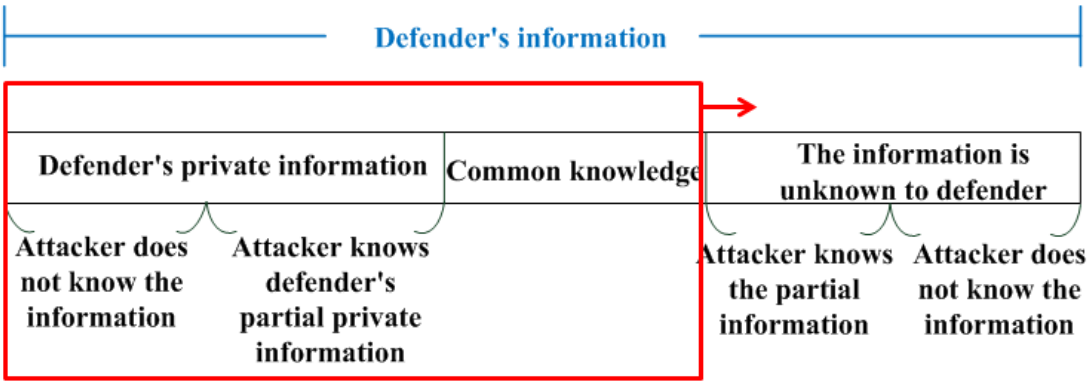


Figure 2-7 : The defender knowing information would increase

We also considered bounded rationality in this model by using an influence factor which would affect attack success probability. Both the defender and the attacker would be full or bounded rationality. And the bounded rationality in here meant that the defender and the attacker might have emotive irrationality such as suicide attacks. However, we only considered the attacker having more irrationality comparing to the defender. The result of the defender having more irrationality might cause a serious consequence. So, we believed that the defender should possess more rationality comparing to the attacker. Besides, we did not consider the defender and the attacker possessing the same degree of rationality. In reasonable assumption, the defender and the attacker possessing rationality would hardly be the same.

Hence, the attacker and the defender's attributes are summarized in Table 2-4.

Table 2-4 : The defender and the attacker's attributes

		Defender	**Attacker**
Defender's information	1. Common knowledge	The information was known to both.	
	2. Defender's private information (ex. node's type, and network topology)	The defender knew all of it.	The attacker knew a part of it.
	3. The defender's other information	The defender did not know it before	The attacker knew a part of it.

	(ex. some system vulnerabilities)	the game starts.	
Budget	Based on the importance of node	Defense.	Attack.
	On each node	Releasing message.	Updating information.
	Reallocated or recycled	Yes. But the defender with extra cost.	No.
	Reward	No.	Yes. If the attacker used system vulnerabilities to compromise a node, the resources on the node could be controlled by the attacker before the defender did not repair it yet.
	Repaired node	Yes.	No.
	Resource accumulation	Yes. But the resources needed to be discounted.	
Immune benefit		Yes. The defender could update information about system vulnerabilities or did penetration test to patch system vulnerabilities.	No.

Rationality		Full or bounded rationality.	Full or bounded rationality.

2.2.2 Defensive Messaging

In the preceding section, we introduced the defender and the attacker's attributes. In this section, we would introduce two kinds of situations of defensive messaging. According to [18], we developed a scenario considering the defender could choose message which might be truth, secrecy, deception or doing nothing at all to each node in each round. And the defender could manipulate his private information by releasing these messages to confuse the attacker to increase defense efficiency.

The first kind of situation of defensive messaging was dividing a node's information into some parts and according to the importance of different part to release messages by the defender. Assuming the information of each node was a collection and the defender could choose a part of information from a node according to his strategy to release truthful message, deceptive message and secrecy or do nothing at all as shown in Figure 2-8. In each round, the defender could choose different part of each node's information to release different message.

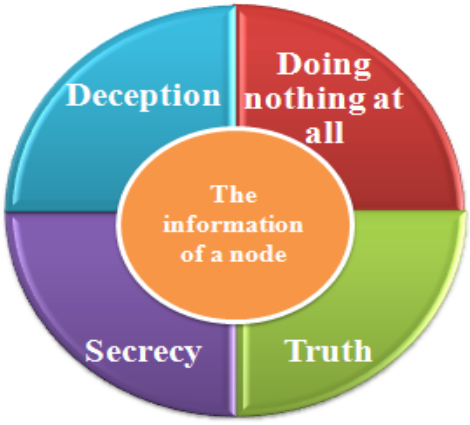


Figure 2-8 : An example of the first kind of message releasing

The defender chose doing nothing at all if and only if the defender did not publicize message. The defender chose truthful message if and only if the public message equaled to actual information; the defender chose secrecy if and only if the message was secret; the defender chose deceptive message if and only if the message not equaled to actual information. The cost of releasing truthful message was lower than the costs of releasing secrecy and deception, respectively. Also, the cost of releasing secrecy was lower than the cost of releasing deception. Because of a successful deception required to keep the truth secret and release the deceptive information. Besides, the cost of truthful, secret and deceptive message was higher than doing nothing at all respectively.

For example, assuming a defender had a computer which used Linux as its OS, Filezilla server as its FTP server and MYSQL as its database. Before an attacker

attacked this computer, the attacker would collect information about this computer. When the information collecting by the attacker was this computer using Linux as its OS, Filezilla server as its FTP server and MYSQL as its database, representing the defender chose doing nothing at all. In other words, as long as the attacker was willing to pay his resources to collect information and he would get truthful information about the defender. And the attacker could use this information to attack the computer. When the information truthful disclosing by the defender was this computer using Linux as its OS, Filezilla server as its FTP server and MYSQL as its database, representing the defender chose complete truthful message. And the attacker could use this information to attack the computer. The difference between doing nothing at all and truthful message was the defender whether to publicize his information. When the information collecting by the attacker was this computer using Windows 7 as its OS and no information about its FTP server and database, representing the defender chose partial deceptive and partial secret message. Though the attacker could use this information to attack the computer, the information did not complete correct. Therefore, the attack might fail and might collect information about the target again. This kind of message releasing could increase the attacker's uncertainty for the defender's information and consume the attacker's resources to analyze information about the defender.

On the other hand, the message releasing may be considered as a node level. The second kind of situation of defensive messaging was using a node's defensive state as a message and releasing to the attacker. The defender had different probability to choose doing nothing at all, truthful, deceptive and secret message. The defender might prefer doing nothing at all, to release truthful, deceptive or secret message for one node, and might not. The defender released different message, which was truth, deception, secrecy or doing nothing to each node as a mixed strategy in each round.

For example, assuming a defender had allocating resources on a node. When the defender did not publicize the information which he allocated resources on the node, representing the defender used doing nothing at all strategy. When the defender released a message which he allocated resources on the node to an attacker, representing the defender used truthful strategy. When the defender released a message which he did not allocate resources on the node to the attacker, representing the defender used deceptive strategy. When the defender did not release a message to the attacker, representing the defender used secret strategy. This kind of message releasing could increase the attacker's uncertainty about the defender's strategies and consume the attacker's resources to analyze information.

Though the defender could use different message to manipulate his private

information to confuse the attacker, the effect of deception or secrecy would be discounted if the attacker knew defender's partial private information. Besides, the effect of deception or secrecy would be discounted if the attacker knew something that the defender did not know such as system vulnerabilities. For example, if the attacker knew some system vulnerabilities about the defender, no matter what message using by the defender the attacker could ignore the message and attack the vulnerabilities forming zero-day attack.

2.2.3 The Defender's Network Topology

In this section, we would introduce some attributes of network topology. As we mentioned previously, the network topology was the part of the defender's private information. Therefore, the attacker only knew partial network topology. The attacker could only attack nodes of the network which had been known to the attacker and keep collecting information about the other nodes.

We considered a complex system with n nodes in series-parallel. A node consists of M components which may be different component or the same to conduct high availability system, where $M \geq 1$. A node's composition could be classified into two types which were a node with backup component and a k-out-of-m node as shown in

Figure 2-9. In Figure 2-9, node *i* was composed of a database and a backup database. When the active database of node *i* failed, node *i* could still operate normally by the backup database. In Figure 2-9, node *j* was composed of 6 servers and it could operate normally using only 4 servers. Using the system design approach of high availability could increase the system survivability. But, we did not use the system design approach of high availability for all nodes in the network topology. We just used it for important nodes. Then, the attacker had to invest more resources to attack the important nodes.

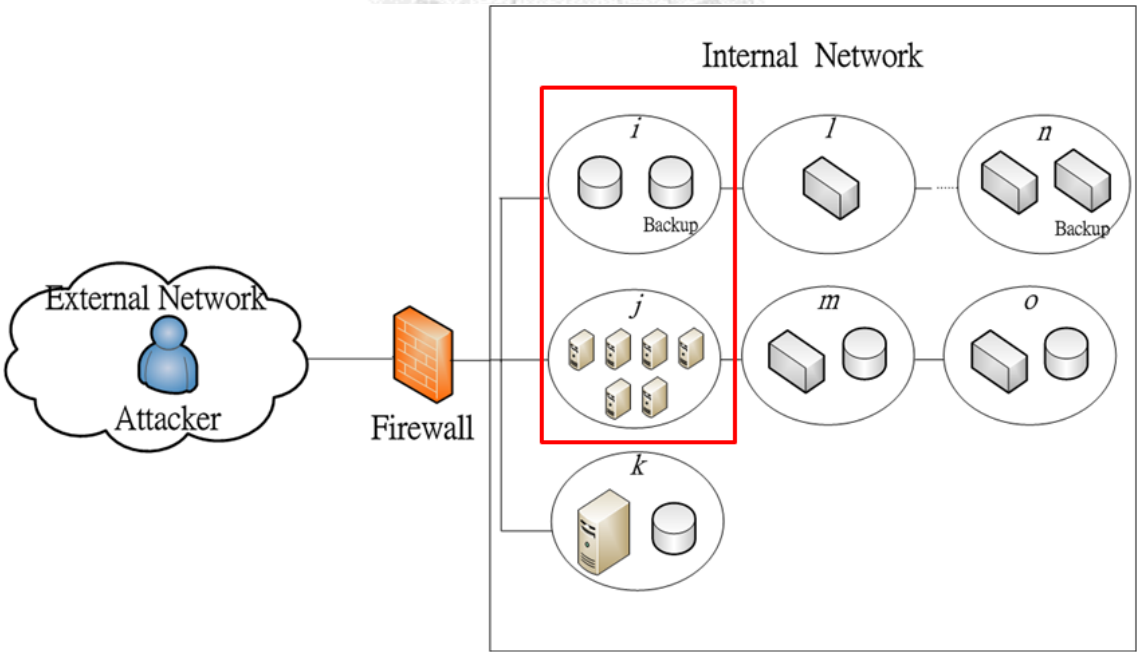


Figure 2-9 : An example of nodes' composition

We also considered three kinds of relationships between nodes which included independence, dependence and interdependence. Independence meant that a node

could function solely and the other nodes without this node could still function. For instance, in Figure 2-10 node *k* could function solely and the other nodes without node *k* could still function.

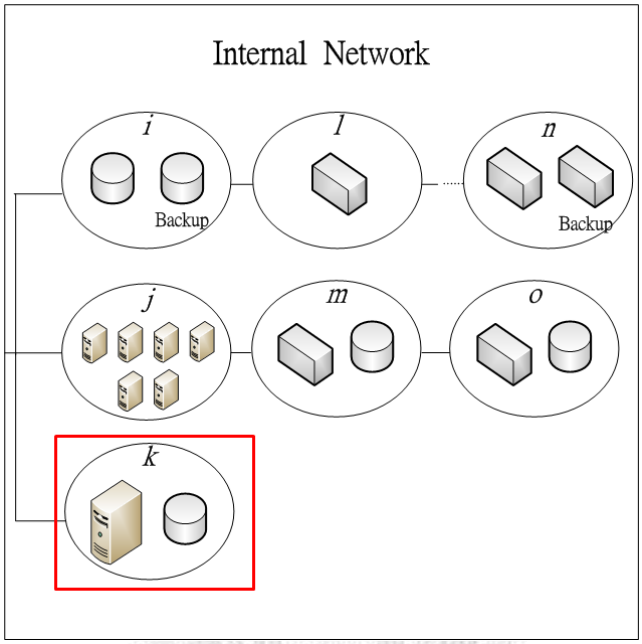


Figure 2-10 : An example of independence

Dependence meant that when a node was destroyed, the other nodes dependent on the destroyed node could not operate normally. For example, in Figure 2-11 node *i* was composed of a database and a backup database. Node *l* was composed of a server. And node *l* needed to gain data from node *i* to keep normal operation. Node *l* could not get data from node *i* when node *i* was destroyed. Though node *l* did not be destroyed, node *l* could not operate normally. Therefore, the relationship between node *i* and node *l* was dependent.

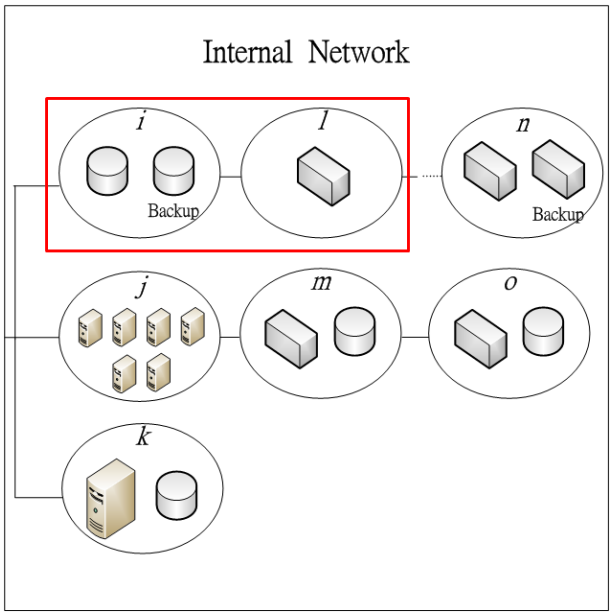


Figure 2-11 : An example of dependence

Interdependence meant that when a node was destroyed, the other nodes interdependent on the destroyed node could not operate normally and vice versa. For instance, in Figure 2-12 both node *m* and node *o* were composed of a server and a database. In daily operation, node *m* and node *o* were gaining data from each other's database. Node *m* could not operate normally when node *o* was destroyed and vice versa. Therefore, the relationship between node *m* and node *o* is interdependent.

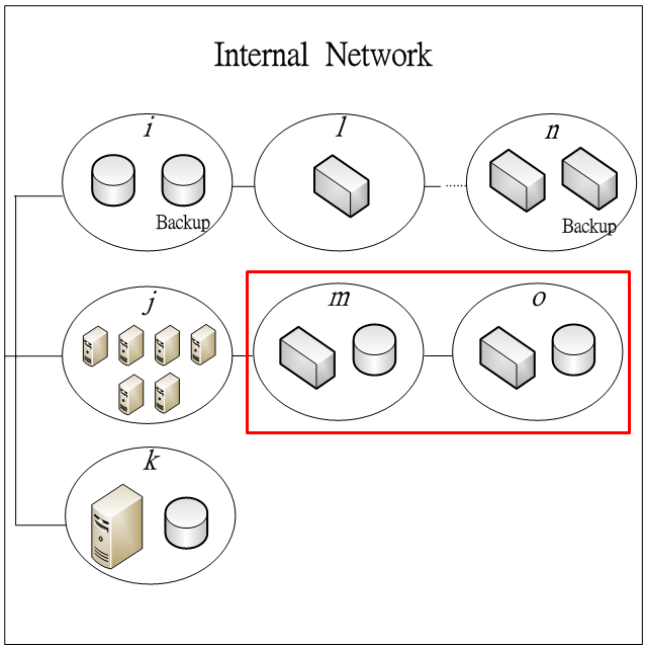


Figure 2-12 : An example of interdependence

In this thesis, we considered two players including cyber attacker and network defender. Besides, we considered both cyber attacker and network defender having private information. Therefore, Figure 2-13 provided the sequence of actions for this problem. At the beginning of the first round, nature chose the defender each node's type, which could be lower or higher valuation. For each round, the decision process was as follows. First, network defender needed to determine whether to reallocate or recycle nodes' resources, whether to repair compromised nodes, whether to patch or using penetration test to patch system vulnerabilities and network defender should also determine actual defense and release messages to each node. And then, cyber attacker

observed the messages releasing by network defender to take actions. Then, we could calculate the result (Average DOD) in this round. Finally, if the game was already the N round, then the game ended. Otherwise, both cyber attacker and network defender would update information about each other after observing the outcome of the contest, and then the game moved to the next round.

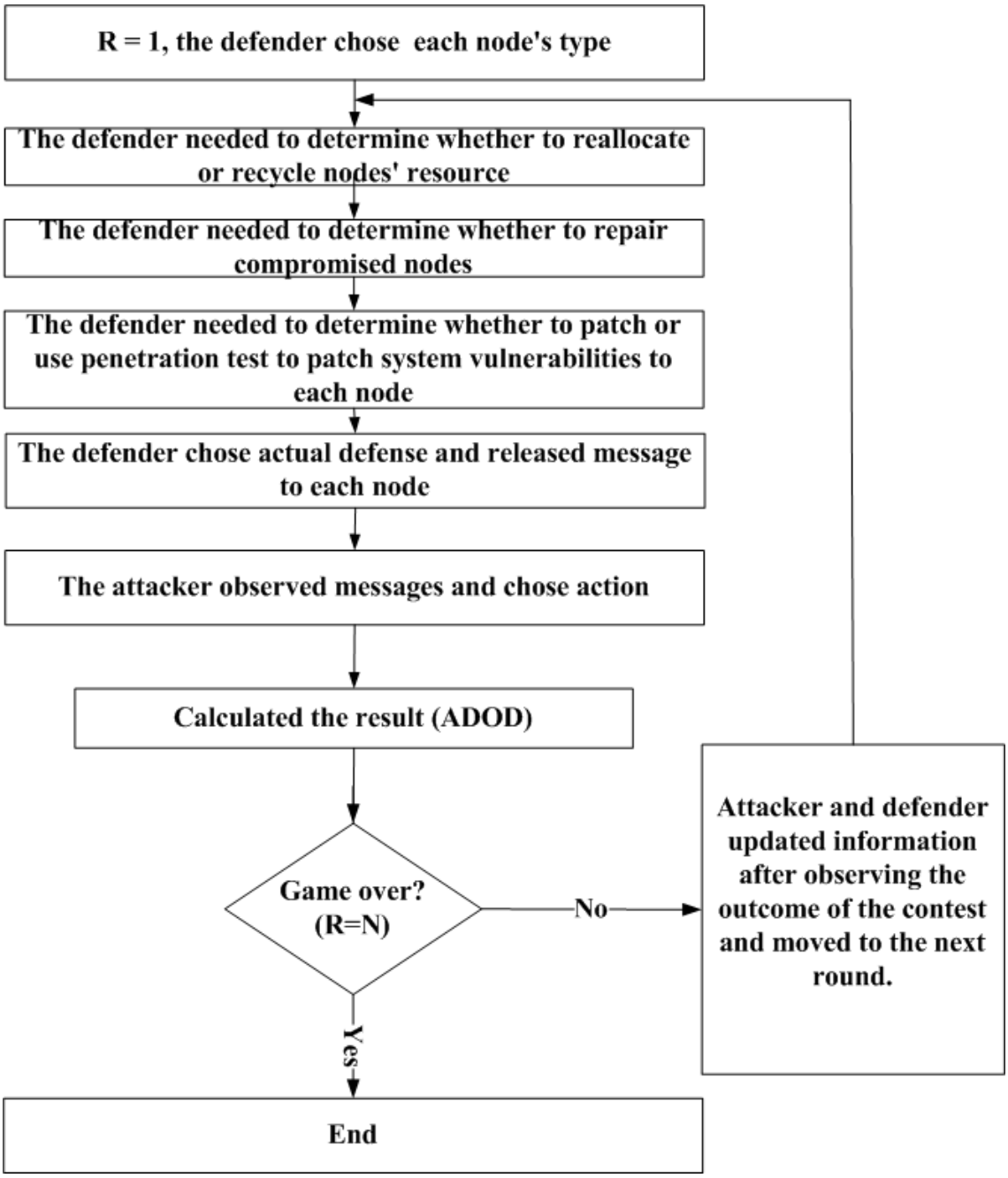


Figure 2-13 : The sequence of actions for this problem

Therefore, the problem descriptions and problem assumptions were summarized in the Table 2-5 and Table 2-6.

Table 2-5 : Problem descriptions

Given :

1. The total budget of network defender.
2. The total budget of cyber attacker.
3. Both the defender and the attacker had incomplete information about each other.

Objective :

The objective of the attacker was to maximize the damage degree of the network, but the defender's goal was to minimize the damage degree of the network. Therefore, to minimize the maximum damage degree of network would be this problem. Besides, the Average DOD value would be used to evaluate the damage degree of the network.

Subject to :

1. The total budget constraint of network defender.
2. The total budget constraint of cyber attacker.

To determine :

1. The attacker needs to determine how to allocate attack budget to each node and whether to use the system vulnerabilities of node *i* to attack node *i* in each round.
2. The defender is usually looking forward to determining how to allocate defense budget, whether to repair the compromised node, whether to patch or using penetration test to patch system vulnerabilities, how to recycle or reallocate the node's resource and determine which message strategy would use to each node in each round.

Table 2-6 : Problem assumption

1. The problem involved both cyber attacker and network defender. The objective of attacker was to maximize the value of the Average DOD. On the other hand, the defender's goal was to minimize the value of the Average DOD.
2. Both the attacker and the defender were based on the importance of node to take actions.
3. Cyber attacker had incomplete information about:

   ① Network topology: The attacker could only attack nodes of the network which had been known to the attacker and kept collecting information;

② Defender's private information: The defender did not know the attacker knew it;

③ Defender's system vulnerabilities: The defender did not know it.

