國立臺灣大學資訊管理學研究所碩士論文

指導教授： 林永松 博士

考慮單一核心節點攻擊下
網路近似最佳化防護策略

Near Optimal Protection Strategies against Targeted Attacks on the Core Node of a Network

研究生： 林義倫 撰

中華民國九十五年七月

考慮單一核心節點攻擊下

網路近似最佳化防護策略

Near Optimal Protection Strategies against Targeted Attacks on the Core Node of a Network

本論文係提交國立台灣大學
資訊管理學研究所作為完成碩士
學位所需條件之一部份

研究生： 林義倫 撰

中華民國九十五年七月

謝　　詞

回顧兩年來的日子，充滿了許多的回憶，也很高興，能夠在人生第一本論文中，寫下我心中滿滿的感激。首先，我要感謝我的父親林耀川先生與張秀香女士，你們的身教言教，讓我獲益良多。謝謝你們對於家庭的犧牲奉獻，讓我在求學之路上能無後顧之憂地完成學業。

謝謝我的指導老師林永松博士，謝謝您不論是在學業或是待人處事方面，都給予學生莫大的指導與鼓勵。您嚴謹的治學態度，讓學生學習到學術研究的精煉精神，也謝謝您的教導，讓學生能學習到許多關於人生的道理；謝謝口試委員孫雅麗所長、林盈達博士、呂俊賢博士、趙啟超博士對於本論文所提出的寶貴意見，使本論文能漸趨於完善；特別感謝博士班柏皓學長，在我人生中最黑暗，最需要幫助的時候，您總是伸出您的援手，指引我曙光的方向，不論在學術研究領域以及其他方面，都給予我莫大的幫助，真的很感激您；此外，謝謝博士班國維、演福、政達學長，謝謝你們在這兩年來所給予我的鼓勵與幫助。

謝謝建宏學長，在研究領域方面所給予我的啟發與幫助；謝謝琳智、書平、孝澤、明源學長， 謝謝你們在我剛進入實驗室時給我的指導與鼓勵；謝謝我的好伙伴們中蓮、孝穎、文政、弘翕、勇誠，謝謝你們陪我一起加油打氣，度過這兩年來的時光，以及所發生的一切，這將會是我未來人生中永難忘懷的一段記憶，真的很謝謝你們；謝謝學弟妹們雅芳、坤道、俊維、承賓、岦毅、翊恆、怡孜，謝謝你們的幫忙以及歡笑，真的很謝謝你們，讓我能順利地完成口試；謝謝怡靜與小米，在我人生最低潮的時候，陪我走過那一段特別的時光。最後，謝謝上帝，賜給我無比的勇氣，來面對未來未知的挑戰。

林義倫　謹識

于臺大資訊管理研究所

中華民國九十五年七月

論文摘要

論文題目：考慮單一核心節點攻擊下網路近似最佳化防護策略

作　　者：林義倫　　　　　　　　　　　　　　　　　民國九十五年七月

指導教授：林永松　博士

隨著近年來網路科技的蓬勃發展，網際網路已成為21世紀最重要的傳播媒體，伴隨而來，資訊安全的議題也越形重要。我們發現，在網路攻防下，攻防雙方都會依據對方的策略而改變自己的對策，就如矛與盾一般地相互抗衡。

在本篇論文中，我們以防守方的角度來思考，在有限的防禦資源限制下，提出一個有效的防禦資源配置策略，來最大化攻擊者的攻擊成本，以提高核心節點的防護能力。分析此問題，為一非線性混合整數規劃的數學最佳化問題，由於問題本身高度的複雜性與困難度，所以我們以格拉蘭日鬆弛法為基礎的演算法來處理此問題，並針對與真實網路環境相似之無尺度網路，進行其存活度分析與探討。

關鍵詞：防禦資源配置策略、資訊安全、網路攻防、存活度、拉格蘭日鬆弛法、最佳化、無尺度網路。

THESIS ABSTRACT

GRADUATE INSTITUTE OF INFORMATION MANAGEMENT

NATIONAL TAIWAN UNIVERSITY

NAME: YI-LUEN LIN MONTH/YEAR:JULY/2006

ADVISOR: DR. YEONG-SUNG LIN

NEAR OPTIMAL PROTCTION STRATEGIES AGAINST

TARGETED ATTACKS ON THE CORE NODE OF A NETWORK

With the rapid growth of network technologies, the Internet may well become the single most important medium of the 21st century. Therefore, the issue of information security has drawn increasing attention. In network attack and defense, attackers and defenders constantly change their respective strategies. The situation is like the balance between a lance and a targe.