4. The attacker had private information which included the attacker's budget and the defender's system vulnerabilities.
5. The defender had private information which included each node's type and the network topology.
6. Both attacker and defender were limited by the total budget.
7. Both attacker and defender might be rational or bounded rational.
8. Both attacker and defender knew that there were two types (lower or higher valuation) of nodes.
9. Both attacker and defender knew each node's prior belief in the first round.
10. Both attacker and defender could update information after observing the result of each round's contest.
11. The defender could use resources doing penetration test to patch system vulnerabilities.
12. There were no enforceable agreements between attacker and defender which meant that the attacker and the defender could not cooperate.

13. In each round, the defender determines strategy and chooses message which may be truth, secrecy, deception or doing nothing at all to each node.
14. The cost of releasing truthful message was lower than the costs of releasing secrecy and deception, respectively. Also, the cost of releasing secrecy was lower than the cost of releasing deception. The cost of truthful, secret and deceptive message would not be accumulated or recycled and was higher than doing nothing at all respectively.
15. The defender using deceptive messages could lower the attack success probability.
16. The defensive messaging could be classified into two situations:

    ①A node's information could be divided into different part to release message by the defender;

    ②The defender could release a node's defensive state as a message to the attacker.
17. Only node attack was considered. (We did not consider the link attack)
18. Only malicious attack was considered. (We did not consider the random errors)
19. Cyber attacker could accumulate experiences to increase attack success probability to compromise network nodes in next time.
20. Network defender could accumulate resources to decrease attack success probability to defend network nodes in next time.

21. The attacker could increase budget when the attacker used system vulnerabilities to compromise network nodes. This meant that the compromised network nodes were controlled by the attacker.
22. From the view of the defender, the budget could be reallocated or recycled but the discount factor was also considered.
23. From the view of the defender, the compromised nodes could be repaired.
24. Only static network was considered. (We did not consider the growth of network)
25. The defender used redundant components to design system to achieve high availability.
26. The network survivability was measured by Average DOD value.
27. Any two nodes of network could form to be an O-D pair.
28. The attack success probability was calculated by contest success function, considering the resource allocation on each node of both parties.

2.3 Mathematical Formulation

In the following, the notations of given parameter and decision variable in this model were listed in Table 2-7 and Table 2-8.

Table 2-7 : Given parameter

Given parameter	
Notation	***Description***
V	Index set of nodes
V_r	Index set of nodes of the attacker knowing in round r, where $r \in R$ and $V_r \subseteq V$
R	Index set of rounds in the attack and defense actions
F	Index set of all nodes' system vulnerability
F_{Ar}	Index set of system vulnerability of the attacker knowing in round r, where $r \in R$ and $F_{Ar} \subseteq F$
F_{Dr}	Index set of system vulnerability of the defender knowing in round r, where $r \in R$ and $F_{Dr} \subseteq F$
w_r	The weight of the Average DOD in round r, where $r \in R$
$\hat{A}$	Total budget of attacker

$\hat{B}$	Total budget of defender
θ_{Di}	Existing defense resource allocated on node i, where $i \in V$
θ_{Ai}	Existing attack resource allocated on node i, where $i \in V_r$
e_{ri}	Repair cost of defender when node i is dysfunctional in round r, where $i \in V$ and $r \in R$
λ_{rj}	The cost of the defender only patches the j-th type of system vulnerability in round r, where $j \in F_{Dr}$ and $r \in R$
μ_{rj}	The cost of the defender uses penetration test to patch the j-th type of system vulnerability in round r, where $j \in F_{Dr}$ and $r \in R$
π_{mri}	m = 0,1, 2 and 3 represent the cost of doing nothing at all and the cost of defensive messaging of truth, secrecy, deception on node i by defender in round r respectively, where $i \in V$, $r \in R$ and $m \in \{0, 1, 2, 3\}$
d_{ri}	The discount rate of defender reallocates resources on node i in round r, where $i \in V$ and $r \in R$
C_{ri}	The discount rate of defender recycles resources on node i in round r,

	where $i \in V$ and $r \in R$
$h_{ri}(t)$	The discount rate of attacker accumulated resources would be increased with time t on node i, where $i \in V_r$ and $r \in R$
U_i	The discount rate of attacker controls the resources of node i by using system vulnerabilities to compromise node i, where $i \in V_r$
ε	The cost of attacker updating information
δ_{ri}	1 if node i is compromised by attacker in round r-1, 0 otherwise where $i \in V_r$ and $r \in R$
γ_{ij}	The reward of the attacker uses the j-th type of system vulnerability on node i to attack node i, where $i \in V$ and $j \in F_{Ar}$
η_{rij}	1 if the attacker considers that the node i still has the j-th type of system vulnerability in round r, 0 otherwise where $i \in V_r$, $j \in F_{Ar}$ and $r \in R$
ζ_{rij}	The system vulnerability status on node i in round r. 1 if the node i has the j-th type of system vulnerability in round r, 0 otherwise where $i \in V$, $j \in F$ and $r \in R$ (Once the defender finds the j-th type of system

	vulnerability in round r, the ζ_{rij} value of the nodes, which have the j-th type of system vulnerability, are 1 in round r.)

Table 2-8 : Decision variable

Decision variable	
Notation	***Description***
A_r	Attacker's attack budget in round r, where $r \in R$
B_r	Defender's defense budget in round r, where $r \in R$
$\overrightarrow{a_r}$	Attacker's budget allocation, which is a vector of attack cost a_{r1}, a_{r2} to a_{ri} in round r, where $i \in V_r$ and $r \in R$
$\overrightarrow{b_r}$	Defender's budget allocation, which is a vector of defense cost b_{r1}, b_{r2}, to b_{ri} in round r, where $i \in V$ and $r \in R$
x_{ri}	Attacker's budget allocation on node i in round r, where $i \in V_r$ and $r \in R$
y_{ri}	Defender's budget allocation on node i in round r, where $i \in V$ and $r \in R$
$\overrightarrow{s_r}$	Defender's node recovery status, which is a vector of repaired status z_{r1},

	z_{r2}, to z_{ri} in round r, where $i \in V$ and $r \in R$
s_{ri}	1 if node i is repaired by defender in round r, 0 otherwise where $i \in V$ and $r \in R$
α_{ri}	The proportion of resources on node i is reallocated by defender in round r, where $i \in V$ and $r \in R$
β_{ri}	The proportion of resources on node i is recycled by defender in round r, where $i \in V$ and $r \in R$
p_{mri}	m = 0,1, 2 and 3 represent the information proportion or probability of defender doing nothing at all, using truthful, secrecy, deceptive message on node i in round r respectively, which falls in (0,1), where $i \in V$, $r \in R$ and $m \in \{0, 1, 2, 3\}$
q_{rij}	1 if the attacker uses the j-th type of system vulnerability on node i to attack node i in round r, 0 otherwise where $i \in V_r$, $j \in F_{Ar}$ and $r \in R$
φ_{rij}	1 if the defender only patches the j-th type of system vulnerability on node i in round r, 0 otherwise where $i \in V$, $j \in F_{Dr}$ and $r \in R$

τ_{rij}	1 if the defender uses penetration test to patch the *j*-th type of system vulnerability on node *i* in round *r*, 0 otherwise where $i \in V, j \in F_{Ar}$ and $r \in R$
$\overline{D}(\overrightarrow{a_r}, \overrightarrow{b_r})$	The Average DOD, which is considering under attacker's and defender's budget allocation are $\overrightarrow{a_r}$ and $\overrightarrow{b_r}$ in round *r*, where $r \in R$

Using the above notations of given parameter and decision variable, the problem was formulated as the following.

Objective function:

$$\min_{\overrightarrow{b_r}} \max_{\overrightarrow{a_r}} \sum_{r \in R} w_r \, \overline{D}(\overrightarrow{a_r}, \overrightarrow{b_r}) \qquad \text{(IP 1)}$$

Subject to:

$$\sum_{i \in V_r} x_{ri} + \varepsilon \le A_r + \sum_{i \in V_r} U_i \, \theta_{Di} \sum_{r \in R} (\delta_{ri} - s_{ri}) \sum_{j \in F_{Ar}} q_{(r-1)ij}(\zeta_{rij} - \varphi_{rij} - \tau_{rij}) + \sum_{i \in V_r} \theta_{Ai} h_{ri}(t) + \sum_{i \in V_r} \sum_{j \in F_{Ar}} q_{rij} \gamma_{ij} \eta_{rij} (\zeta_{rij} - \varphi_{rij} - \tau_{rij})$$

$$\forall \, r \in R \qquad \text{(IP 1.1)}$$

$$\sum_{i \in V} y_{ri} + \sum_{i \in V} e_{ri} s_{ri} + \sum_{i \in V} \sum_{m \in \{0,1,2,3\}} p_{mri} \pi_{mri} + \sum_{i \in V} \sum_{j \in F_{Dr}} \lambda_{rj} \varphi_{rij} \zeta_{rij} + \sum_{i \in V} \sum_{j \in F_{Dr}} \mu_{rj} \tau_{rij} \zeta_{rij} \leq B_r + \sum_{i \in V} \theta_{Di} (d_{ri} \alpha_{ri} + C_{ri} \beta_{ri}) \sum_{r \in R} [1 - (\delta_{ri} - s_{ri})]$$

$$\forall\, r \in R \qquad \text{(IP 1.2)}$$

$$\sum_{r \in R} A_r \leq \hat{A} \qquad \text{(IP 1.3)}$$

$$\sum_{r \in R} B_r \leq \hat{B} \qquad \text{(IP 1.4)}$$

$$\sum_{r \in R} s_{ri} \leq \sum_{r \in R} \delta_{ri} \qquad \forall\, i \in V_r \qquad \text{(IP 1.5)}$$

$$\sum_{m \in \{0,1,2,3\}} p_{mri} = 1 \qquad \forall\, r \in R, i \in V \qquad \text{(IP 1.6)}$$

$$0 \leq \alpha_{ri} \qquad \forall\, r \in R, i \in V \qquad \text{(IP 1.7)}$$

$$0 \leq \beta_{ri} \qquad \forall\, r \in R, i \in V \qquad \text{(IP 1.8)}$$

$$\alpha_{ri} + \beta_{ri} \leq 1 \qquad \forall\, r \in R, i \in V \qquad \text{(IP 1.9)}$$

$$\sum_{r \in R} \varphi_{rij} \leq \sum_{i \in V_r} \sum_{r \in R} q_{rij} \qquad \forall\, i \in V_r, j \in F_{Dr} \qquad \text{(IP 1.10)}$$

$$\sum_{r \in R} \varphi_{rij} + \sum_{r \in R} \tau_{rij} + \zeta_{rij} \leq 1 \qquad \forall\, r \in R, i \in V, j \in F_{Dr} \qquad \text{(IP 1.11)}$$

Explanation of the objective function:

(IP 1) The objective function was to minimize the maximum sum of the product of Average DOD and weight in each round. The important degree of Average DOD value in each round was usually different, so the weight would be assigned to the Average DOD value in each round in this model.

Explanation of the constraint function:

(IP 1.1) Describing the sum of the allocated attack budgets in each node and the cost of updating information should not exceed the sum of attack budgets, the collection of compromised nodes' resources, accumulated resources and the reward of using system vulnerability to attack in that round.

(IP 1.2) Describing the sum of the allocated defense budgets in each node, repaired cost of the compromised nodes, the cost of releasing messages, the cost of only patching and the cost of using penetration test to patch system vulnerability in each node should not exceed the sum of the new allocated, reallocated and recycled budgets in that round.

(IP 1.3) Describing the sum of the allocated attack budgets in each round should not exceed the total budget of the attacker.

(IP 1.4) Describing the sum of the allocated defense budgets in each round should not exceed the total budget of the defender.

(IP 1.5) Describing only after the nodes were compromised by the attacker, the nodes could be repaired by the defender.

(IP 1.6) Describing the sum of the information proportion or probability of defender using different message on node *i* in round *r* should be 1.

(IP 1.7) Describing the proportion of resources on node *i* was reallocated by defender in round *r* should between 0 and 1.

(IP 1.8) Describing the proportion of resources on node *i* was recycled by defender in round *r* should between 0 and 1.

(IP 1.9) Describing the sum of the proportion of resources reallocated and resources recycled on node *i* in round *r* should between 0 and 1.

(IP 1.10) Describing once after the attacker used the *j*-th type of system vulnerability on node *i* to attack node *i*, the *j*-th type of system vulnerability could be patched by the defender.

(IP 1.11) Describing the sum of the number of only patching, the number of using penetration test to patch the *j*-th type of system vulnerability on node *i* in each round and the system vulnerability status of node *i* in round *r* should not exceed 1.

Chapter 3 Solution Approach

In this model, we would introduce how to optimize resource allocation of each node in each round for both cyber attacker and network defender and how to evaluate damage degree of network by the Average DOD value. We combined game theory with gradient method to find the optimal resource allocation strategy for both cyber attacker and network defender. The gradient method was used to find the optimal resource allocation strategy on each node for both cyber attacker and network defender. Besides, the game theory was applied to find the optimal resource allocation in each round for both cyber attacker and network defender. In the first section, the solution procedure of this problem would be introduced. The concept of gradient method would be introduced in the second section. And then, a method used to accelerate calculation of the Average DOD value and how to calculate Average DOD value in multiple rounds would be introduced in third and the fourth section. The game theory used to find the optimal resource allocation in each round would be introduced in the fifth section. In the final section, we would discuss the time complexity in our model.

3.1 The Solution Procedure

In this thesis, we would combine game theory and gradient method to find the optimal resource allocation strategy on each node in each round for both cyber attacker and network defender. The detailed process was shown in Figure 3-1.

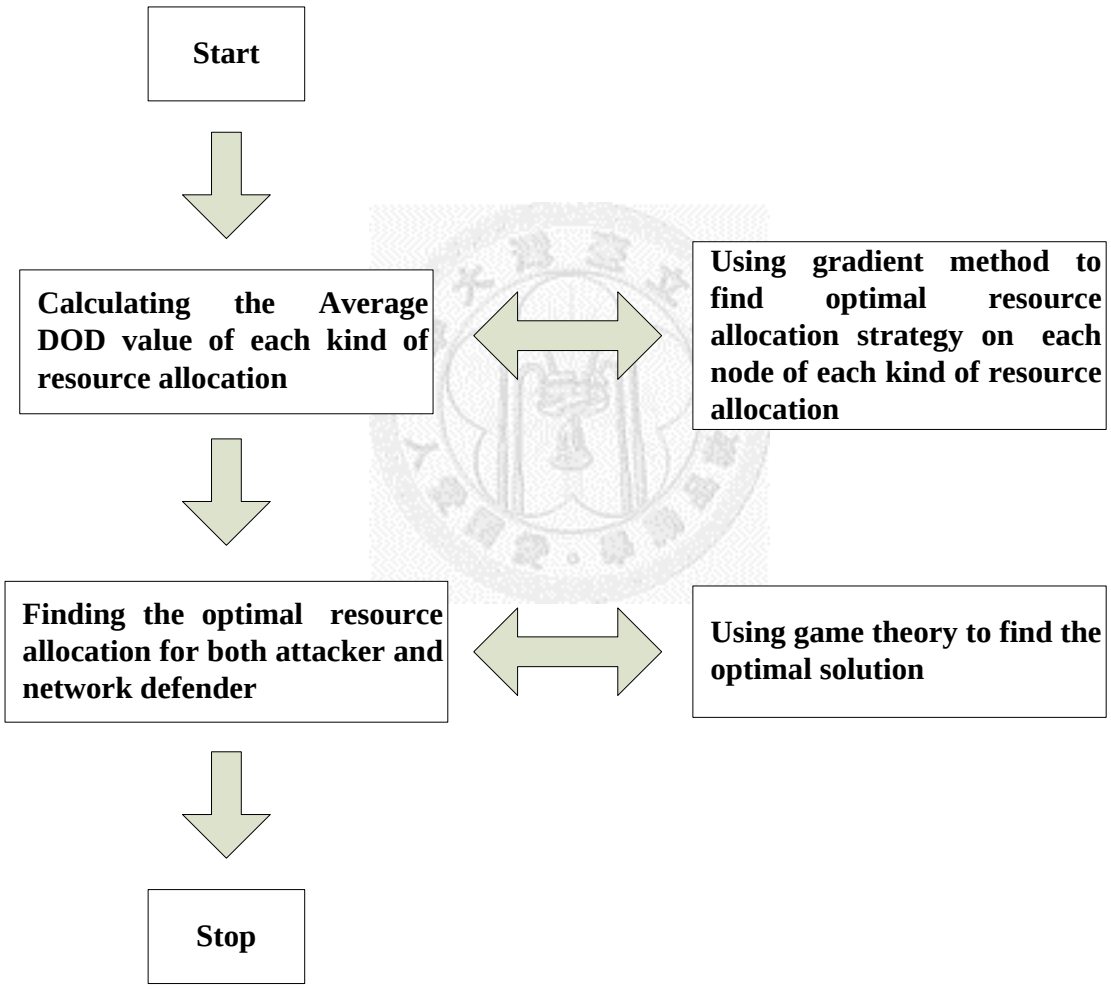


Figure 3-1 : The solution procedure of this model

Therefore, gradient method and game theory would be introduced in the

following.

3.2 Gradient Method

The gradient method was a general framework for solving optimization problems where was to maximize or minimize functions of continuous parameters. The problem in this model was a min-max formulation and both cyber attacker and network defender were assumed that they could allocate continuous budgets on each node in each round. Therefore, the gradient method was extremely suitable for solving this problem.

The gradient method could be classified into two types, one was the gradient descent and the other was the gradient ascent. The gradient descent method could be used to solve optimization minimization problem and the optimization maximization problem could be solved by the gradient ascent method. The concept of gradient descent and gradient ascent was similar, so both of them could adopt the following algorithm:

1) Initially, to get a start point. The selection of start point was important, because it might influence the result and computational efficiency.

2) To determine a direction, it could be positive or negative. If a maximization problem wanted to be solved, a positive direction should be chosen. On the other hand, a negative direction was another choice which could be used to solve minimization problem.

3) The gradient method adopted a step-by-step method to find the optimization. Therefore, the step size which was the move size in each step should be determined.

4) To determine the dimension to move. The gradient method used the **derivative method** to find the dimension which had most influence, move a step in the most impact dimension and set the new position to be the next start point. And then repeat step 4 until stopping criterion was satisfied.

In this model, inner problem was a maximization problem, so the gradient ascent method was used to solve the inner problem. Besides, the gradient descent was suitable to solve the outer problem which was a minimization situation. Before using the gradient method to solve this problem, something should be determined:

1) How many dimensions are there in this problem? Both cyber attacker and

network defender should determine how many budgets to be allocated in each node, so the number of network nodes would be the number of dimension.

2) What's the start point for both cyber attacker and network defender? Both cyber attacker and network defender were assumed evenly allocate their limited resources on each node, so the start point would be R/N in each dimension. (where R was the total attack or defense resources in that round; N was the total number of network nodes)

3) How calculates derivative of the Average DOD? The derivative of the Average DOD was difficult to calculating, so the following method was used to calculate it：

$$\lim_{h\to 0}\frac{\overline{D}(r_i+h)-\overline{D}(r_i)}{h}$$

$\overline{D}$ meant the Average DOD value

r_i meant the number of resources on node *i*

4) What is the stopping criterion? If the impact of each dimension was the same, the gradient method could stop calculating.

In the following, the solution procedure of this problem would be introduced. There were four steps in this approach and the detailed procedure was as below:

Step 1. Initially, both cyber attacker and network defender were assumed evenly

allocate their limited resources on each node. For example, there was a network consisting of three nodes. Both cyber attacker and network defender had six units of attack or defense resources in the same round. As a result, cyber attacker and network defender would respectively allocate two units of attack or defense resource on each node.

Step 2. The cyber attacker had the limited resource in each round, so cyber attacker would adopt gradient ascent method to maximize damage degree of network.

Step 3. On the other hand, the defense resources were also limited in each round. The network defender would use the gradient descent method to find the minimization solution.

Step 4. Repeating step 2 and step 3 until the stop criterion was satisfied.

Therefore, we could find the optimal resource allocation strategy for both cyber attacker and network defender in each round. Besides, the Average DOD was used to evaluate the damage degree of network.

3.3 Accelerating Calculation of the Average DOD Value

In this problem, the Average DOD value was used to evaluate damage degree of network. In order to calculate Average DOD, we should consider all possible network configurations. Once the number of network node was too huge, it would take much time to calculate the Average DOD value. Hence, the method to accelerate calculation of the Average DOD value would be proposed.

Average DOD value was calculated by the DOD value and probability of each possible network configuration. Therefore, when the probability was larger, the possibility of network configuration occurring would be bigger. The calculation of the probability was easier than the calculation of the DOD value, so we used the probability value of each network configuration to reduce complexity of the calculation of the Average DOD value.

When the probability of network configuration occurring was extremely low, the influence on Average DOD value would also low. For example, if the probability of network configuration equaled to 0.00000000001 and the DOD value equals to 10000 or 1, the product of probability and the DOD value in two different situations were almost identical. Therefore, this method would be applied to reduce complexity in this model.

3.4 The Calculation of Average DOD Value in Multi-Round

In this section, we would introduce how to use the Average DOD value to evaluate damage degree of network in multiple rounds. In each round, both the defender and the attacker would use gradient method to find the optimal strategy. Besides, both of them have to allocate resources in each node. Therefore, each node would have a compromised probability which was calculated by contest success function. So, the probability of different states of network configuration could be calculated by the product of compromised probability of each node. There are multiple likelihoods in next round, and consequently the concept of the expected value would be used to calculate the Average DOD value in next round. Finally, combining the Average DOD value with the weight of each round would be the final damage degree of the network. As a result, the final Average DOD value would be

The final Average DOD value would be = $W_1 \times \overline{D}_1 + \sum_{r=2}^{n} W_r \times \sum_{j=0}^{m} \left(\overline{D}_{rj} \times P_{(r-1)j} \right)$

(W_r is the weight of round r, $\overline{D}_{rj}$ is the Average DOD value of the configuration j in round r and $P_{(r-1)j}$ is the incidence of the configuration j in previous round)

3.5 Using Game Theory to Find the Optimal Solution

In the preceding section, we introduced gradient method which could find the optimal resource allocation strategy on each node for both cyber attacker and network defender. In this section, we would introduce game theory which could help us to find the optimal percentage resource allocation in each round for both cyber attacker and network defender.

In this problem, both cyber attacker and network defender needed to determine how to allocate resources efficiently on each node in each round. Besides, in this model we assumed the defender determining strategy and choosing message which might be truth, secrecy, deception or doing nothing at all to each node in each round. Moreover, we assumed both the defender and the attacker having incomplete information about each other. Though this model was a problem of incomplete information, the definition of complete information game in [31] was "Every player knows both the strategies and payoffs of all players in the game, but not necessarily the actions." Basically, the defender and the attacker in this problem knew both the strategies and payoffs of each other, but the actions were not. Therefore, this problem could be viewed as a complete information game.

However, how to find the optimal strategies in the game theory was another issue. Therefore, the solution approach of this game would be introduced in the following [32].

Step 1. Finding out dominant strategy. The dominant strategy was always better than other strategies no matter what kind of strategy the opponent to take.

Step 2. If only one strategy was remained of each player, it would be the optimal strategy. Otherwise, go to step 3.

Step 3. Using the min-max strategy to find the optimal strategy of each player. If min-max strategy still could not find the optimal strategy, go to step 4.

Step 4. Using the mixed strategy (Linear programming) to find the optimal strategy of each player.

For example, both cyber attacker and network defender had 3 different strategies about allocating different resources percentage in each round as shown in Table 3-1. In addition, the combined results of different percentage resource allocation strategies for

both cyber attacker and network defender would be calculated by the Average DOD.

Step 1. Finding out dominant strategy. From the view of the attacker, the attacker wanted to maximize the damage degree (Average DOD) of the network, so the S_{13} strategies would be the optimal strategy. On the other hand, the defender wanted to minimize the damage degree of network, so the S_{21} would be the optimal strategy.

Step 2. Because only one result was remained for each player, it would be regarded as the optimal solution for both parties. The optimal strategy of the attacker would be S_{13} and the optimal strategy of the defender would be S_{21}. Finally, the result of this example would be 3.

Table 3-1 : An example of game theory

Strategy		Attacker		
		S_{11}	S_{12}	S_{13}
Defender	S_{21}	3	2	3
	S_{22}	2	2	5
	S_{23}	2	1	4

3.6 Time Complexity Analysis

The time complexity of the algorithm can quantify the amount of time which is taken by the algorithm to run as a function of the size of the input to the problem. Therefore, we would discuss the time complexity of the algorithm in this section.

In this model, we use the Average DOD value to evaluate the damage degree of the network. Moreover, Average DOD combined the concept of probability calculated by the contest success function [30] with the DOD metric. Furthermore, we used

gradient method to find the optimal resource allocation in each node to calculate attack success probability. Lemma 1 states the time complexity of gradient method.

Lemma 1 *Given a total budget of network defender and cyber attacker, and a network topology, G = (V, E), the time complexity of gradient method is O(nV).*

Proof. Because the impact degree of each node would be checked in each round, the time complexity of the gradient method would be *O(nV)*. (Where *n* is the maximum number of the checked round and *V* is the number of total nodes in the network)

The DOD value would not only be used to measure the damage degree of each configuration but also considered all OD pairs. Therefore, lemma 2 states the time complexity of calculating the DOD value of each configuration.

Lemma 2 *Given a network topology, G = (V, E), and using Dijkstra's shortest path algorithm to find all OD pairs the time complexity of calculating the DOD value of each configuration is* $O(WV^2)$.

Proof. Because the time complexity of Dijkstra's shortest path algorithm is $O(V^2)$, the time complexity of calculating the DOD value of each configuration would be

$O(WV^2)$. (Where $W (= C_2^V)$ is the number of the OD pair)

However, we needed to consider 2^V different kinds of network configuration to calculate Average DOD value in one round. Therefore, lemma 3 states the time complexity of calculating Average DOD value in one round.

Lemma 3 *Given a network topology, G = (V, E), and using Dijkstra's shortest path algorithm to find all OD pairs the time complexity of calculating Average DOD value is* $O(2^V WV^2)$ *in one round.*

Proof. Because we needed to consider 2^V different kinds of network configuration to calculate Average DOD value, the time complexity to compute the Average DOD value in one round would be $O(2^V WV^2)$. (Where $W (= C_2^V)$ is the number of the OD pair)

As a result, once the number of node is too huge, it must take much time to compute the Average DOD value in only one round.

Besides, in this model we considered defense-attack scenario in multi-rounds. After one round, it would lead to 2^V different kinds of network state. Therefore, lemma

4 states the time complexity of calculating Average DOD value in multiple rounds.

Lemma 4 *Given a network topology, G = (V, E), and using Dijkstra's shortest path algorithm to find all OD pairs the time complexity of calculating Average DOD value is* $O(2^{RV}WV^2)$ *in R rounds.*

Proof. After one round, it would lead to 2^V different kinds of network state. Therefore, in the R round $2^{(R-1)V}$ different kinds of network state needed to be considered and $2^{(R-1)V}$ of the Average DOD value needed to be calculated. As a result, the time complexity would be $O((2^{(R-1)V})(2^VWV^2)) = O(2^{RV}WV^2)$ in R rounds. (Where W $(= C_2^V)$ is the number of the OD pair)

Besides, the defender could choose message which might be truth, secrecy, deception or doing nothing at all to each node in each round. Therefore, lemma 5 states the time complexity of considering defensive messaging in multiple rounds.

Lemma 5 *Given a network topology, G = (V, E), using Dijkstra's shortest path algorithm to find all OD pairs, and in each round the defender could choose message which might be truth, secrecy, deception or doing nothing at all to each node, the time complexity of calculating Average DOD value which considered*

defensive messaging in R rounds is $O(4^{RV}WV^3)$.

Proof. According to lemma 4, the time complexity of calculating Average DOD value is $O(2^{RV}WV^2)$ in R rounds. Besides, in each round the defender having 4 kinds of message could choose to each node. Therefore, the time complexity of considering defensive messaging in R rounds is $O(4*2^{(R-1)V}V)$. As a result, the time complexity would be $O((2^{RV}WV^2)(4*2^{(R-1)V}V)) = O(4^{RV}WV^3)$ in R rounds. (Where W (= C_2^V) is the number of the OD pair)

Moreover, both cyber attacker and network defender have different percentage of resources allocation in each round as their strategies. And we adopted game theory to find the optimal solution for both cyber attacker and network defender. Therefore, lemma 6 states the time complexity of computing the payoff values of different kinds of resource allocation strategy for both cyber attacker and network defender in multiple rounds.

Lemma 6 *Given a network topology, G = (V, E), using Dijkstra's shortest path algorithm to find all OD pairs, l strategies that the attacker can take, and k strategies that the defender can take the time complexity of computing the payoff*

values of different kinds of resource allocation strategy for both cyber attacker and network defender in R rounds *is* $O(lk4^{RV}WV^3)$.

Proof. According to lemma 5, the time complexity of calculating Average DOD value which considered defensive messaging is $O(4^{RV}WV^3)$ in R rounds. Therefore, the time complexity of computing the payoff values of different kinds of resource allocation strategy for both cyber attacker and network defender in R rounds would be $O(lk4^{RV}WV^3)$. (Where W (= C_2^V) is the number of the OD pair)

According to the time complexity of the algorithm, this model could be viewed as an extremely complicated problem. As a result, there are some restrictions would be considered in the experiments. The detailed computational experiments would be demonstrated in Chapter 4.

Chapter 4 Computational Experiments

4.1 Experiment Environment

The proposed solution approach is implemented in Eclipse and run on the PC with AMD Phenom(tm) IIX4 B40 Processor 3.00 GHz, 6 GB RAM, and on the OS of the MS Windows 7.

With the time complexity analysis, we know this problem is an extremely complicated problem. It costs eight days to get the results of one experiment considering three kinds of topology, three rounds and nine nodes. Therefore, we only considered 9 nodes and three-round interaction between the attacker and the defender in the experiments. Moreover, we also considered three kinds of network topology including the grid network (GD), random network 1 (RD) and scale-free network 1 (SF). The GD is really regular network. The SF is a kind of network whose degree distribution follows a power law. And, the RD is connected with other nodes randomly. Three kinds of network topology which were demonstrated in Figure 4-1, Figure 4-2 and Figure 4-3 respectively would be adopted to take the experiments in this thesis.

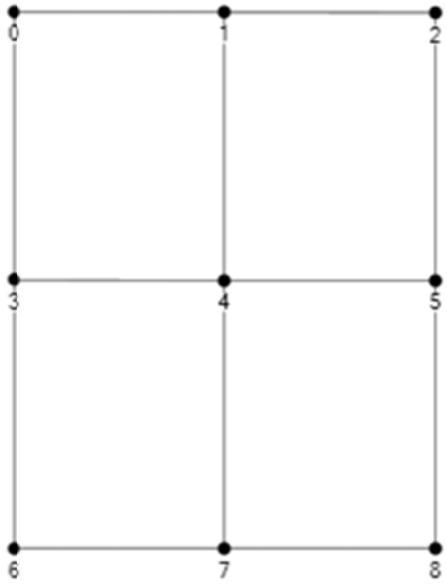


Figure 4-1 : Grid network

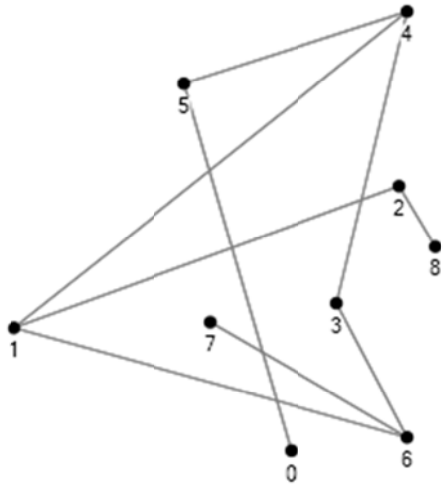


Figure 4-2 : Random network 1

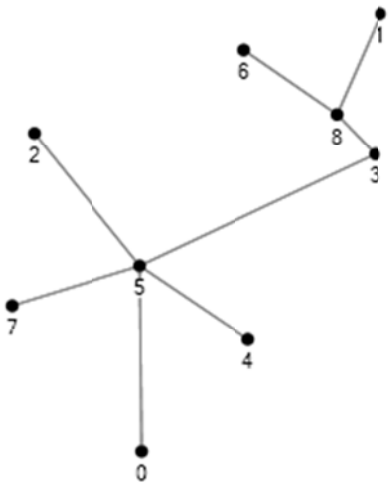


Figure 4-3 : Scale-free network 1

Both the attacker and the defender would determine how to allocate resources on

each node in each round. Both cyber attacker and network defender would consider different level of importance to each round, so the different weight of each round would be considered. In this model, four kinds of different weight in three rounds would be (1, 1, 1) (3, 0, 0) (0, 3, 0) and (0, 0, 3), respectively. (The notation of (a, b, c) means that the weight in the first round equals a, the weight in the second round equals b and the weight in the third round equals c.)

In this model, the policies of the defender are the node recovery, resource reallocation, resource recycle, defensive messaging, and vulnerabilities patch. On the other hand, the policy of the attacker is the vulnerabilities attack. Besides, both of the attacker and the defender also considered the accumulated experience.

The defender could use defensive messaging to increase defense efficiency. Therefore, we would discuss two kinds of situations of defensive messaging how to affect the attack success probability in the following.

The first kind of situation of defensive messaging was dividing a node's information into some parts and according to the importance of different part to release messages by the defender. In this kind of situation of defensive messaging, a node's attack success probability would different due to the attacker knowing different degree

of the node's information. When the defender chose doing nothing at all to the information on the node, as long as the attacker was willing to pay his resources to collect information and he would get truthful information about the node. When the defender chose truthful message to the information on the node, the attacker would get truthful information about the node. When the defender chose deceptive message to the information on the node, the attacker would not get truthful information about the node. When the defender chose secrecy to the information on the node, the probability which the attacker would get truthful information about the node was 0.2. Besides, we considered that this kind of situation of defensive messaging would only affect the half attack success probability of a node. As a result, the attack success probability of a node would be

$$S_{ri} = S_{ri} \times \frac{1}{2}\left(1 + \frac{n_{ri}}{N_{ri}}\right)$$

Table 4-1 : The parameter of calculating the attack success probability of the first kind of situation of defensive messaging

Notation	***Description***
S_{ri}	The attack success probability of node *i* in round *r*
N_{ri}	The number of total information on node *i* in round *r*
n_{ri}	The number of information the attacker knows on node *i* in round *r*

The second kind of situation of defensive messaging was using a node's defensive state as a message and releasing to the attacker. In this kind of situation of defensive messaging, we considered that the defender would get different benefit due to the defender choosing different message for a node. As a result, the attack success probability of a node would be

$$S_{ri} = \sum_{m} \left(\frac{T_{ri}}{T_{ri} + t_{ri} \times BF_{mi}} \times p_{mri} \right)$$

Table 4-2 : The parameter of calculating the attack success probability of the second kind of situation of defensive messaging

Notation	***Description***
S_{ri}	The attack success probability of node *i* in round *r*
T_{ri}	The attack resource allocated on node *i* in round *r*
t_{ri}	The defensive resource allocated on node *i* in round *r*
BF_{mi}	*m* = 0,1, 2 and 3 represent the defensive benefit of defender doing nothing at all, using truthful, secrecy, deceptive message on node *i* in round *r* respectively
p_{mri}	*m* = 0,1, 2 and 3 represent the probability of defender doing nothing at all, using truthful, secrecy, deceptive message on node *i* in round *r* respectively, which falls in (0,1)

The parameters used in the experiments are shown in Table 4-3.

Table 4-3 : Experiment parameters settings

Parameters	***Value***
Test Platform	1. CPU ： AMD Phenom(tm) IIX4 B40 Processor 3.00 GHz 2. RAM：6GB 3. OS：MS Windows 7
Network Topology	1. Grid (Figure 4-1) 2. Random 1 (Figure 4-2) 3. Scale-free 1 (Figure 4-3)
Contest intensity	1
The number of total rounds	3

The number of total nodes	9
The number of nodes the attacker knows initially	4
The number of link	8~12
The number of O-D pair	36 (considering all OD pairs)
The total resource of both players	36
The cost of doing nothing at all and the cost of defensive messaging of truth, secrecy, deception respectively	0, 0.25, 0.75, 1.5

There are lots of different kinds of policy that the attacker and defender could take, so there are lots of different kinds of attack-defense situations taking place. Therefore, some experiments would be taken in the following.

4.2 The Experiments of Same Weight in Three Rounds

In this experiment, we considered the weight in three rounds would be (1, 1, 1). The experiment results would be demonstrated in the following.

4.2.1 The Experiments of Incomplete Information

The solution approach would be used to solve this problem. There are ten different kinds of resource allocation strategy in three rounds for both cyber attacker and network defender in this experiment. The gradient method would be used to calculate the final Average DOD vale in 100 different payoff values. Therefore, the results would be demonstrated in the following.

4.2.1.1 The Results of the First Kind of Situation of Defensive Messaging

The results of grid network would be demonstrated in the Table 4-4.

Table 4-4 : The results of the incomplete information experiment under the first kind of defensive messaging (grid network)

Grid network												
Strategy		Attacker										
		(0, 0, 1)	**(0, 0.3, 0.7)**	**(0, 0.6, 0.4)**	**(0, 1, 0)**	**(0.3, 0, 0.7)**	**(0.33, 0.33, 0.33)**	**(0.3, 0.6, 0.1)**	**(0.6, 0, 0.4)**	**(0.6, 0.3, 0.1)**	**(1, 0, 0)**	**MAX**
Defender	**(0, 0, 1)**	0.32	1.94	1.87	1.55	2.94	4.56	4.46	2.87	4.34	2.53	4.56
	(0, 0.3, 0.7)	0.27	0.89	0.59	0.52	1.97	2.56	3.21	2.82	3.32	2.42	3.32
	(0, 0.6, 0.4)	0.29	0.75	0.84	0.63	1.73	2.13	2.2	2.16	2.38	2.23	2.38
	(0, 1, 0)	0.31	0.69	0.94	0.73	1.78	1.73	1.86	1.89	1.84	1.95	1.95
	(0.3, 0, 0.7)	0.27	0.92	0.72	0.57	1.83	1.76	2.23	2.04	2.77	0.89	2.77
	(0.33, 0.33, 0.33)	0.29	0.85	0.66	0.51	1.02	1.37	1.29	0.77	0.76	0.72	**1.37**
	(0.3, 0.6, 0.1)	0.4	0.61	0.93	0.59	0.99	0.88	1.64	1.29	1.53	0.71	1.64
	(0.6, 0, 0.4)	0.3	0.68	0.56	0.59	0.94	1.74	1.62	1.82	2.57	0.73	2.57
	(0.6, 0.3, 0.1)	0.32	0.78	0.89	0.56	0.78	1	1.14	1.06	1.47	0.71	1.47
	(1, 0, 0)	0.35	0.78	1.02	0.55	0.72	1.13	1.31	1.12	1.7	1.47	1.7
	MIN	0.27	0.61	0.56	0.51	0.72	0.88	**1.14**	0.77	0.76	0.71	

The game theory would be adopted to find the optimal resource allocation strategy for both cyber attacker and network defender. According to the solution procedure of game theory, the dominant strategy eliminating method and min-max method could not be used to find the optimal resource allocation strategy for both cyber attacker and network defender in this experiment. Therefore, the mixed strategy would be adopted to find the optimal percentage resource allocation strategy for both cyber attacker and network defender. The optimal solution of the probability of each strategy that the attacker would take is {(0.3, 0.6, 0.1), (0.6, 0.3, 0.1)}={(0.83, 0.17)}. In addition, the optimal solution of the probability of each strategy that the defender would take is {(0.6, 0.3, 0.1), (0.33, 0.33, 0.33)}={(0.62, 0.38)}. The final average DOD value was 1.2.

- Discussion of Results

  Because the weight in three rounds was the same and this experiment was incomplete information, both the attacker and the defender would choose to allocate resources in three rounds. However, the first kind of situation of defensive messaging could aim at different information on a node to release messages. So, the protective effect was stronger than the

second kind of situation of defensive messaging. Hence, the attacker would choose to allocate some resources in the first round to collect information, and allocate more resources in the second round to attack. In the view of the defender, in order to reduce the information which the attacker could collect the defender would choose to allocate more resources in the first round to reduce the damage.

The results of random network 1 would be demonstrated in the Table 4-5.

Table 4-5 : The results of the incomplete information experiment under the first kind of defensive messaging (random network 1)

Random network 1												
Strategy		Attacker										
		(0, 0, 1)	**(0, 0.3, 0.7)**	**(0, 0.6, 0.4)**	**(0, 1, 0)**	**(0.3, 0, 0.7)**	**(0.33, 0.33, 0.33)**	**(0.3, 0.6, 0.1)**	**(0.6, 0, 0.4)**	**(0.6, 0.3, 0.1)**	**(1, 0, 0)**	**MAX**
Defender	**(0, 0, 1)**	0.34	2.49	2.28	1.91	3.73	5.65	5.55	3.52	5.4	3.1	5.65
	(0, 0.3, 0.7)	0.35	1.29	0.85	0.75	2.56	3.29	3.63	3.49	4.08	3.03	4.08
	(0, 0.6, 0.4)	0.37	0.86	1.13	0.62	2.11	2.63	3.14	2.56	2.93	2.7	3.14
	(0, 1, 0)	0.41	0.86	1.09	0.99	2.27	2.31	2.36	2.56	2.31	2.32	2.56
	(0.3, 0, 0.7)	0.36	0.91	0.96	0.72	2.25	2.54	3.03	1.39	1.85	1.1	3.03
	(0.33, 0.33, 0.33)	0.39	0.94	1.19	0.67	1.45	1.83	1.91	0.96	1.17	0.99	**1.91**
	(0.3, 0.6, 0.1)	0.4	0.83	1.01	0.73	1.22	1.14	1.96	0.94	1.69	0.94	1.96
	(0.6, 0, 0.4)	0.39	1.04	0.72	0.68	1.1	2.32	1.93	2.13	3.16	0.86	3.16
	(0.6, 0.3, 0.1)	0.42	1.08	1.29	0.67	0.99	1.29	1.43	1.51	1.91	0.83	1.91
	(1, 0, 0)	0.45	1.13	1.64	0.64	0.99	1.52	1.95	1.26	1.8	1.72	1.95
	MIN	0.34	0.83	0.72	0.62	0.99	1.14	**1.43**	0.94	1.17	0.83	

Because this experiment could not find pure strategy, the mixed strategy would be adopted to find the optimal percentage resource allocation strategy for both cyber attacker and network defender. The optimal solution of the probability of each strategy that the attacker would take is {(0.3, 0.6, 0.1), (0.6, 0.3, 0.1)}={(0.61, 0.39)}. In addition, the optimal solution of the probability of each strategy that the defender would take is {(0.6, 0.3, 0.1), (0.33, 0.33, 0.33)}={(0.61, 0.39)}. The final average DOD value was 1.62.