In this thesis, we view the problem of security from the defender's perspective. Given that defense resources are limited, we propose an effective defense resource allocation strategy that maximizes the attackers' costs, and improves the protection of the core node. The problem is analyzed as a mixed nonlinear integer programming optimization problem. The solution approach is based on the Lagrangean relaxation method, which effectively solves this complicated problem. Furthermore, we evaluate the survivability of real network environment-like scale-free networks.

Key Words: Defense Resource Allocation Strategy, Information Security, Lagrangean Relaxation Method, Network Attack and Defense, Optimization, Scale-Free Networks, Survivability.

Contents

List of Figures

List of Tables

Chapter 1 Introduction

1.1 Background

The 21st century is the so-called age of the Internet, which implies the Internet has become an indispensable application in our daily lives. A substantial number of Internet applications have been developed for our convenience, and they have had a great impact on information communications worldwide, such that a network user can communicate or obtain information unboundedly. However, the downside of this phenomenon is that attackers can target organizations or individuals who connect to the Internet and thereby obtain sensitive information because of its high availability.

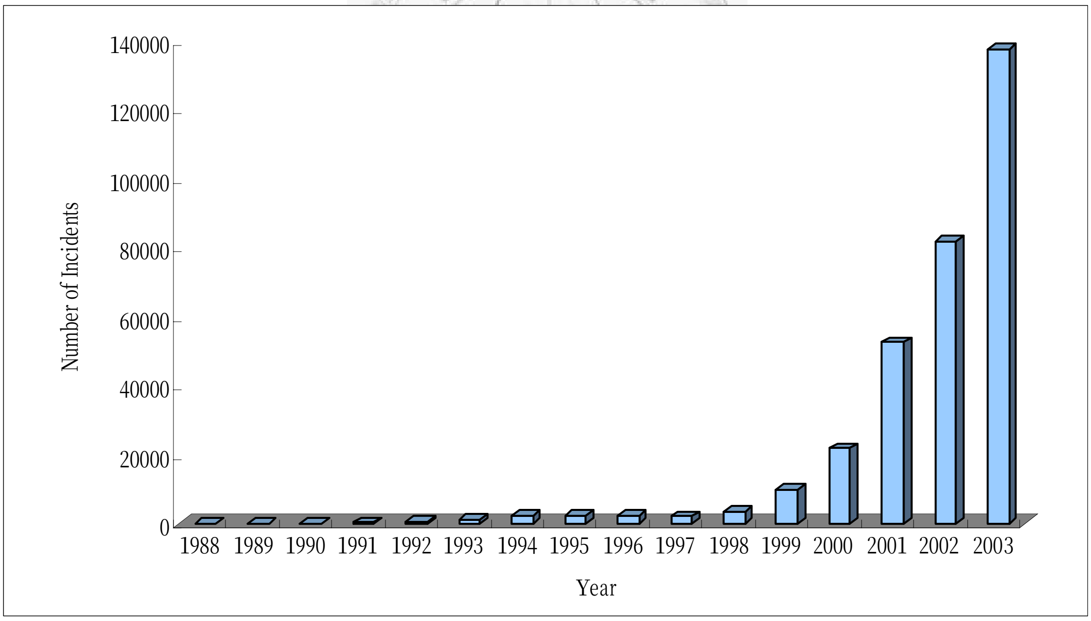

Figure 1-1 Trend of Incidents

With the rapid growth of the Internet, the realm of information security has attracted more and more attention. In recent years, according to the report from CERT

[1], the number of incidents [2] has increased as **Figure 1-1** shows. An incident indicates a violation of security policy, such as an attack on a computer or an attempt to gain unauthorized access to some data. Because of this trend, information security has become increasingly important. A substantial number of techniques and methodologies have been proposed to protect networks against malicious attacks. Many researchers in the field of information security have focused on the behavior of attackers and the defense methods of those under attack. From such research, we know that attackers and defenders constantly change their respective strategies. Thus, if defenders change their defense methods, attackers will change their strategies to find new vulnerabilities to gain the same benefits. Moreover, defenders will modify their defense methods in order to increase the difficulties of attacks, and then attackers will react again. The situation is like the balance between a lance and a targe.

Another important research domain is network survivability, and a great deal of research has been conducted on survivability. Initially, researchers focused on the effect of random failures on networks, like large-scale power failures, and tested how robust and dependable a network was. They have proposed many definitions, techniques, and architectures to evaluate the survivability of networks. Therefore, given the trend of improving information security, many researchers are paying ever-increasing attention on combining survivability and information security.