- Discussion of Results

  Because the weight in three rounds was the same and this experiment was incomplete information, both the attacker and the defender would choose to allocate resources in three rounds. However, the first kind of situation of defensive messaging could aim at different information on a node to release messages. So, the protective effect was stronger than the second kind of situation of defensive messaging. Hence, the attacker would choose to allocate some resources in the first round to collect information, and allocate more resources in the second round to attack. Because the distribution of important nodes was random and scattered in

random network 1, local nodes damage would cause network fragmentation. In the view of the defender, in order to avoid the network would become fragmentation the defender would choose to allocate more resources in the first round. Moreover, in order to enhance the survivability in remaining rounds, the defender would allocate resources in these rounds.

The results of scale-free network 1 would be demonstrated in the Table 4-6.

Table 4-6 : The results of the incomplete information experiment under the first kind of defensive messaging (scale-free network 1)

Scale-free network 1												
Strategy		Attacker										
		(0, 0, 1)	**(0, 0.3, 0.7)**	**(0, 0.6, 0.4)**	**(0, 1, 0)**	**(0.3, 0, 0.7)**	**(0.33, 0.33, 0.33)**	**(0.3, 0.6, 0.1)**	**(0.6, 0, 0.4)**	**(0.6, 0.3, 0.1)**	**(1, 0, 0)**	**MAX**
Defender	**(0, 0, 1)**	0.23	1.74	1.7	1.33	2.68	4.81	4.44	2.56	4.31	2.15	4.81
	(0, 0.3, 0.7)	0.25	0.96	0.64	0.47	1.75	3.18	3.24	2.57	3.02	2.17	3.24
	(0, 0.6, 0.4)	0.26	0.68	0.82	0.45	1.5	2.4	2.69	1.78	2.66	1.93	2.69
	(0, 1, 0)	0.29	0.74	1.15	0.67	1.78	1.57	1.84	1.78	1.9	1.68	1.9
	(0.3, 0, 0.7)	0.25	0.69	0.58	0.51	1.85	2.11	2.82	0.99	1.44	0.65	2.82
	(0.33, 0.33, 0.33)	0.27	0.79	1.03	0.46	0.92	1.57	1.59	0.7	0.96	0.58	**1.59**
	(0.3, 0.6, 0.1)	0.29	0.68	0.87	0.47	0.91	0.82	1.81	0.69	0.82	0.58	1.81
	(0.6, 0, 0.4)	0.27	0.66	0.81	0.5	0.76	1.87	1.75	1.81	3.1	0.61	3.1
	(0.6, 0.3, 0.1)	0.29	0.7	0.93	0.46	0.77	0.89	1.22	1.15	1.73	0.65	1.73
	(1, 0, 0)	0.32	0.84	1.03	0.51	0.76	1.25	1.56	1.11	1.94	1.34	1.94
	MIN	0.23	0.66	0.58	0.45	0.76	0.82	**1.22**	0.69	0.82	0.58	

Because this experiment could not find pure strategy, the mixed strategy would be adopted to find the optimal percentage resource allocation strategy for both cyber attacker and network defender. The optimal solution of the probability of each strategy that the attacker would take is {(0.3, 0.6, 0.1), (0.6, 0.3, 0.1)}={(0.68, 0.32)}. In addition, the optimal solution of the probability of each strategy that the defender would take is {(0.6, 0.3, 0.1), (0.33, 0.33, 0.33)}={(0.55, 0.45)}. The final average DOD value was 1.39.

- Discussion of Results

  Because the weight in three rounds was the same and this experiment was incomplete information, both the attacker and the defender would choose to allocate resources in three rounds. However, the first kind of situation of defensive messaging could aim at different information on a node to release messages. So, the protective effect was stronger than the second kind of situation of defensive messaging. Hence, the attacker would choose to allocate some resources in the first round to collect information, and allocate more resources in the second round to attack. Because the core nodes damage in scale-free network 1 would cause

network fragmentation, in order to avoid the network would become fragmentation the defender would choose to allocate more resources in the first round. Moreover, in order to enhance the survivability in remaining rounds, the defender would allocate resources in these rounds.

4.2.1.2 The Results of the Second Kind of Situation of Defensive Messaging

The results of grid network would be demonstrated in the Table 4-7 and Figure 4-4.

Table 4-7 : The results of the incomplete information experiment under the second kind of defensive messaging (grid network)

Grid network												
Strategy		Attacker										
		(0, 0, 1)	**(0, 0.3, 0.7)**	**(0, 0.6, 0.4)**	**(0, 1, 0)**	**(0.3, 0, 0.7)**	**(0.33, 0.33, 0.33)**	**(0.3, 0.6, 0.1)**	**(0.6, 0, 0.4)**	**(0.6, 0.3, 0.1)**	**(1, 0, 0)**	**MAX**
Defender	**(0, 0, 1)**	0.64	1.87	1.72	1.52	2.89	4.02	3.91	2.64	3.89	2.5	4.02
	(0, 0.3, 0.7)	0.65	1.06	1.25	1.16	1.98	2.8	3.18	2.5	3.12	2.23	3.18
	(0, 0.6, 0.4)	0.65	0.78	1.12	1	1.87	1.91	2.3	1.94	2.31	2.01	2.31
	(0, 1, 0)	0.63	0.82	1.21	1.41	1.96	1.52	1.83	1.88	1.73	1.89	1.96
	(0.3, 0, 0.7)	0.65	0.91	1.44	1.34	1.96	2.29	2.58	2.27	2.88	1.96	2.88
	(0.33, 0.33, 0.33)	0.6	0.81	1.16	1.14	1.03	1.52	1.54	1.57	1.59	1.76	1.76
	(0.3, 0.6, 0.1)	0.64	0.74	1.02	1.33	1.08	1.14	1.46	1.53	1.65	1.69	1.69
	(0.6, 0, 0.4)	0.6	0.63	1.24	1.29	0.93	1.52	1.48	1.62	2.2	1.59	2.2
	(0.6, 0.3, 0.1)	0.6	0.73	1.21	1.29	0.79	0.99	1.13	1.32	1.42	**1.55**	1.55
	(1, 0, 0)	0.64	0.84	1.35	1.39	0.73	0.98	1.21	1.09	1.6	2.17	2.17
	MIN	0.6	0.63	1.02	1	0.73	0.98	1.13	1.09	1.42	1.55	

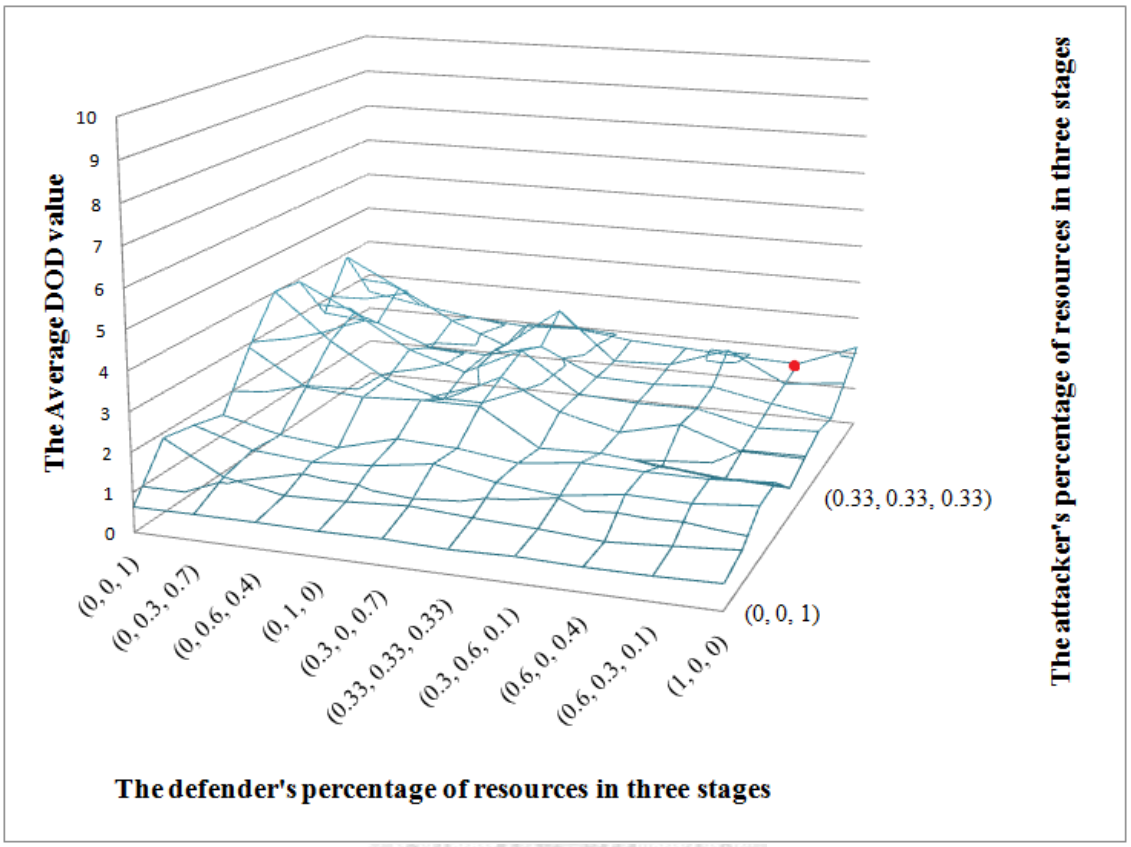


Figure 4-4 : The results of the incomplete information experiment under the second kind of defensive messaging (grid network)

The optimal percentage resource allocation strategy in three rounds in this experiment for both cyber attacker and network defender would be (1, 0, 0) and (0.6, 0.3, 0.1), respectively. The final average DOD value was 1.55.

- Discussion of Results

  Because this experiment was incomplete information and the protective effect of the second kind of defensive messaging was weaker than the

first, the attacker would choose to allocate more resources in the first round to attack. Hence, the attacker could use system vulnerability attack in the first round to prevent the defender patching. In the view of the defender, he would choose to allocate more resources in the first round to reduce damage. Moreover, in order to enhance the survivability in remaining rounds, the defender would allocate resources in these rounds.

The results of random network 1 would be demonstrated in the Table 4-8.

Table 4-8 : The results of the incomplete information experiment under the second kind of defensive messaging (random network 1)

Random network 1												
Strategy		Attacker										
		(0, 0, 1)	**(0, 0.3, 0.7)**	**(0, 0.6, 0.4)**	**(0, 1, 0)**	**(0.3, 0, 0.7)**	**(0.33, 0.33, 0.33)**	**(0.3, 0.6, 0.1)**	**(0.6, 0, 0.4)**	**(0.6, 0.3, 0.1)**	**(1, 0, 0)**	**MAX**
Defender	**(0, 0, 1)**	0.81	2.41	2.24	1.95	3.6	5.02	5	3.36	4.96	3.05	5.02
	(0, 0.3, 0.7)	0.76	1.38	1.64	1.6	2.56	3.78	4.58	3.18	4.16	2.89	4.58
	(0, 0.6, 0.4)	0.81	0.96	1.54	1.4	2.41	2.52	3.22	2.56	2.9	2.44	3.22
	(0, 1, 0)	0.83	1.11	1.43	1.78	2.4	1.96	2.3	2.56	2.21	2.31	2.56
	(0.3, 0, 0.7)	0.76	1.45	2.02	1.78	2.34	3.05	3.35	2.55	3.48	2.36	3.48
	(0.33, 0.33, 0.33)	0.83	1.06	1.74	1.64	1.79	1.94	2.26	1.87	2.56	2.44	2.56
	(0.3, 0.6, 0.1)	0.82	1	1.23	1.57	1.41	1.65	1.96	1.74	2.14	2.19	2.19
	(0.6, 0, 0.4)	0.77	1.18	1.64	1.56	1.19	1.99	1.79	2.34	3.07	2.24	3.07
	(0.6, 0.3, 0.1)	0.82	1.12	1.45	1.61	1.01	1.32	1.47	1.75	2.11	2.06	**2.11**
	(1, 0, 0)	0.83	1.06	1.69	1.61	0.95	1.23	1.55	1.23	1.84	2.98	2.98
	MIN	0.76	0.96	1.23	1.4	0.95	1.23	1.47	1.23	1.84	**2.06**	

Because this experiment could not find pure strategy, the mixed strategy would be adopted to find the optimal percentage resource allocation strategy for both cyber attacker and network defender. The optimal solution of the probability of each strategy that the attacker would take is {(0.6, 0.3, 0.1), (1, 0, 0)}={(0.77, 0.23)}. In addition, the optimal solution of the probability of each strategy that the defender would take is {(0.6, 0.3, 0.1), (1, 0, 0)}={(0.96, 0.04)}. The final average DOD value was 2.1.

- Discussion of Results

  Because the protective effect of the second kind of defensive messaging was weaker than the first and local nodes damage would cause network fragmentation in random network 1, the attacker would choose to allocate more resources in the first round to attack. In the view of the defender, in order to avoid the network would become fragmentation the defender would choose to allocate more resources in the first round. Moreover, in order to enhance the survivability in remaining rounds, the defender would allocate resources in these rounds.

The results of scale-free network 1 would be demonstrated in the Table 4-9.

Table 4-9 : The results of the incomplete information experiment under the second kind of defensive messaging (scale-free network 1)

Scale-free network 1												
Strategy		Attacker										
		(0, 0, 1)	**(0, 0.3, 0.7)**	**(0, 0.6, 0.4)**	**(0, 1, 0)**	**(0.3, 0, 0.7)**	**(0.33, 0.33, 0.33)**	**(0.3, 0.6, 0.1)**	**(0.6, 0, 0.4)**	**(0.6, 0.3, 0.1)**	**(1, 0, 0)**	**MAX**
Defender	**(0, 0, 1)**	0.58	1.75	1.7	1.34	2.64	4.24	4.03	2.49	3.9	2.06	4.24
	(0, 0.3, 0.7)	0.56	1.08	1.23	1.04	1.99	3.41	3.72	2.36	3.12	2	3.72
	(0, 0.6, 0.4)	0.55	0.78	1.16	0.89	1.71	2.22	2.74	1.84	2.65	1.74	2.74
	(0, 1, 0)	0.52	0.92	1.41	1.24	1.78	1.44	1.86	1.78	1.9	1.76	1.9
	(0.3, 0, 0.7)	0.52	1.02	1.35	1.2	1.93	2.68	2.95	1.82	2.78	1.56	2.95
	(0.33, 0.33, 0.33)	0.52	0.85	1.28	0.92	1.15	1.78	2.02	1.35	2.04	1.58	2.04
	(0.3, 0.6, 0.1)	0.52	0.72	1	1.02	1.05	1.12	1.69	1.24	1.82	1.49	**1.82**
	(0.6, 0, 0.4)	0.52	0.71	1.15	1.1	0.69	1.69	1.61	1.67	2.68	1.4	2.68
	(0.6, 0.3, 0.1)	0.52	0.69	1.11	0.97	0.9	0.9	1.28	1.28	1.84	1.36	1.84
	(1, 0, 0)	0.57	0.86	1.31	1.06	0.69	1.09	1.29	0.97	1.75	1.88	1.88
	MIN	0.52	0.69	1	0.89	0.69	0.9	1.28	0.97	**1.75**	1.36	

Because this experiment could not find pure strategy, the mixed strategy would be adopted to find the optimal percentage resource allocation strategy for both cyber attacker and network defender. The optimal solution of the probability of each strategy that the attacker would take is {(0.6, 0.3, 0.1), (1, 0, 0)}={(0.85, 0.15)}. In addition, the optimal solution of the probability of each strategy that the defender would take is {(1, 0, 0), (0.6, 0.3, 0.1)}={(0.79, 0.21)}. The final average DOD value was 1.77.

- Discussion of Results

  Because the protective effect of the second kind of defensive messaging was weaker than the first and the core nodes damage in scale-free network 1 would cause network fragmentation, the attacker would choose to allocate more resources in the first round to attack. Moreover, the attacker would allocate some resources in remaining rounds to attack the nodes which were explored by the attacker after the first round. In order to avoid the network would become fragmentation after the first round, the defender would choose to allocate more resources in the first round.

4.2.1.3 Comparing the Results of Three Different Kinds of Network Topology

To compare three different kinds of network topology in these two kinds of defensive messaging as shown in Figure 4-5, the average DOD value in grid network was lower than random 1 and scale-free 1, respectively. Also, the average DOD value in scale-free network 1 was lower than random 1. Because the weight in three rounds was the same, the attacker had sufficient time to collect information to attack. Besides, the distribution of important nodes was random and scattered in random network 1, so local nodes damage would cause network fragmentation which let the average DOD value was higher than the others. Moreover, the core nodes in scale-free network 1 would not be explored easily under incomplete information, so the average DOD value was lower than random network 1. The distribution of important nodes was even in grid network, so comparing to random 1 and scale-free network 1 it would not become islands easily.

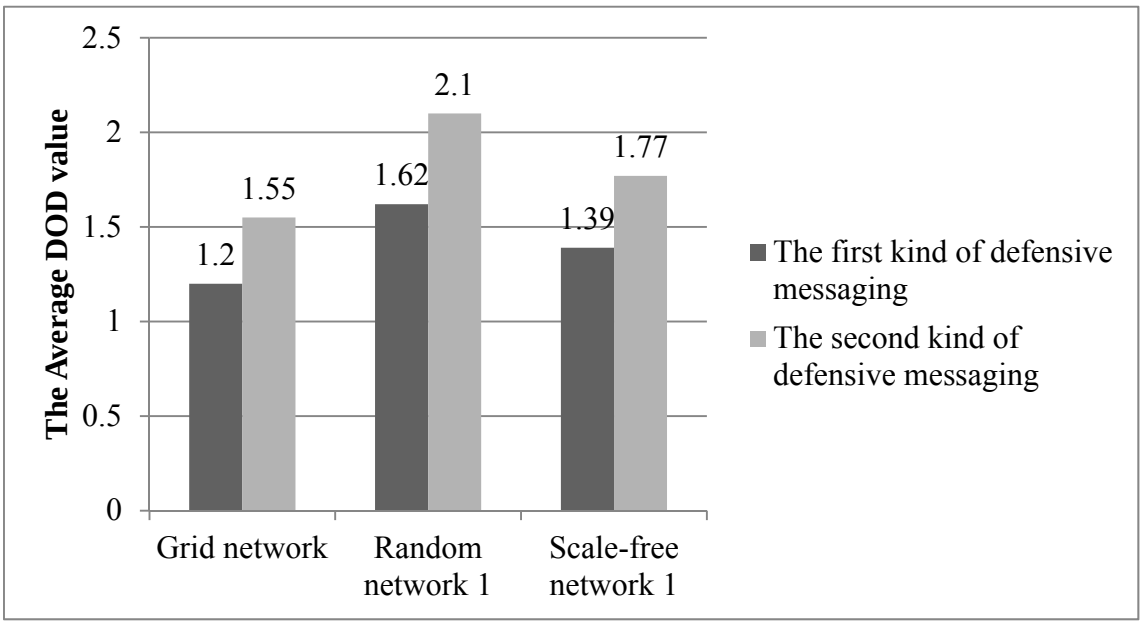


Figure 4-5 : Comparing the results of three different kinds of networks in incomplete information experiments

4.2.1.4 Comparing the Results of Two Different Kinds of Defensive Messaging

Because the first kind of situation of defensive messaging could aim at different information on a node to release messages, the protective effect was stronger than the second kind of situation of defensive messaging. Therefore, the average DOD values of the second kind of defensive messaging were higher than the first kind in three different kinds of networks as shown in Figure 4-5.

4.2.2 The Experiments of Complete Information

In order to compare with the incomplete information experiments, in this experiments we considered complete information between the attacker and the defender. Because the experiments would be complete information, the defender would not need to consider defensive messaging.

The solution approach would be used to solve this problem. There are ten different kinds of resource allocation strategy in three rounds for both cyber attacker and network defender in this experiment. The gradient method would be used to calculate the final Average DOD vale in 100 different payoff values. Therefore, the results would be demonstrated in the following.

The results of grid network would be demonstrated in the Table 4-10.

Table 4-10 : The results of the complete information experiment (grid network)

Grid network												
Strategy		Attacker										
		(0, 0, 1)	**(0, 0.3, 0.7)**	**(0, 0.6, 0.4)**	**(0, 1, 0)**	**(0.3, 0, 0.7)**	**(0.33, 0.33, 0.33)**	**(0.3, 0.6, 0.1)**	**(0.6, 0, 0.4)**	**(0.6, 0.3, 0.1)**	**(1, 0, 0)**	**MAX**
Defender	**(0, 0, 1)**	0.52	1.72	1.7	1.67	2.84	2.82	2.8	2.81	2.78	2.75	2.84
	(0, 0.3, 0.7)	0.55	1.08	1.17	1.3	2.17	2.75	2.7	2.7	2.67	2.63	2.75
	(0, 0.6, 0.4)	0.58	0.78	1.02	1.07	1.89	2.35	2.42	2.16	2.38	2.36	2.42
	(0, 1, 0)	0.64	0.68	0.79	1.04	1.87	1.98	2.04	1.96	2.02	2	2.04
	(0.3, 0, 0.7)	0.56	1.04	1.32	1.44	1.79	1.62	1.9	1.83	1.85	2.06	2.06
	(0.33, 0.33, 0.33)	0.61	0.81	1.11	1.14	1.28	1.69	1.6	1.41	1.57	1.84	1.84
	(0.3, 0.6, 0.1)	0.64	0.7	0.86	1.05	1.21	1.29	1.6	1.39	1.59	1.8	1.8
	(0.6, 0, 0.4)	0.61	0.86	1.05	1.25	0.95	1.21	1.24	1.53	1.54	1.52	1.54
	(0.6, 0.3, 0.1)	0.66	0.76	0.9	1.06	0.86	1.06	1.16	1.32	1.52	1.53	**1.53**
	(1, 0, 0)	0.71	0.8	1.14	1.13	0.8	1	1.13	0.99	1.22	1.62	1.62
	MIN	0.52	0.68	0.79	1.04	0.8	1	1.13	0.99	1.22	**1.52**	

Because this experiment could not find pure strategy, the mixed strategy would be adopted to find the optimal percentage resource allocation strategy for both cyber attacker and network defender. The optimal solution of the probability of each strategy that the attacker would take is {(1, 0, 0), (0.6, 0.3, 0.1)}={(0.76, 0.24)}. In addition, the optimal solution of the probability of each strategy that the defender would take is {(0.6, 0, 0.4), (1, 0, 0)}={(0.95, 0.05)}. The final average DOD value was 1.525.

- Discussion of Results

  In the complete information, the attacker would choose to allocate more resources in the first round to attack. Hence, the attacker could use system vulnerability attack in the first round to prevent the defender patching. In the view of the defender, he would choose to allocate more resources in the first round to reduce damage. Moreover, in order to enhance the survivability in remaining rounds, the defender would allocate resources in the third round.

The results of random network 1 would be demonstrated in the Table 4-11 and Figure 4-6.

Table 4-11 : The results of the complete information experiment (random network 1)

Random network 1												
Strategy		Attacker										
		(0, 0, 1)	**(0, 0.3, 0.7)**	**(0, 0.6, 0.4)**	**(0, 1, 0)**	**(0.3, 0, 0.7)**	**(0.33, 0.33, 0.33)**	**(0.3, 0.6, 0.1)**	**(0.6, 0, 0.4)**	**(0.6, 0.3, 0.1)**	**(1, 0, 0)**	**MAX**
Defender	**(0, 0, 1)**	0.81	2.61	2.58	2.54	3.86	3.86	3.86	3.86	3.86	3.86	3.86
	(0, 0.3, 0.7)	0.84	1.52	1.83	2.08	3.43	3.84	3.86	3.76	3.86	3.84	3.86
	(0, 0.6, 0.4)	0.89	1.21	1.48	1.57	3	3.49	3.7	3.29	3.65	3.64	3.7
	(0, 1, 0)	0.98	1.09	1.31	1.52	2.88	3.08	3.37	2.88	3.25	3.22	3.37
	(0.3, 0, 0.7)	0.86	1.75	2.1	2.23	2.24	2.52	2.53	2.82	2.92	3.31	3.31
	(0.33, 0.33, 0.33)	0.93	1.18	1.54	1.79	1.68	2.19	2.17	2.33	2.57	3.01	3.01
	(0.3, 0.6, 0.1)	0.98	1.13	1.32	1.58	1.74	2.06	2.1	2.17	2.5	2.88	2.88
	(0.6, 0, 0.4)	0.94	1.33	1.74	2	1.54	1.87	2.03	2.17	2.25	2.25	2.25
	(0.6, 0.3, 0.1)	1.01	1.17	1.63	1.7	1.43	1.68	1.76	2.01	2.13	**2.13**	2.13
	(1, 0, 0)	1.08	1.23	1.72	1.83	1.32	1.64	1.64	1.73	1.94	2.24	2.24
	MIN	0.81	1.09	1.31	1.52	1.32	1.64	1.64	1.73	1.94	2.13	

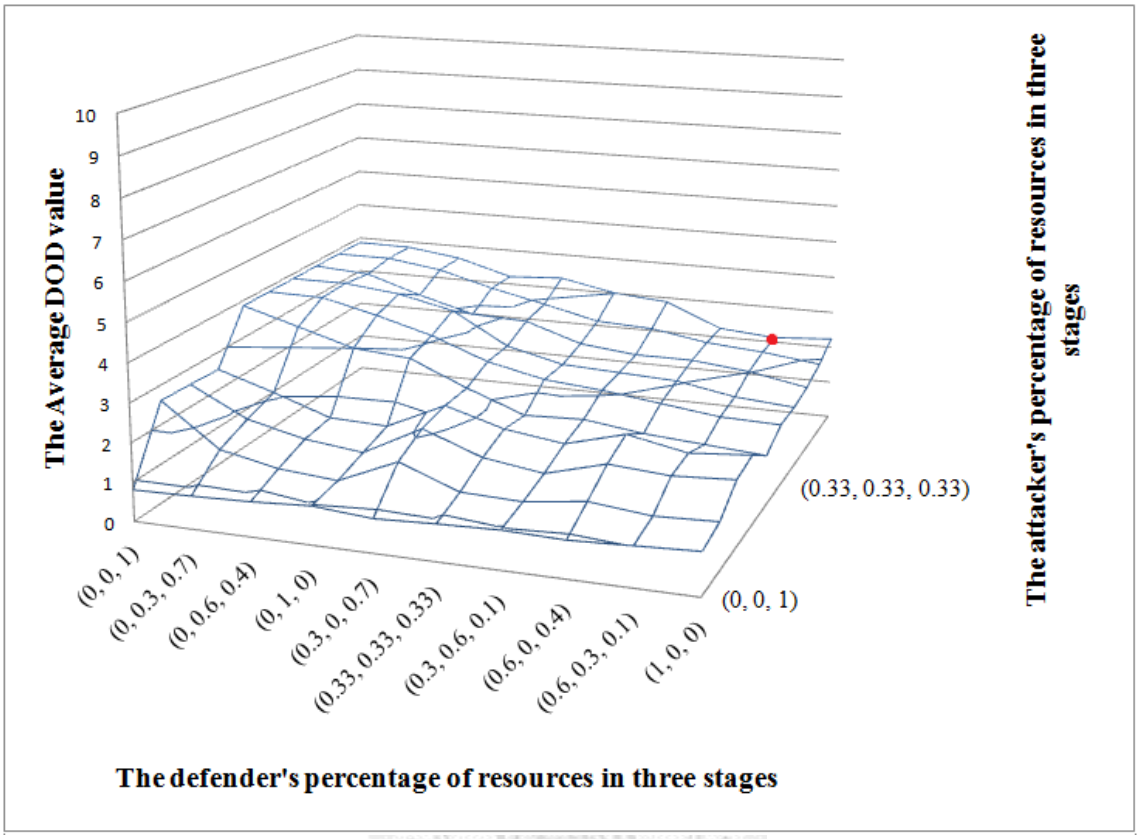


Figure 4-6 : The results of the complete information experiment (random network 1)

The optimal percentage resource allocation strategy in three rounds in this experiment for both cyber attacker and network defender would be (1, 0, 0) and (0.6, 0.3, 0.1), respectively. The final average DOD value was 2.13.

- Discussion of Results

  Because the distribution of important nodes was random and scattered in random network 1, local nodes damage would cause network

fragmentation. Therefore, the attacker would choose to allocate more resources in the first round to attack. In the view of the defender, he would choose to allocate more resources in the first round to reduce damage. Moreover, in order to enhance the survivability in remaining rounds, the defender would allocate resources in these rounds.

The results of scale-free network 1 would be demonstrated in the Table 4-12 and Figure 4-7.

Table 4-12 : The results of the complete information experiment (scale-free network 1)

Scale-free network 1												
Strategy		Attacker										
		(0, 0, 1)	**(0, 0.3, 0.7)**	**(0, 0.6, 0.4)**	**(0, 1, 0)**	**(0.3, 0, 0.7)**	**(0.33, 0.33, 0.33)**	**(0.3, 0.6, 0.1)**	**(0.6, 0, 0.4)**	**(0.6, 0.3, 0.1)**	**(1, 0, 0)**	**MAX**
Defender	**(0, 0, 1)**	0.87	2.87	2.84	2.8	4.76	4.72	4.7	4.71	4.67	4.62	4.76
	(0, 0.3, 0.7)	0.91	1.6	2.11	2.25	3.77	4.23	4.32	4.13	4.27	4.22	4.32
	(0, 0.6, 0.4)	0.96	1.28	1.58	1.89	3.16	3.8	4.16	3.59	4.11	4.06	4.16
	(0, 1, 0)	1.06	1.19	1.4	1.55	3.18	3.45	3.59	3.23	3.49	3.45	3.59
	(0.3, 0, 0.7)	0.93	1.85	2.31	2.43	2.32	2.66	2.66	3.3	3.46	3.59	3.59
	(0.33, 0.33, 0.33)	1	1.34	1.67	2.04	1.81	2.23	2.28	2.8	3.13	3.28	3.28
	(0.3, 0.6, 0.1)	1.06	1.23	1.49	1.7	1.83	2.13	2.19	2.63	2.94	3.08	3.08
	(0.6, 0, 0.4)	1.01	1.49	1.88	2.24	1.63	1.95	2.03	2.31	2.4	2.88	2.88
	(0.6, 0.3, 0.1)	1.09	1.22	1.74	1.83	1.49	1.72	1.83	2	2.19	2.68	2.68
	(1, 0, 0)	1.16	1.33	1.86	1.96	1.44	1.62	1.81	1.85	2.01	**2.14**	2.14
	MIN	0.87	1.19	1.4	1.55	1.44	1.62	1.81	1.85	2.01	2.14	

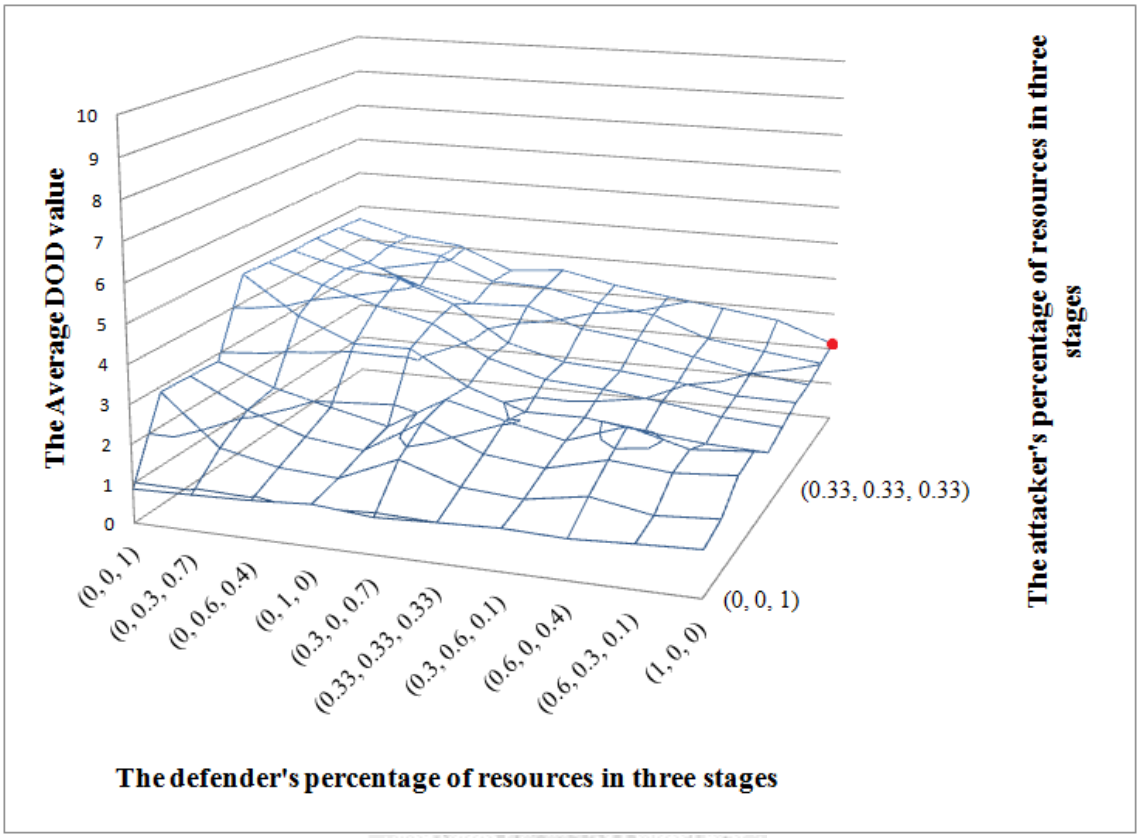


Figure 4-7 : The results of the complete information experiment (scale-free network 1)

The optimal percentage resource allocation strategy in three rounds in this experiment for both cyber attacker and network defender would be (1, 0, 0) and (1, 0, 0), respectively. The final average DOD value was 2.14.

- Discussion of Results

  Because the core nodes damage in scale-free network 1 would cause network fragmentation, both the attacker and the defender would choose

to allocate more resources in the first round.

4.2.2.1 Comparing the Results of Three Different Kinds of Network Topology

To compare three different kinds of network topology as shown in Figure 4-8, the average DOD value in grid network was lower than random 1 and scale-free 1, respectively. Also, the average DOD value in random network 1 was lower than scale-free 1. In complete information, because the core nodes damage in scale-free network 1 would cause network fragmentation, the nodes could not connect to each other which let the average DOD value was higher than the others. Besides, the distribution of important nodes was random and scattered in random network 1, so local nodes damage would cause network becoming several blocks which let the average DOD value was higher than grid network. Moreover, the distribution of important nodes was even in grid network, so comparing to random 1 and scale-free network 1 it would not become islands easily.

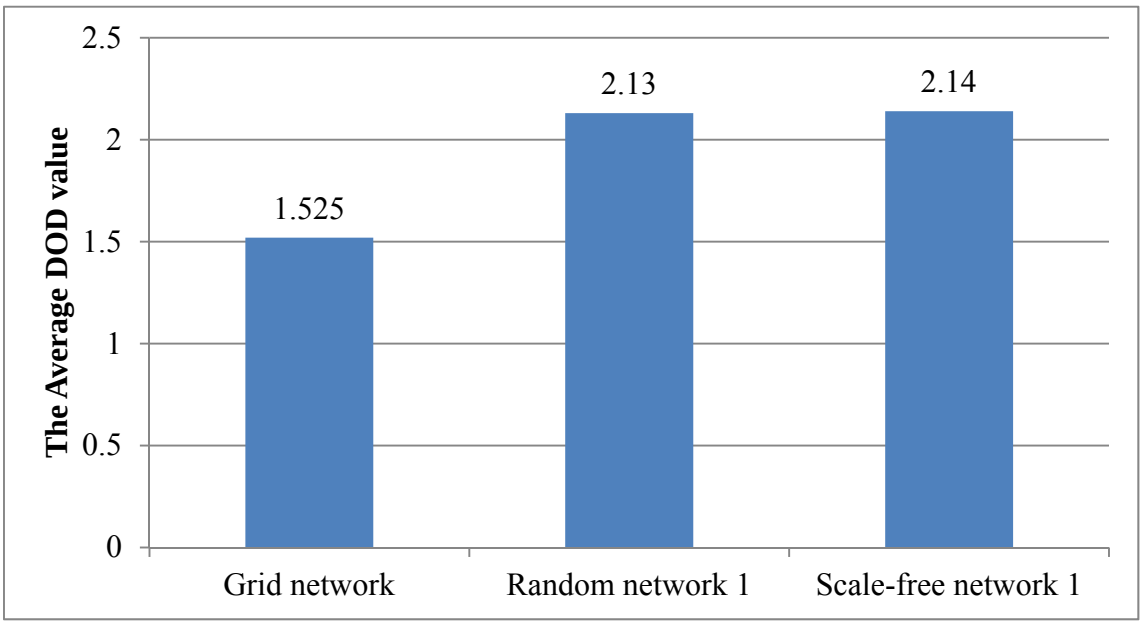


Figure 4-8 : Comparing the results of three different kinds of networks in complete information experiments

4.2.3 The Experiments of Considering High Availability System

In order to enhance the reliability of system, in this incomplete information experiment the important nodes having backup and the attacker having bounded rationality would be considered. The node's backup would quickly take over the work of the original node when the original node failed. The experiment results would be demonstrated in Table 4-13 and Table 4-14.

Table 4-13 : The results of considering high availability system under the first kind of defensive messaging

The first kind of defensive messaging			
Network Topology	Average DOD	Strategy of Attacker	Strategy of Defender
Grid	0.95	(0.3, 0.6, 0.1)	(0.6, 0.3, 0.1)
Random 1	1.265	(0.3, 0.6, 0.1)	(0.6, 0.3, 0.1)
Scale-free 1	1.06	(0.3, 0.6, 0.1)	(0.6, 0.3, 0.1)

Table 4-14 : The results of considering high availability system under the second kind of defensive messaging

The Second kind of defensive messaging			
Network Topology	Average DOD	Strategy of Attacker	Strategy of Defender
Grid	1.11	(0.6, 0, 0.4)	(0.6, 0.3, 0.1)
Random 1	1.57	(0.6, 0.3, 0.1)	(0.3, 0.6, 0.1)
Scale-free 1	1.19	(0.6, 0, 0.4)	(0.6, 0.3, 0.1)

4.2.3.1 Discussion of Results

To compare three different kinds of network topology in these two kinds of defensive messaging as shown in Figure 4-9, the average DOD value in grid network was lower than random 1 and scale-free 1, respectively. Also, the average DOD value in scale-free network 1 was lower than random 1. Because the weight in three rounds was

the same, the attacker had sufficient time to collect information to attack. Besides, the distribution of important nodes was random and scattered in random network 1, so local nodes damage would cause network fragmentation which let the average DOD value was higher than the others. Moreover, the core nodes in scale-free network 1 would not be explored easily under incomplete information, so the average DOD value was lower than random network 1. The distribution of important nodes was even in grid network, so comparing to random 1 and scale-free network 1 it would not become islands easily.

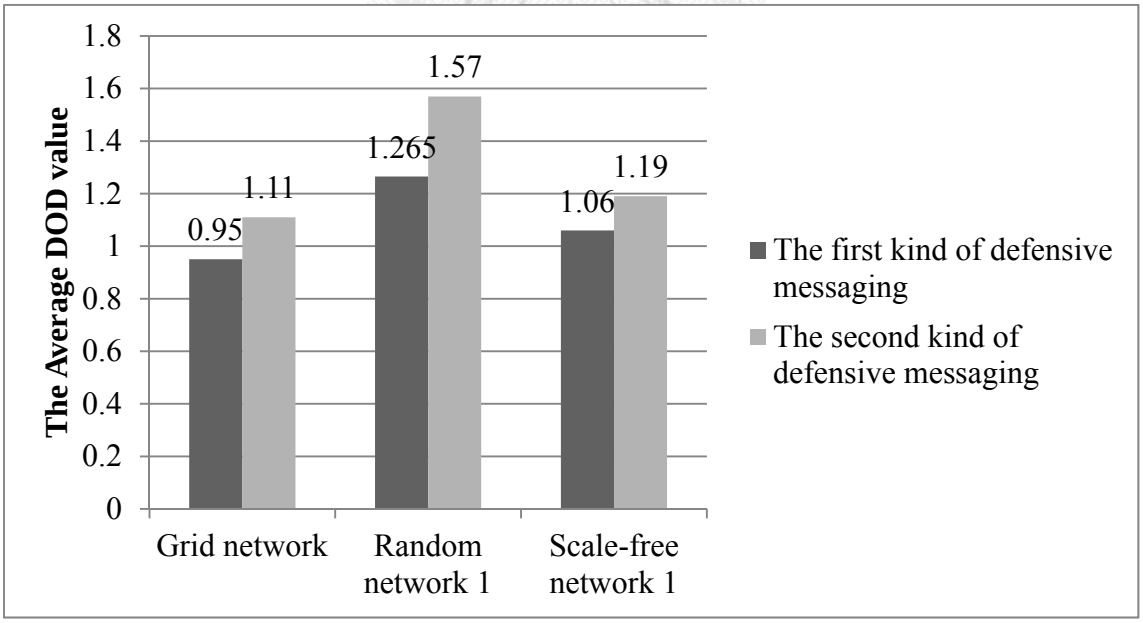


Figure 4-9 : Comparing the results of three different kinds of networks in considering high availability system

4.2.4 Experiments Comparison

In this series of experiments, different experiments would be compared in the following.

4.2.4.1 Comparing the Results of Incomplete Information with Complete Information

Comparing the results of incomplete information with complete information was shown in Figure 4-10. Basically, in the view of the attacker, complete information would be more advantageous than incomplete information. However, the average DOD value of the second kind of defensive messaging under incomplete information was higher than complete information. The distribution of important nodes was even in grid network. Under complete information though the attacker knew the important nodes and allocated a lot of resources on it, the attacker would not compromise the important nodes because of the defender would also allocate a lot of resources on it to protect. But, under incomplete information the attacker could only attack the nodes that he knew it. Besides, the protective effect of the second kind of defensive messaging was weaker than the first and in grid network the attacker explored nodes easier than the

others network. Therefore, the attacker could compromise some nodes in the grid network. Hence, the average DOD value of the second kind of defensive messaging under incomplete information was higher than complete information.