Another way to evaluate the survivability of a network is to study its topology. The scale-free network is attracting more and more attention from the domain of network research. This topology structure follows the power-law distribution [3]. The best practice of the scale-free network is the Internet. Most parts of the Internet operate normally when random failures happen; however, if the Internet suffered intelligent attacks, its performance would be significantly impaired. These facts motivate us to investigate how different topologies influence survivability.

The key asset of enterprises or organizations is their know-how. Usually, they store their most valuable and sensitive knowledge in a network domain, called the “core node”, which attackers try their hardest to compromise. However, enterprises or organizations have finite information security budgets to purchase security products or obtain expert advice to enhance network survivability. From a network operator’s perspective, there are few guidelines on how to allocate security budgets effectively. Thus, there is an urgent need for research in the field of combining survivability and information security.

1.2 Motivation

Because of the critical importance of the core node, defenders and attackers change their strategies to protect and compromise the node respectively. With limited defense resources, defenders need to deploy the resources more effectively. However, until now, there has only been limited theoretical research on the economic allocation of defense resources. Therefore, we propose a mathematical model to formulate the attack-defense behavior, and propose defense strategies to improve the protection of the core node. The motivation of this thesis is to provide defenders with useful defense resource allocation strategies, and that will make the cost of attacking the core node unacceptable to the attacker.

1.3 Literature Survey

1.3.1 Survivability

The research of survivability has a long history, and a wealth definitions, models, and architectures. The discipline of survivability can be classified into three categories, performance, connectivity, and other measurements. With ever-increasing attention of information security, many researchers have focused on the combination of survivability and information security. Thus, in this thesis, the survivability is the measurement of information security, which indicates the protection of the core node.

In [4], the author summarizes definitions of survivability, and we extract some information security related ones. Therefore, we find that the general concept of information security related survivability has three parts: 1) the continuity of service under an attack; 2) the provision of strategy against an attack; 3) the ability to protect the system from being compromised. In [5], the definition of survivability is the capability of a system to fulfill its mission in a timely manner in the presence of attacks, failures, or accidents, which satisfies part 1. In [6], the definition of survivability is a property of a system, subsystem, equipment, process, or procedure that provides a defined degree of assurance that the named entity will continue to function during and after a natural or man-made disturbance; this also satisfies part 1, too. In this thesis, we focus on part 2, thereby improving parts 1 and 3.

Along with the trends, a substantial number of models are proposed or modified to evaluate the security related survivability. In [7], the authors summarize several models to quantitatively evaluate the survivability. For example, the attack tree is a graphical one, which consists of a goal, attack scenarios, and logic gates, as shown in **Figure 1-2**.

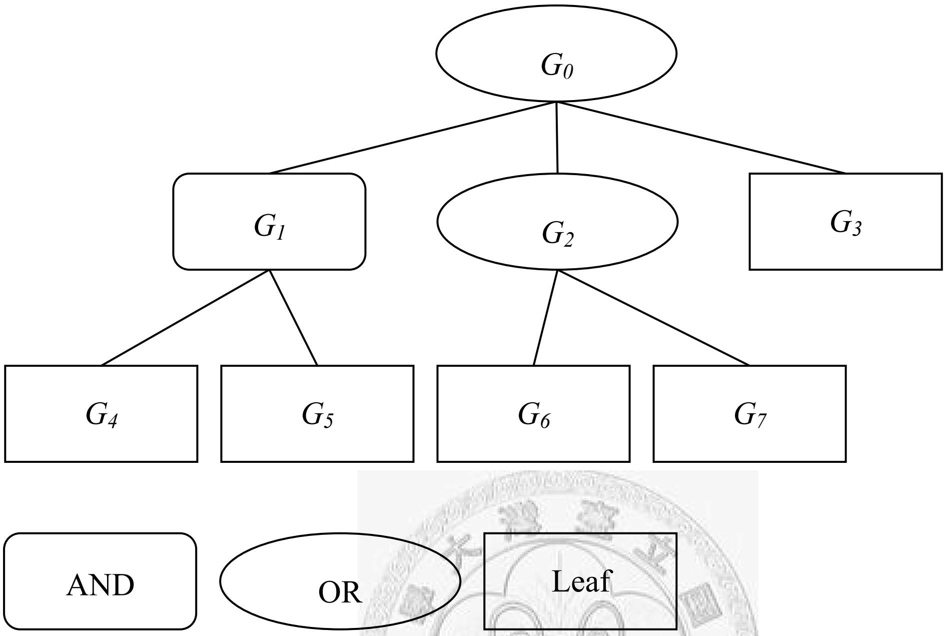

Figure 1-2 Attack Tree Example

G_0 denotes the goal, e.g., the crash of the system. The leaf node denotes the attack scenario. Initially, we set the value to each attack scenario, so we can obtain the value of G_0 via logic gates. That is, if the probability is assigned to each leaf node, one can finally obtain the probability of achieving the goal via the attack tree.