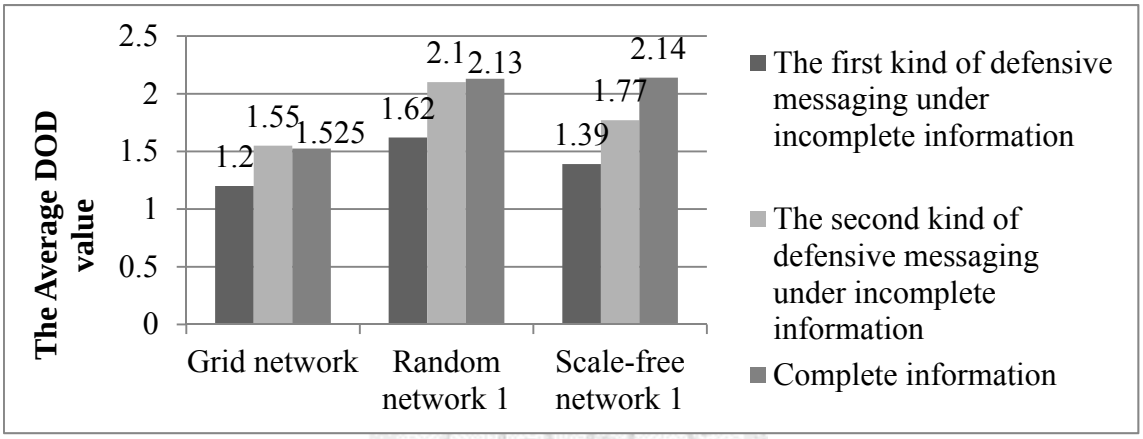


Figure 4-10 : Comparing the results of incomplete information with complete information

4.2.4.2 Comparing the Results of Considering High Availability System or not under Incomplete Information

Comparing the results of considering high availability system or not under incomplete information was shown in Figure 4-11 and Figure 4-12. The node's backup would quickly take over the work of the original node when the original node failed. Besides, in this experiment the attacker having bounded rationality would be

considered. Therefore, the damage caused by the attacker would be lower than full rationality. Hence, the average DOD value of considering high availability system would lower than without considering high availability system.

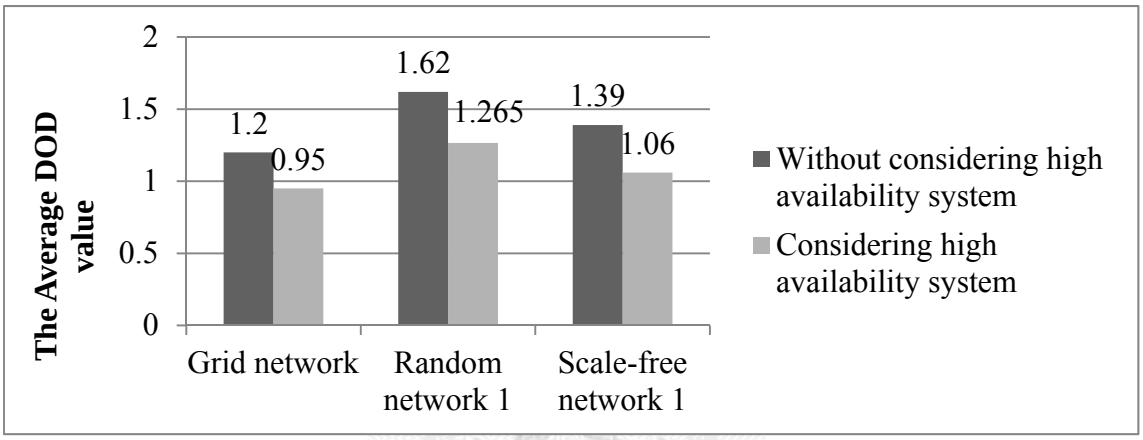


Figure 4-11 : Comparing the results of considering high availability system or not under incomplete information and the first kind of defensive messaging

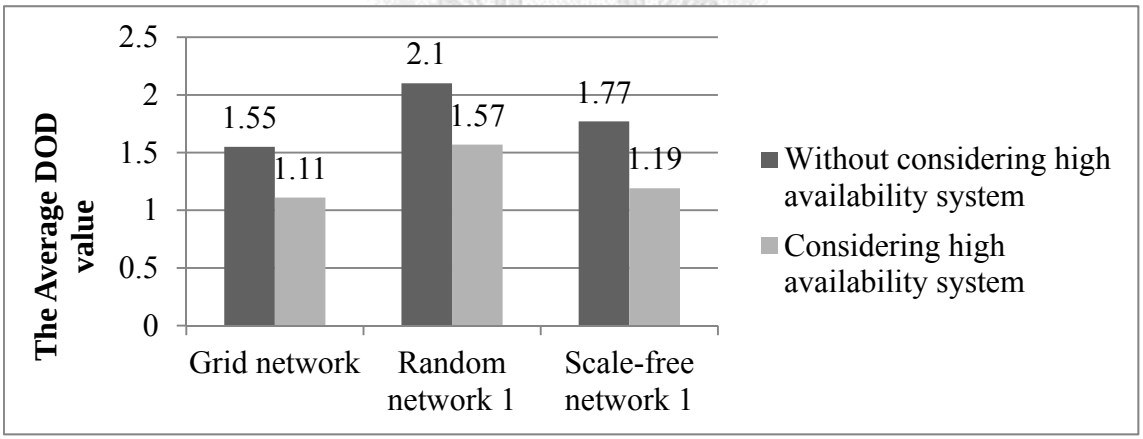


Figure 4-12 : Comparing the results of considering high availability system or not under incomplete information and the second kind of defensive messaging

4.3 The Experiments of Different Weight in Three Rounds

In reality, the importance of each round would not always be the same. Therefore, the experiment about the different weight in each round under incomplete information would be taken in the following.

4.3.1 Experiments Results

In these series of experiments, the weight (3, 0, 0) of three rounds would be considered to represent that the first round was the most important and the weight (0, 0, 3) of three rounds would be considered to represent that the final round was the most important. The experiment results would be demonstrated in Table 4-15, Table 4-16, Table 4-17 and Table 4-18.

Table 4-15 : The weight of the experiment is (3, 0, 0)

The first kind of defensive messaging			
Network Topology	Average DOD	Strategy of Attacker	Strategy of Defender
Grid	0.78	(1, 0, 0)	(1, 0, 0)
Random 1	1.01	(1, 0, 0)	(1, 0, 0)
Scale-free 1	0.72	(1, 0, 0)	(1, 0, 0)
The second kind of defensive messaging			
Grid	1.85	(1, 0, 0)	(0.6, 0, 0.4), (0.6, 0.3, 0.1)
Random 1	2.48	(1, 0, 0)	(1, 0, 0)
Scale-free 1	1.64	(1, 0, 0)	(0.6, 0, 0.4), (0.6, 0.3, 0.1)

Table 4-16 : The weight of the experiment is (0, 0, 3)

The first kind of defensive messaging			
Network Topology	Average DOD	Strategy of Attacker	Strategy of Defender
Grid	0.93	(0.6, 0, 0.4)	(0.3, 0, 0.7)
Random 1	1.15	(0, 0.3, 0.7)	(0.3, 0, 0.7)
Scale-free 1	0.8	(0, 0.6, 0.4)	(0.3, 0, 0.7)
The second kind of defensive messaging			
Grid	2.1	(0, 0.6, 0.4)	(0, 0.3, 0.7)
Random 1	2.72	(0.6, 0, 0.4)	(0, 0.6, 0.4)
Scale-free 1	2.09	(0.6, 0, 0.4)	(0.6, 0, 0.4)

Table 4-17 : The results of the weight (3, 0, 0) for the defender and the weight (1, 1, 1) for the attacker

The first kind of defensive messaging			
Network Topology	Average DOD	Strategy of Attacker	Strategy of Defender
Grid	0.9	(1, 0, 0)	(1, 0, 0)
Random 1	1.01	(1, 0, 0)	(1, 0, 0)
Scale-free 1	0.71	(1, 0, 0)	(1, 0, 0)
The second kind of defensive messaging			
Grid	1.85	(1, 0, 0)	(0.6, 0, 0.4), (0.6, 0.3, 0.1)
Random 1	2.48	(1, 0, 0)	(1, 0, 0)
Scale-free 1	1.64	(1, 0, 0)	(0.6, 0, 0.4), (0.6, 0.3, 0.1)

Table 4-18 : The results of the weight (0, 0, 3) for the defender and the weight (1, 1, 1) for the attacker

The first kind of defensive messaging			
Network Topology	Average DOD	Strategy of Attacker	Strategy of Defender
Grid	0.94	(0, 0, 1)	(0.3, 0.6, 0.1)
Random 1	1.31	(0, 0.6, 0.4)	(0.3, 0, 0.7)
Scale-free 1	0.84	(0, 0.6, 0.4)	(0.3, 0, 0.7)
The second kind of defensive messaging			
Grid	2.14	(0, 0.6, 0.4)	(0, 0.6, 0.4)

Random 1	2.77	(0.6, 0, 0.4)	(0, 0.6, 0.4)
Scale-free 1	2.08	(0.6, 0, 0.4)	(0.6, 0, 0.4)

4.3.2 Experiments Comparison

Comparing the experiment results of the weight (3, 0, 0) with (0, 0, 3) was shown in Figure 4-13 and Figure 4-14. In Figure 4-13 and Figure 4-14, the average DOD values of the weight (3, 0, 0) of three rounds in three kinds of networks were all lower than the weight (0, 0, 3).

Moreover, comparing the experiment results of the weight (3, 0, 0) with the weight (0, 0, 3) for the defender and the weight (1, 1, 1) for the attacker in three rounds was shown in Figure 4-15 and Figure 4-16. In Figure 4-15 and Figure 4-16, the average DOD values of the weight (3, 0, 0) for the defender in three kinds of networks were all lower than the weight (0, 0, 3) for the defender.

Therefore, in the view of the defender, to defend early would be more advantageous.

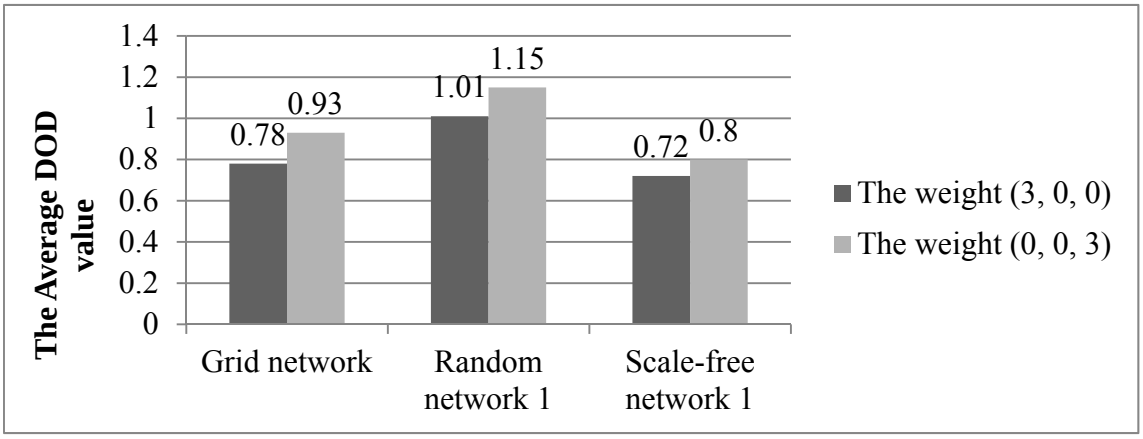


Figure 4-13 : Comparing the results of the weight (3, 0, 0) with (0, 0, 3) in three rounds under the first kind of defensive messaging

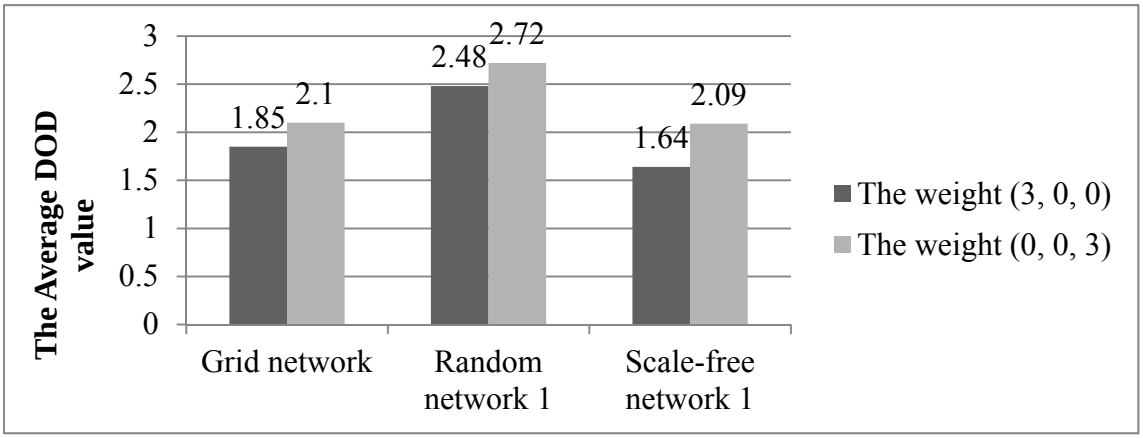


Figure 4-14 : Comparing the results of the weight (3, 0, 0) with (0, 0, 3) in three rounds under the second kind of defensive messaging

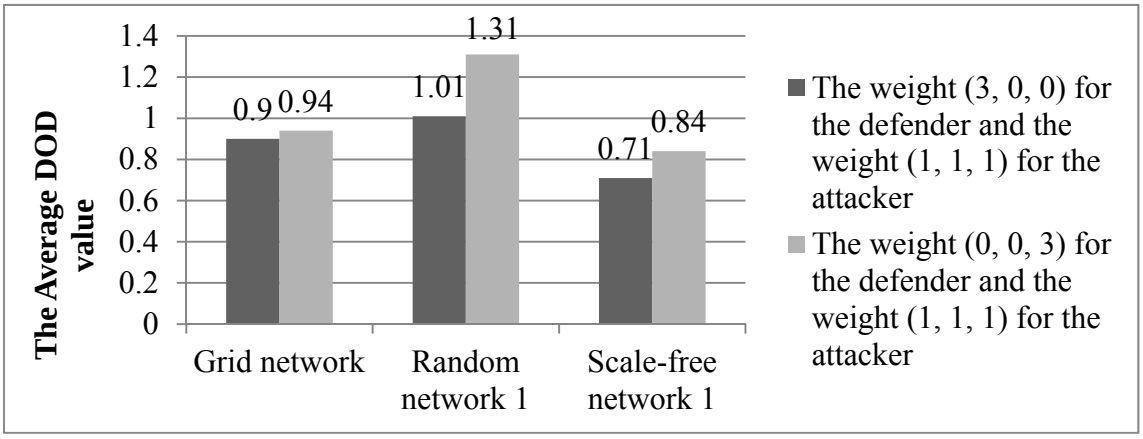


Figure 4-15 : Comparing the results of the weight (3, 0, 0) with (0, 0, 3) for the defender and the weight (1, 1, 1) for the attacker in three rounds under the first kind of defensive messaging

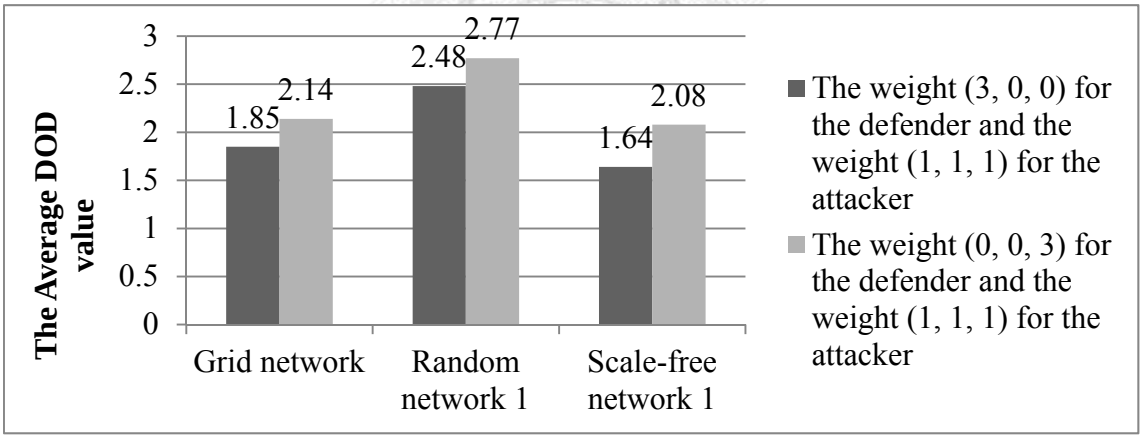


Figure 4-16 : Comparing the results of the weight (3, 0, 0) with (0, 0, 3) for the defender and the weight (1, 1, 1) for the attacker in three rounds under the second kind of defensive messaging

4.4 The Experiments of Different Total Resources

In reality, the total resources of the attacker and the total resources of the defender

would not always be the same. When the attacker was an organization, the total resources of the attacker would larger than the defender. When the attacker was just a person, the total resources of the attacker would smaller than the defender. Therefore, in these series of experiments, the defender and the attacker having different total resources under incomplete information and the weight (1, 1, 1) in three rounds would be considered.

4.4.1 The Experiments of the Defender Having More Total Resources

In this experiment, the attacker having fewer total resources would be considered and the total resources of the attacker would be 24. The experiment results would be demonstrated in Table 4-19.

Table 4-19 : The results of the defender having more total resources

The first kind of defensive messaging			
Network Topology	Average DOD	Strategy of Attacker	Strategy of Defender
Grid	0.84	(0.3, 0.6, 0.1)	(0.6, 0.3, 0.1)
Random 1	1.1	(0.3, 0.6, 0.1)	(0.6, 0.3, 0.1)
Scale-free 1	0.82	(0.3, 0.6, 0.1)	(0.6, 0.3, 0.1)

The second kind of defensive messaging			
Grid	0.99	(1, 0, 0)	(0.6, 0.3, 0.1)
Random 1	1.41	(1, 0, 0)	(0.6, 0.3, 0.1)
Scale-free 1	0.86	(1, 0, 0)	(0.6, 0.3, 0.1)

4.4.1.1 Discussion of Results

To compare three different kinds of network topology in these two kinds of defensive messaging as shown in Figure 4-17, the average DOD value in scale-free network 1 was lower than random 1 and grid, respectively. Also, the average DOD value in grid network was lower than random 1. Though the weight in three rounds was the same and the attacker had sufficient time to collect information to attack, the defender having more total resources could reduce the information that the attacker could explore. Moreover, the defender having more total resources could also reduce the damage which caused by the attacker. The distribution of important nodes was random and scattered in random network 1, so local nodes damage would cause network fragmentation which let the average DOD value was higher than the others. The distribution of important nodes was even in grid network, so comparing to random network 1 it would not become islands easily. The core nodes in scale-free network 1

would not be explored easily under the defender having more total resources, so the average DOD value was lower than random 1 and grid network.

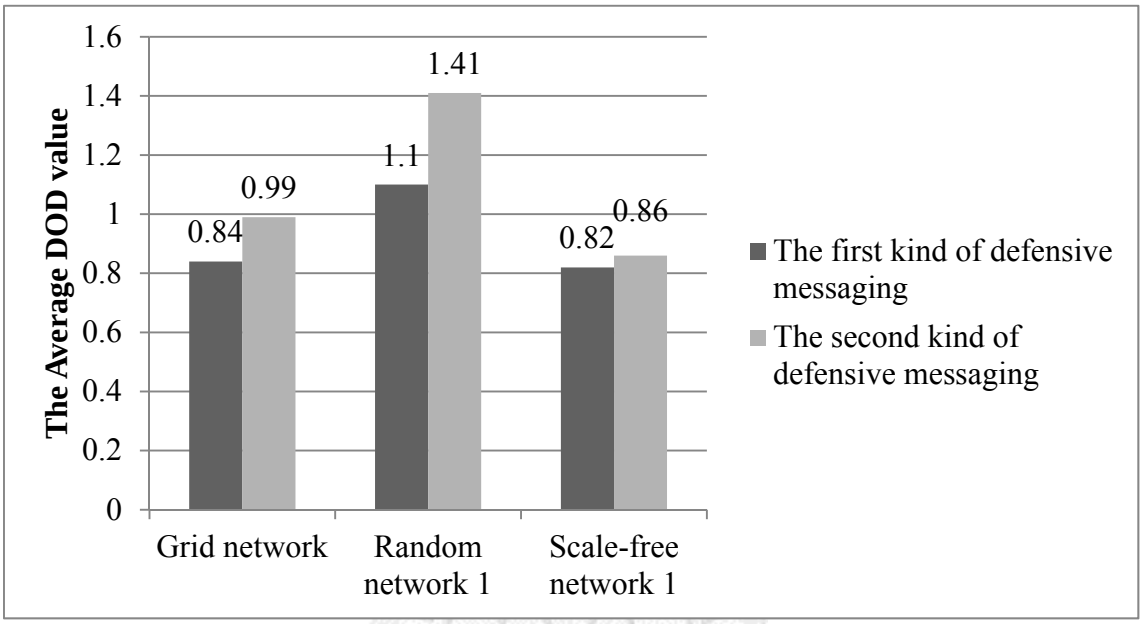


Figure 4-17 : Comparing the results of three different kinds of networks for the defender having more total resources

4.4.2 The Experiments of the Attacker Having More Total Resources

In this experiment, the defender having fewer total resources would be considered and the total resources of the defender would be 24. The experiment results would be demonstrated in Table 4-20.

Table 4-20 : The results of the attacker having more total resources

The first kind of defensive messaging			
Network Topology	Average DOD	Strategy of Attacker	Strategy of Defender
Grid	1.03	(1, 0, 0)	(0.3, 0.6, 0.1)
Random 1	1.44	(0.3, 0.6, 0.1)	(0.3, 0.6, 0.1)
Scale-free 1	1.2	(0.33, 0.33, 0.33)	(0.3, 0.6, 0.1)
The second kind of defensive messaging			
Network Topology	Average DOD	Strategy of Attacker	Strategy of Defender
Grid	2.08	(1, 0, 0)	(0.6, 0.3, 0.1)
Random 1	2.63	(1, 0, 0)	(0, 1, 0)
Scale-free 1	2.11	(0.6, 0.3, 0.1)	(0.6, 0.3, 0.1)

4.4.2.1 Discussion of Results

To compare three different kinds of network topology in these two kinds of defensive messaging as shown in Figure 4-18, the average DOD value in grid network was lower than random 1 and scale-free 1, respectively. Also, the average DOD value in scale-free network 1 was lower than random 1. Because the weight in three rounds was the same, the attacker had sufficient time to collect information to attack. Besides, the distribution of important nodes was random and scattered in random network 1, so local nodes damage would cause network fragmentation which let the average DOD

value was higher than the others. Moreover, the core nodes in scale-free network 1 would not be explored easily under incomplete information, so the average DOD value was lower than random network 1. The distribution of important nodes was even in grid network, so comparing to random 1 and scale-free network 1 it would not become islands easily.

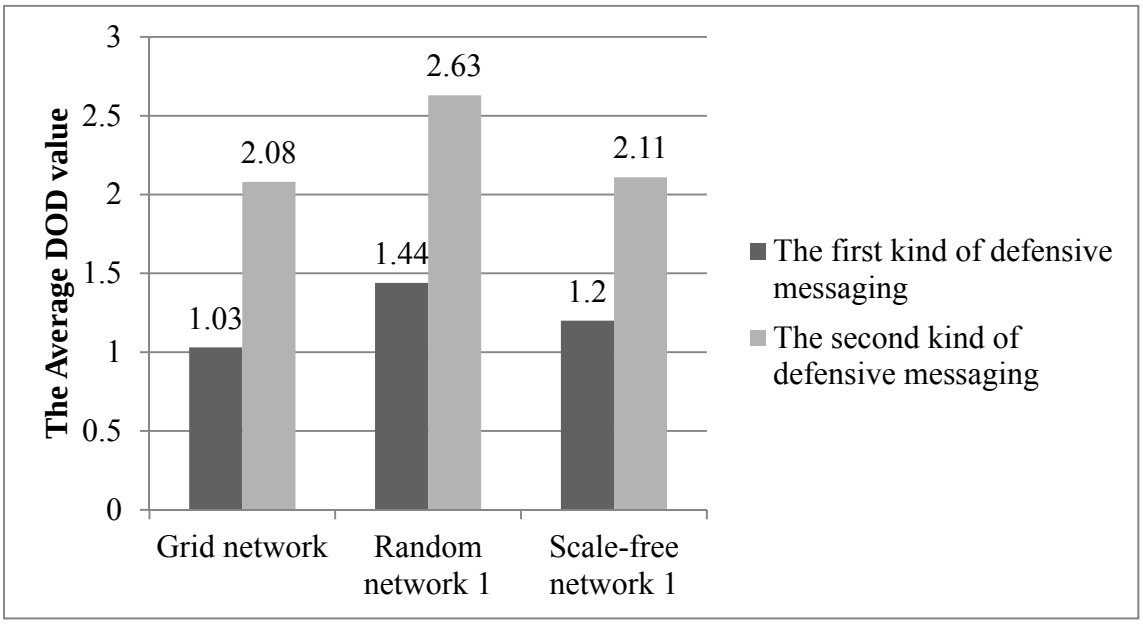


Figure 4-18 : Comparing the results of three different kinds of networks for the attacker having more total resources

4.4.3 Experiments Comparison

Comparing the experiment results of the attacker having more total resources with the defender having more total resources was shown in Figure 4-19 and Figure 4-20.

The defender having more total resources could reduce the information that the attacker could explore. Moreover, the defender having more total resources could also reduce the damage which caused by the attacker. Hence, the average DOD value of the defender having more total resources would lower than the attacker having more total resources.

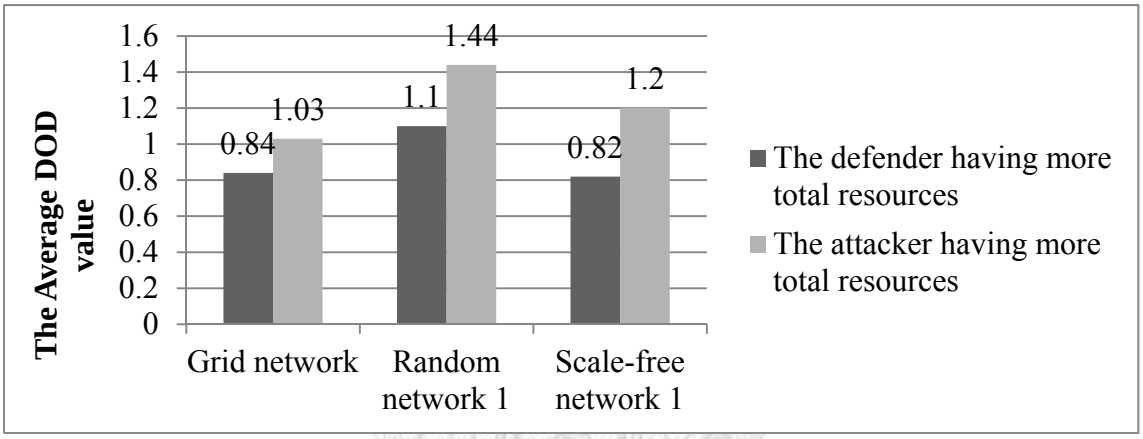


Figure 4-19 : Comparing the results of the defender with the attacker having more total resources under the first kind of defensive messaging

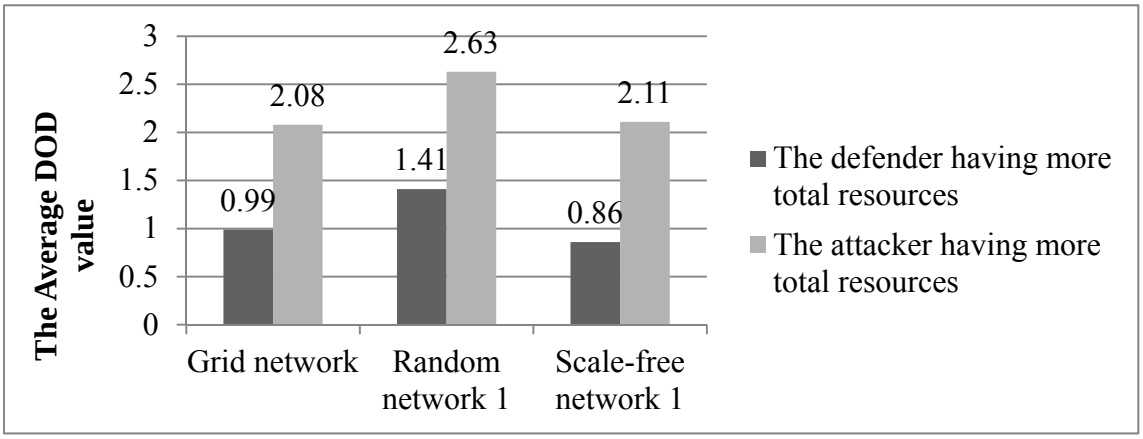


Figure 4-20 : Comparing the results of the defender with the attacker having more

total resources under the second kind of defensive messaging

4.5 The Experiments of Other Networks

In order to reduce the bias between different networks and let the results be more persuasive, we considered other random and scale-free networks which the number of links and the diameter of the network were the same as grid network. Besides, we also considered two common networks, ring and star network, in these series of experiments. The six different network topologies which were demonstrated in Figure 4-21 to Figure 4-26 respectively would be adopted to take the experiments.

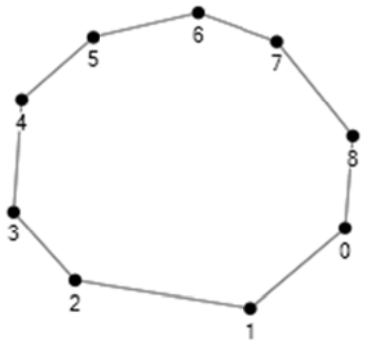


Figure 4-21 : Ring network

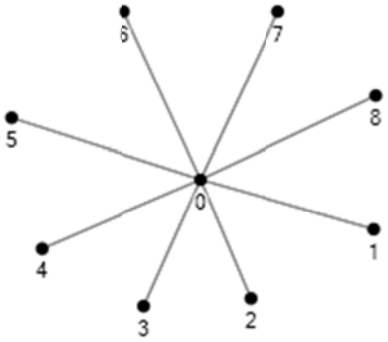


Figure 4-22 : Star network

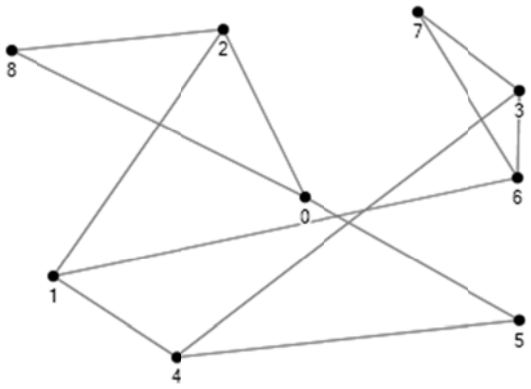


Figure 4-23 : Random network 2

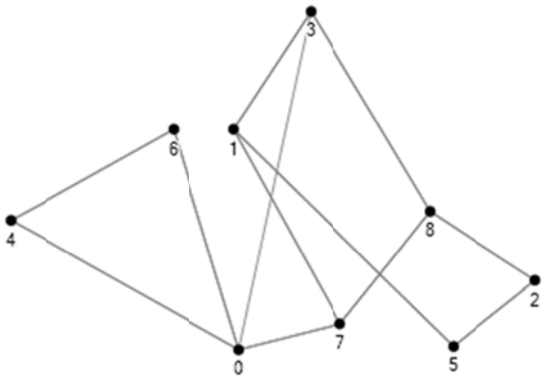


Figure 4-24 : Random network 3

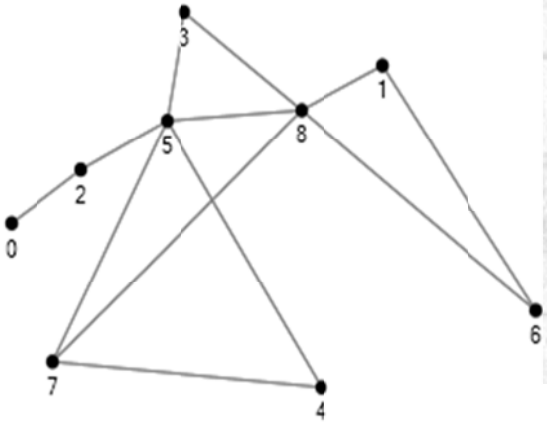


Figure 4-25 : Scale-free network 2

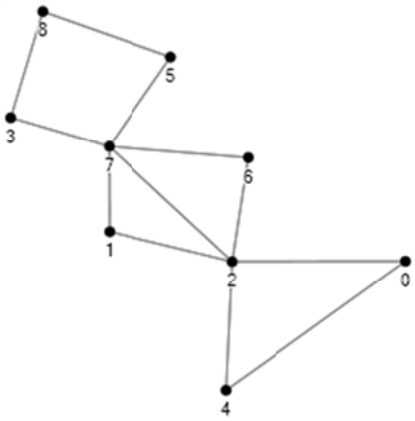


Figure 4-26 : Scale-free network 3

4.5.1 The Experiments Results of Complete Information

In these series of experiments, the weight (1, 1, 1) of three rounds and complete information would be considered. The experiment results would be demonstrated in Table 4-21.

Table 4-21 : The results of other networks under complete information

Network Topology	Average DOD	Strategy of Attacker	Strategy of Defender
Grid	1.525	(1, 0, 0)	(0.6, 0, 0.4)
Ring	2.45	(1, 0, 0)	(0.6, 0, 0.4)
Star	2.1	(1, 0, 0)	(1, 0, 0)
Random 2	2.36	(1, 0, 0)	(1, 0, 0)
Scale-free 2	2.38	(1, 0, 0)	(1, 0, 0)
Random 3	2.07	(1, 0, 0)	(1, 0, 0)
Scale-free 3	2.14	(1, 0, 0)	(0.6, 0.3, 0.1)

4.5.1.1 Discussion of Results

To compare grid, ring and star network topology as shown in Figure 4-27, the average DOD value in grid network was lower than ring and star, respectively. Also, the average DOD value in star network was lower than ring. Under complete information, because local nodes damage in ring network would cause network fragmentation, the

nodes could not connect to each other which let the average DOD value was higher than the others. In star network, though the attacker knew the important nodes and allocated a lot of resources on it, the attacker would not compromise the important nodes because of the defender would also allocate a lot of resources on it to protect resulting in the average DOD value was lower than ring network. Moreover, the distribution of important nodes was even in grid network, so comparing to ring and star network it would not become islands easily.

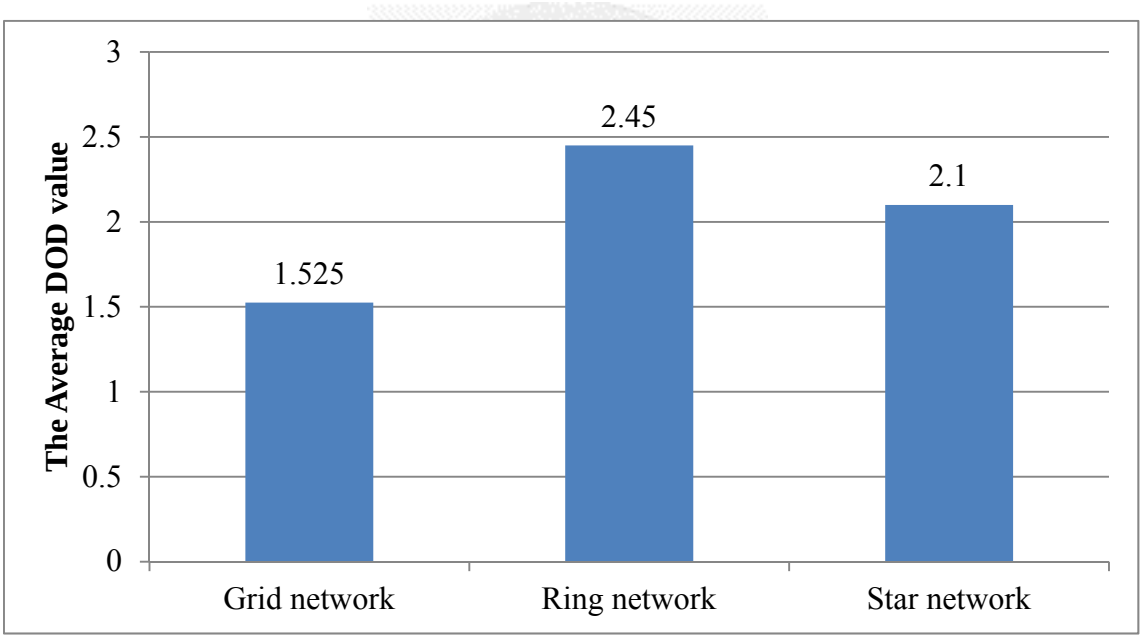


Figure 4-27 : Comparing the results of grid, ring and star network under complete information

To compare grid, random network 2 and scale-free network 2 as shown in Figure 4-28, the average DOD value in grid network was lower than random 2 and scale-free 2 respectively. Also, the average DOD value in random network 2 was lower than scale-free 2. Moreover, comparing the results of grid, random network 3 and scale-free network 3 as shown in Figure 4-29, the average DOD value in grid network was also lower than random 3 and scale-free 3 respectively. Also, the average DOD value in random network 3 was lower than scale-free 3. Under complete information, because the core nodes damage in scale-free network 2 would cause network fragmentation, the nodes could not connect to each other which let the average DOD value was higher than the others. Besides, the distribution of important nodes was random and scattered in random network 2, so local nodes damage would cause network becoming several blocks which let the average DOD value was higher than grid network. Moreover, the distribution of important nodes was even in grid network, so comparing to random 2 and scale-free network 2 it would not become islands easily. And, the results comparison of grid, random network 3 and scale-free network 3 were the same as the results comparison of grid, random network 2 and scale-free network 2. Moreover, the results comparison of grid, random network 2 and scale-free network 2 were also the same as the results comparison of grid, random network 1 and scale-free network 1.

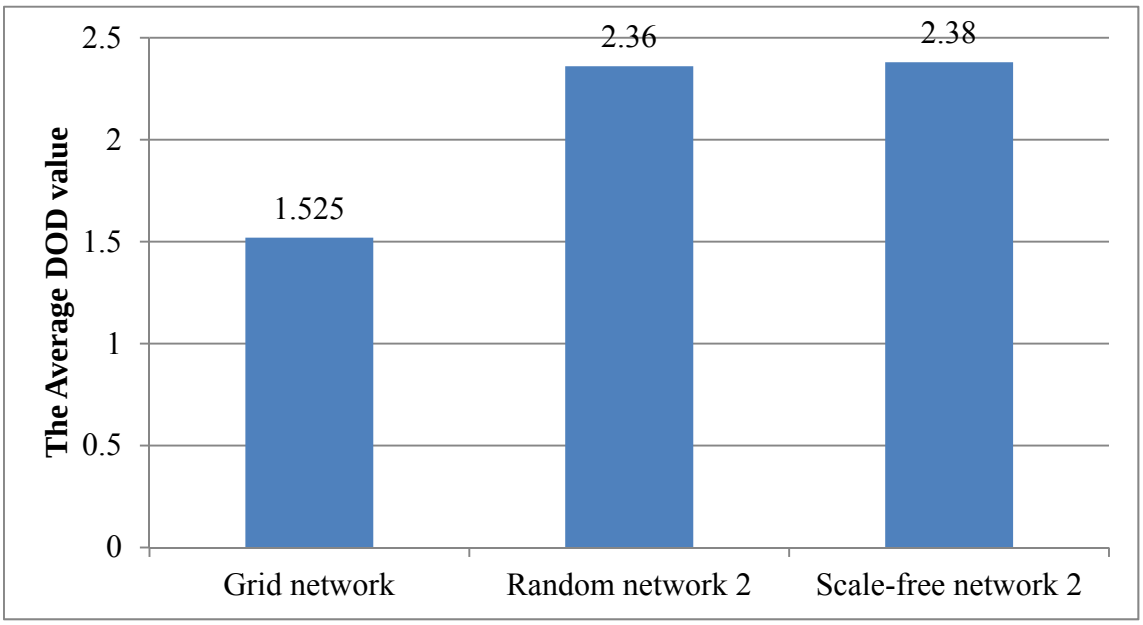


Figure 4-28 : Comparing the results of grid, random network 2 and scale-free network 2 under complete information

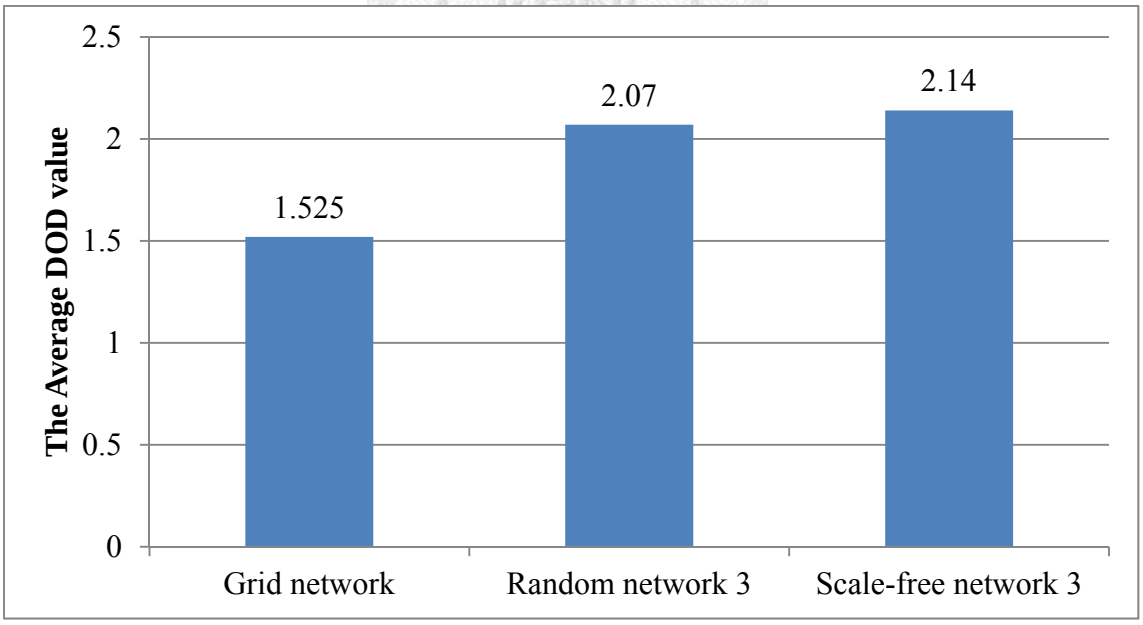


Figure 4-29 : Comparing the results of grid, random network 3 and scale-free network 3 under complete information

4.5.2 The Experiments Results of Incomplete Information

In these series of experiments, the weight (3, 0, 0) of three rounds and incomplete information would be considered. The experiment results would be demonstrated in Table 4-22.