Another means of evaluating the survivability is the state-based model. In [8], the authors propose an architecture to quantitatively analyze the survivability. The survivability specification is a four-tuple, {*E, R, P, M*} where *E* is a definition of the environment where the survivable system has to operate; *R* is a set of specifications of tolerable forms of service for the system; *P* is a probability associated with each member of the set R with the sum of these probabilities being one; M defines precisely how and when the system is required to move from providing one form of tolerable service to another. Therefore, we initialize specifications from R_1 to R_n, with its probability P. Thus, by applying the architecture, we can describe and evaluate the survivability performance level for different scenarios, even under seriously abnormal conditions. Furthermore, in [9], by applying this architecture, the author implemented it by the Markov chain.

In addition, there is still much research about quantitative analysis of the survivability. In [10], the author proposes a survivability function to measure the performance when the network suffers a catastrophic disaster. The survivability function is proposed to evaluate the expected percentage of total data flow delivered after failure, even in the worst case scenario. In [11], researchers discuss issues and approaches, such as application error recovery, and securing the survivability mechanism, for developing survivable architectures. To concentrate on securing the survivability mechanism, if the survivability mechanism were completely isolated, the security of the survivability mechanism is possible. However, it is impossible, e.g., the firewall configuration on a web server may be changed by attackers via the Internet. Therefore, the authors propose two approaches to solve this problem: 1) one-way translation and diversity, and 2) securing the survivability mechanism. In the summary, the authors summarize approaches then propose survivable architectures to enhance the survivability and security of the system simultaneously.

To summarize the research of quantitative analysis in the discipline of survivability, however, we find that to date there is a lack of a model to formulate the attack-defense behavior. Therefore, the motivation of this thesis is to formulate attack-defense behavior, then provide defenders with strategies to maximize the protection of the core node.

1.3.2 Scale-Free Networks

In 1959, a well-known random graph model was proposed by Erdos and Renyi, called the ER model [12]. The specification of the ER model is the links between nodes are randomly placed. After the random placement of links, most nodes have almost the same number of links. Therefore, there are few nodes with an extremely large or small number of links. The probability $P(k)$ denotes the probability a node connected to k other nodes, and it follows the Poison distribution with a bell shape. The random network is also called the exponential network because its $P(k)$ is rapidly reduced for large k. **Figure 1-3** is an example of random networks [13], which resemble the U.S. highway system.

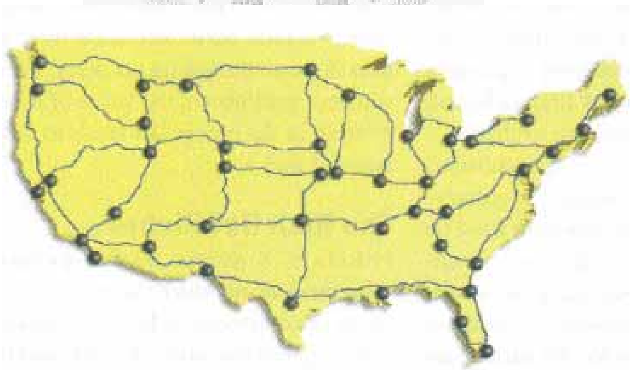

Figure 1-3 Random Network Example

In 1988, Duncan Watts and Steve Strogatz proposed another type of random network, called small-world model [14]. With randomly rewired links, the diameter of the small-world network will be rapidly reduced. Many observations were based on the small-world model, e.g., it was the basis of the popular notion of “six degrees of separation”, which demonstrates the maximum number of hops between any two people are six individuals.