Table 4-22 : The results of other networks under incomplete information

The first kind of defensive messaging			
Network Topology	Average DOD	Strategy of Attacker	Strategy of Defender
Grid	0.78	(1, 0, 0)	(1, 0, 0)
Ring	1.25	(1, 0, 0)	(1, 0, 0)
Star	0.7	(1, 0, 0)	(1, 0, 0)
Random 2	0.86	(1, 0, 0)	(1, 0, 0)
Scale-free 2	0.71	(1, 0, 0)	(1, 0, 0)
Random 3	1.02	(1, 0, 0)	(1, 0, 0)
Scale-free 3	0.7	(1, 0, 0)	(1, 0, 0)
The second kind of defensive messaging			
Grid	1.85	(1, 0, 0)	(0.6, 0, 0.4), (0.6, 0.3, 0.1)
Ring	2.86	(1, 0, 0)	(0.6, 0, 0.4), (0.6, 0.3, 0.1)
Star	1.64	(1, 0, 0)	(0.6, 0, 0.4), (0.6, 0.3, 0.1)
Random 2	2.02	(1, 0, 0)	(1, 0, 0)
Scale-free 2	1.64	(1, 0, 0)	(0.6, 0, 0.4), (0.6, 0.3, 0.1)
Random 3	2.09	(1, 0, 0)	(1, 0, 0)

Scale-free 3	1.63	(1, 0, 0)	(0.6, 0, 0.4), (0.6, 0.3, 0.1)

4.5.2.1 Discussion of Results

To compare grid, ring and star network topology as shown in Figure 4-30, the average DOD value in star network was lower than ring and grid, respectively. Also, the average DOD value in grid network was lower than ring. Because in the experiments we considered the weight (3, 0, 0) in three rounds and incomplete information, the first round was the most important. Therefore, the attacker would not have enough time and information to attack. Local nodes damage in ring network would cause network fragmentation, the nodes could not connect to each other which let the average DOD value was higher than the others. The distribution of important nodes was even in grid network, so comparing to ring network it would not become islands easily. The core nodes in star network would not be compromised easily because the first round was the most important and the attacker would not have enough time and information to attack. So, the average DOD value of star network was lower than ring and grid network.

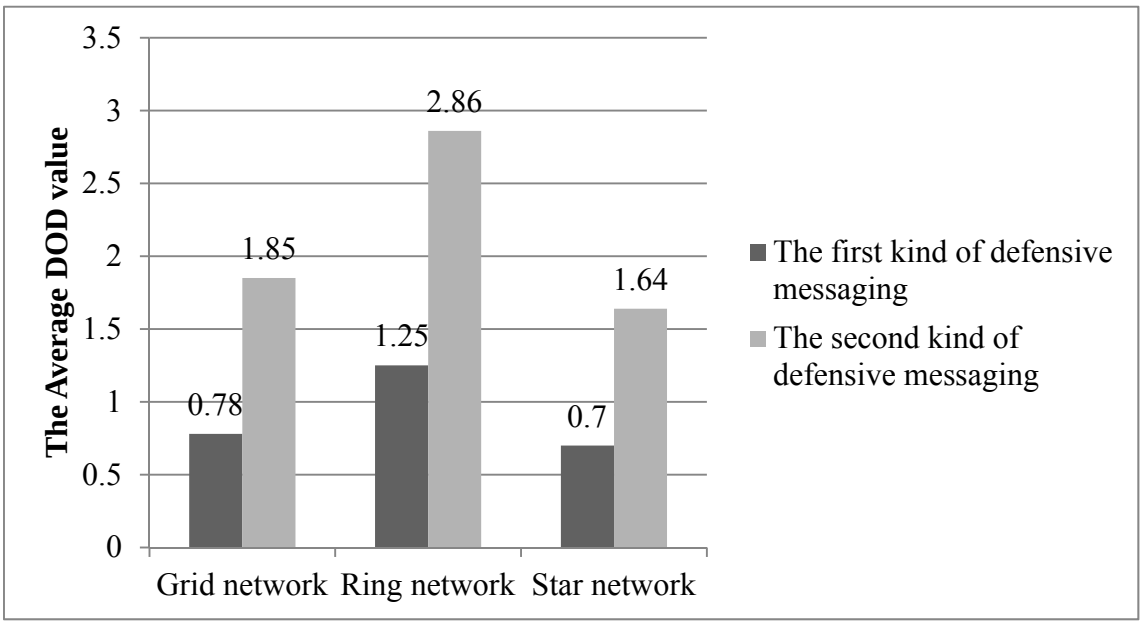


Figure 4-30 : Comparing the results of grid, ring and star network under incomplete information

To compare grid, random network 2 and scale-free network 2 as shown in Figure 4-31, the average DOD value in scale-free network 2 was lower than random 2 and grid respectively. Also, the average DOD value in grid network was lower than random network 2. Moreover, comparing the results of grid, random network 3 and scale-free network 3 as shown in Figure 4-32, the average DOD value in scale-free network 3 was also lower than random 3 and grid respectively. Also, the average DOD value in grid was lower than random network 3. Because in the experiments we considered the weight (3, 0, 0) in three rounds and incomplete information, the first round was the most important. Therefore, the attacker would not have enough time and information to

attack. The distribution of important nodes was random and scattered in random network 2 and 3, so local nodes damage would cause network fragmentation which let the average DOD value was higher than the others. The distribution of important nodes was even in grid network, so comparing to random network 2 it would not become islands easily. The core nodes in scale-free network 2 would not be explored easily because the first round was the most important and the attacker would not have enough time and information to attack. Therefore, the average DOD value in scale-free network 2 was lower than random 2 and grid network. And, the results comparison of grid, random network 3 and scale-free network 3 were the same as the results comparison of grid, random network 2 and scale-free network 2. Moreover, the results comparison of grid, random network 2 and scale-free network 2 were also the same as the results comparison of grid, random network 1 and scale-free network 1.

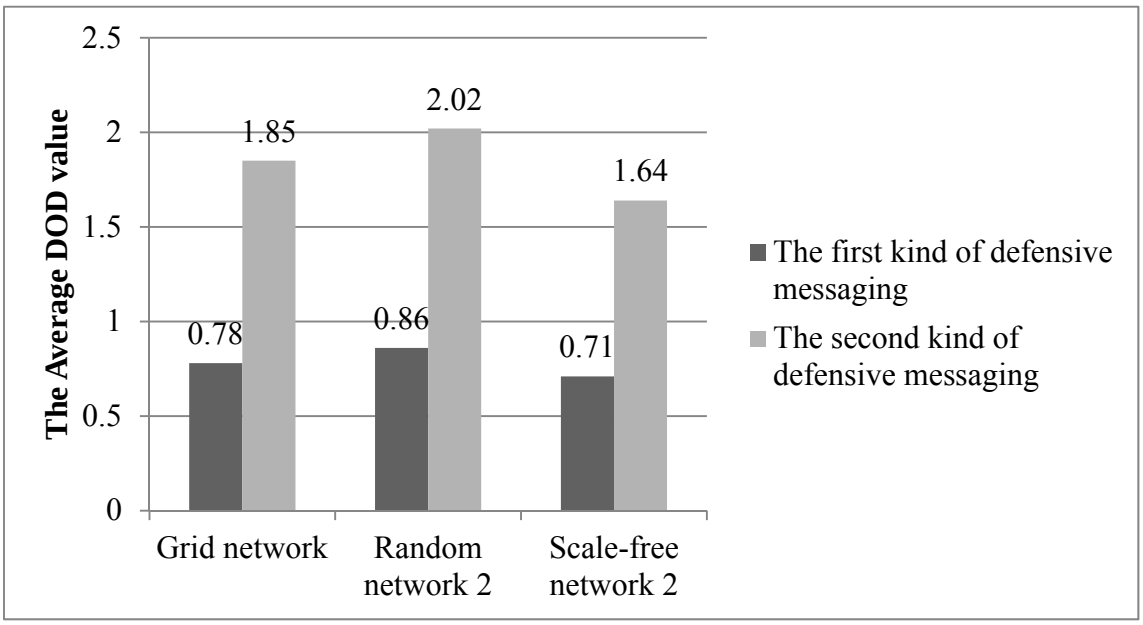


Figure 4-31 : Comparing the results of grid, random network 2 and scale-free network 2 under incomplete information

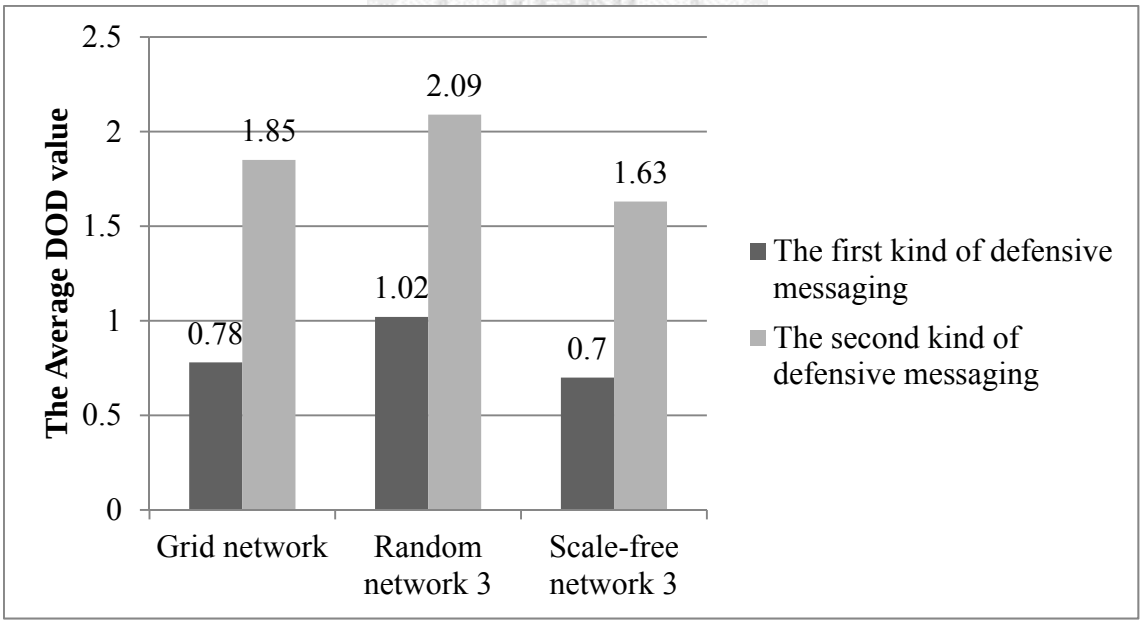


Figure 4-32 : Comparing the results of grid, random network 3 and scale-free network 3 under incomplete information

Chapter 5 Summary and Future Work

5.1 Summary

In this thesis, two issues are considered. First, an incomplete information attack-defense problem was proposed in this thesis. In addition, how to efficiently allocate resources on each node in multiple rounds for both cyber attacker and network defender is needed to be solved.

The main contributions of this work are as follows:

1. An incomplete information attack-defense problem

In reality, the attacker owns information which is often limited. It is impossible for the attacker to know the whole information about the defender. In other words, the information between the attacker and the defender is not always symmetric. Therefore, an incomplete information attack-defense problem was considered in this thesis. Moreover, we also considered the defender releasing message which might be truth, secrecy, deception or doing nothing at all to each node in each round to increase defense efficiency.

2. Solving a multi-round attack-defense problem

A new min-max mathematical formulation was proposed. Moreover, both cyber attacker and network defender could take lots of different policies. From the view of the attacker, the accumulated experiences and vulnerability attacks would be considered. On the other side, the resource reallocation or recycle, node recovery, system vulnerability patch and message releasing problem would be considered for the defender in this thesis.

Besides, the gradient method and game theory would be adopted to find the optimal resource allocation for both cyber attacker and network defender on each node in each round. The gradient method would be used to find the optimal resource allocation on each node. Besides, the game theory would be adopted to find the optimal percentage resource allocation in each round.

3. A more realistic network topology

In this thesis, a complex system with n nodes in series-parallel was considered. Besides, a node with backup component and a k-out-of-m node were adopted on important nodes to conduct high availability system. Moreover, we also considered

three kinds of relationships between nodes which included independence, dependence and interdependence to get closer to realistic network topology.

4. Providing a objective guideline for network operators

In this multi-round attack-defense problem, we conduct a mathematical model for this problem. Besides, we use Average DOD to evaluate damage degree of network to help network operators to predict all possible strategies which both cyber attacker and network defender would take. As a result, network operators could use this model to take strategies and optimally allocate resources to ensure a prearranged level of system survivability.

Considering the multi-round attack-defense scenario, a comprehensive defense strategy should be developed from different aspects.

First, according to the experiments results we could find that incomplete information would be more advantageous for the defender in most cases. Under incomplete information the defender could manipulate his private information to use some tricks to reduce attack success probabilities. For example, the defender could use defensive messaging to protect his private information. Moreover, in the experiments results we also found that the defender according to the importance of different

information of a node to release messages would be more advantageous.

Second, basing on the experiments results conducting high availability system for equipments could ensure the service which would not be interrupted. Therefore, the defender could conduct high availability system for important equipments to increase system survivability.

Third, no matter how many resources the defender had and which round was the most important, defending early would be more advantageous in the light of the experiments results. Though it would cost some resources to reallocate resources, it was a waste to let resources unused.

Last but not least, according to the experiments results we could find that the system survivability in random network under incomplete information was the worst. Therefore, the defender should avoid letting network topology form random network. Moreover, the system survivability in scale-free network under incomplete information was the best. Though the defender could use scale-free network to increase system survivability under incomplete information, the defender should enhance protections of the core nodes or conduct backup for the core nodes. Besides, the system survivability in grid network under incomplete information was medium. Though the system

survivability in grid network under complete information was the best, under incomplete information the attacker could explore nodes easily in grid network. Therefore, the defender could use grid network to conduct network under incomplete information, but the defender should protect all nodes and the information of nodes to reduce the probability which the attacker could explore nodes.

5.2 Future Work

The following issues could be considered in the future:

1. Considering the nodes' weights into Average DOD

In this thesis, we used Average DOD to help evaluating the network survivability. The Average DOD, proposed in [29], is a metric of the network survivability which combined the concept of probability calculated by the contest success function [30] with the DOD metric. However, in reality defenders might think both the network survivability and the confidential data on some nodes are important. For example, the network survivability might not low when a node with confidential data was compromised by the attacker. But, the defender would lose the confidential data such as trade secrets resulting in large revenue loss. Therefore, in the future taking the nodes'

weights into account for calculating Average DOD would more realistic.

2. To extend this problem

There are still multiple different kinds of issue that could be extended in the future. In the following, some issues would be discussed.

- Defense dependency

  In this thesis, a three-round attack-defense game has been discussed, but it is difficult to consider the relation of defense strategy between different rounds because of the complexity of mathematical problem. Therefore, the issues about the relation of defense strategy between different rounds could be considered in the future work and could adopt markov chain to solve this kind of problem.

- Integrated defense

  In this thesis, we considered message releasing to increase defense efficiency. However, integrated defense would be better, such as combining the two kinds of message releasing in this problem or the other defense strategies. Therefore, the issues about integrated defense could be considered in the future.

- Multiple attackers

  In the past, most of papers only considered one defender and one attacker. However, there are multiple kinds of network security that different attackers launched the attacks simultaneously such as collaborative attacks or non-collaborative attacks. For example, the defender might defend attackers with different goals and motivations simultaneously. Therefore, there are some papers considering the multiple attackers in recent years [13]. As a result, the issues about multiple attackers could be considered in the future work.

- Survivability in the cloud

  There are many cloud service providers provide cloud services to enterprises, for example, cloud storages, cloud servers and so forth. Enterprises want their cloud services to be ready to serve them at all times. When the survivability of these cloud service providers was low, their customers would not access their data in the cloud. Then, the survivability of their customers would also low. Therefore, if enterprises used cloud services, they not only needed to ensure the survivability of themselves but also the survivability of cloud service providers. As a result, the issues about the survivability in

cloud could be considered in the future work.

Because of the diversity of the attack-defense problem, there are multiple different kinds of issue that could be discussed. Therefore, more and more issues would be extended to reflect reality in the future.

References

[1] Symantec, "Symantec Report on Attack Kits and Malicious Websites", *Symantec Corporation*, January 2011.

[2] R. Richardson, "2010/2011 CSI Computer Crime and Security Survey", *Computer Security Institute*, December 2010.

[3] Symantec, "Symantec Internet Security Threat Report Trends for 2010", *Symantec Corporation*, Vol. 16, April 2011.

[4] Symantec, "2011 State of Security Survey", *Symantec Corporation*, pp. 1-19, 2011.

[5] J. Hoffer, "Backing Up Business – Industry Trend or Event", *Health Management Technology*, January 2001.

[6] V.M. Bier, S. Oliveros and L. Samuelson, "Choosing What to Protect: Strategic Defensive Allocation Against an Unknown Attacker", *Journal of Public Economic Theory*, Vol. 9, Issue 4, pp. 563–587, August 2007.

[7] J. Zhuang and V.M. Bier, "Balancing Terrorism and Natural Disasters - Defensive

Strategy with Endogenous Attacker Effort", *Operations Research*, Vol. 55, Issue 5, pp. 976–991, September 2007.

[8] T. Sandler and D.G. Arce, "Terrorism and Game Theory", *Simulation & Gaming*, Vol. 34, Issue 3, pp.319–337, September 2003.

[9] C. Harsanyi, "Games with Incomplete Information", *The American Economic Review*, Vol. 85, No. 3, pp. 291-303, June 1995.

[10] F.Y.S. Lin, P.Y. Chen, and P.H. Tsang, "An Evaluation of Network Survivability When Defense Levels Are Discounted by the Accumulated Experience of Attackers", *Proceedings of the Annual Security Conference*, 2009.

[11] R. Peng, G. Levitin, M. Xie and S.H. Ng, "Defending Simple Series and Parallel Systems with Imperfect False Targets", *Reliability Engineering & System Safety*, Vol. 95, Issue 6, pp. 679-688, June 2010.

[12] V.M. Bier, A. Nagaraja and V. Abhichandani, "Protection of Simple Series and Parallel Systems with Components of Different Values", *Reliability Engineering & System Safety*, Vol. 87, Issue 3, pp. 315-323, March 2005.

[13] K. Hausken and V.M. Bier, "Defending against Multiple Different Attackers",

European Journal of Operational Research, Vol. 211, Issue 2, pp. 370-384, June 2011.

[14] J. Zhuang, V.M. Bier and O. Alagoz, "Modeling Secrecy and Deception in a Multiple-period Attacker–defender Signaling Game", *European Journal of Operational Research*, Vol. 203, Issue 2, pp. 409–418, June 2010.

[15] J. Zhuang and V.M. Bier, "Secrecy and Deception at Equilibrium, with Applications to Anti-terrorism Resource Allocation", *Defence and Peace Economics*, Vol. 22, No. 1, pp. 43-61, February 2011.

[16] N.S. Dighe, J. Zhuang and V.M. Bier, "Secrecy in Defensive Allocations as a Strategy for Achieving More Cost-effective", *International Journal of Performability Engineering*, Vol. 5, No. 1, pp. 31-43, January 2009.

[17] R. Powell, "Allocating Defensive Resources with Private Information about Vulnerability", *American Political Science Review*, Vol. 101, No. 4, pp. 799–809, November 2007.

[18] N.C. Rowe, "Deception in Defense of Computer Systems from Cyber Attack", *Cyber Warfare and Cyber Terrorism*, pp. 97-104, 2008.

[19] N.C. Rowe and H.S. Rothstein, "Two Taxonomies of Deception for Attacks on Information Systems", *Journal of Information Warfare*, Vol. 3, No. 2, pp. 27-39, July 2004.

[20] K. Hausken, "Strategic Defense and Attack for Reliability Systems", *Reliability Engineering & System Safety*, Vol. 93, Issue 11, pp. 1740-1750, November 2008.

[21] M.N. Azaiez and V.M. Bier, "Optimal Resource Allocation for Security in Reliability Systems", *European Journal of Operational Research*, Vol. 181, Issue 2, pp. 773-786, September 2007.

[22] F.Y.S. Lin, P.H. Tsang, P.Y. Chen and H.T. Chen, "Maximization of Network Robustness Considering the Effect of Escalation and Accumulated Experience of Intelligent Attackers", *Proc. World Multiconference on Systemics, Cybernetics and Informatics*, 2009.

[23] G. Levitin and K. Hausken, "Resource Distribution in Multiple Attacks Against a Single Target", *Risk Analysis*, Vol. 30, No. 8, pp. 1231–1239, August 2010.

[24] T. Alpcan and T. Baser, "A Game Theoretic Analysis of Intrusion Detection in Access Control Systems", *Proceeding of the 43rd IEEE Conference on Decision*

and Control, 2004.

[25] K. Hausken, "Defense and Attack of Complex and Dependent Systems", *Reliability Engineering & System Safety*, Vol. 95, Issue 1, pp. 29-42, January 2010.

[26] J. Grossklags, N. Christin, J. Chuang, "Secure or Insure? A Game-Theoretic Analysis of Information Security Games", *Proceedings of the 17th International World Wide Web Conference*, April 2008.

[27] 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*, 1997.

[28] F.Y.S. Lin, H.H. Yen, P.Y. Chen and Y.F. Wen, "Evaluation of Network Survivability Considering Degree of Disconnectivity", *Lecture Notes in Artificial Intelligence*, Vol. 6678, pp. 51-58, 2011.

[29] F.Y.S. Lin, P.Y. Chen and Q.T. Chen, "Resource Allocation Strategies to Maximize Network Survivability Considering of Average DOD", *Advances in Intelligent and Soft Computing*, Vol. 151, pp. 751-758, 2012.

[30] S. Skaperdas, "Contest Success Functions", *Economic Theory*, 1996.

[31] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya and Q. Wu, "A Survey of Game Theory as Applied to Network Security", *Proceedings of the 43rd Hawaii International Conference on System Sciences*, 2010.

[32] G. Owen, "Game Theory, 3rded", *Academic Press*, 2001.