However, with the rapid growth of the Internet, the small-world model doesn’t meet the specifications of the Internet. There still exits small-world phenomenon [15], but $P(k)$ of the Internet follows the power-law distribution, where $P(k)$~k^{-r}. It’s a noble network, where a small ratio of nodes own a substantial number of links, called the scale-free network [13]. The notion “scale-free” indicates the scale of the tail distribution of $P(k)$ is unlimited; the scale is “free”. The scale-free network was the newly observational network topology in recent years. Its strength is “the rich get richer”, but that is also its Achilles’ heel. The rich get richer indicates when a new node enters a network, it prefers to attach the node with a substantial number of links. Therefore, the network will eventually dominated by several most-connected nodes. However, this phenomenon also conducts risks. For the random network, because of its democracy of the number of links, if attacks on its most-connected nodes happen, the network will be remain robust because of its homogeneity. But for the scale-free network, if it suffers attacks on its most-connected nodes, the network will be separated into a number of fragmentations and isolations, and that is its so-called Achilles’ heel, as shown by the red circles in **Figure 1-4** [16].

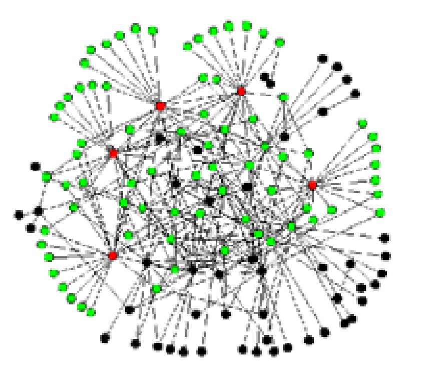

Figure 1-4 Scale-Free Network Example

1.4 Proposed Approach

The problem is a mixed nonlinear integer programming optimization problem, which can be effectively solved by using the Lagrangean relaxation method in conjunction with optimization-based heuristics. Furthermore, in this thesis, the definition of survivability we propose is the degree of protection to the core node against intelligent attacks. To quantitatively analyze the survivability, we propose a novel survivability metric in the following:

The survivability metric = LR / LB, where LR denotes the attack costs conducted by the proposed solution approach; and LB denotes the theoretical attack costs. The survivability metric indicates a level of protection of the core node. The more the survivability is, the better the protection of the core node is.

Chapter 2 Problem Formulation

2.1 Protection Strategy for Defenders (PSD) Model

2.1.1 Problem Description and Assumptions

At the AS (Autonomous System) level, by node we mean a network domain, e.g., a set of subnets. Because the core node contains much sensitive and valuable information, it has high strategic value. Thus, attackers target it to obtain the information. In order to compromise the target node, attackers will find a path from the start node to the core node, and compromise all intermediate nodes on the path to the target. However, compromising a node costs attackers some resources, such as time, money, and man-power.

From the defender's perspective, if more defense resources are allocated to a node, the protection of the node will be improved, and cost of attacking it will be increased. However, defense resources are limited, defenders must adopt an efficient resources allocation strategy that utilizes the resources effectively and economically, and simultaneously maximizes the attacker's costs.

In the worst case scenario, if an attacker can obtain the complete information about a network and use it intelligently, he will find the path of minimal attack cost to minimize the total cost of compromising the core node. Meanwhile, the defender will try to maximize the attacker's total necessary attack costs through different budget allocations to each node. In response, the attacker will then determine another path minimal attack cost to compromise the core node, as shown in **Figure 2-1**.

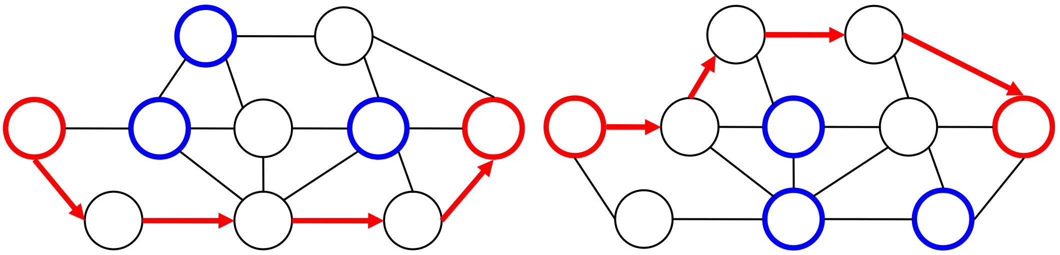

Figure 2-1 Network Attack and Defense Behavior

The red circle denotes the source and core node; the blue node denotes the node the defender allocates defense resources to; and the red arrow indicates the attack path from the source to the core node. In the left-hand graph, the defender allocates a defense budget to the blue nodes. If the attacker can obtain complete information about the network, he will try to find the minimal attack cost path to compromise the core node, and avoid passing through the blue nodes. In the right-hand graph, to maximize the attacker's costs, the defender adopts another resource allocation strategy. In response to the defender's strategy, the attacker tries to determine another minimal attack cost path to reach the target node. Our task is to derive an effective defense resource allocation strategy against intelligent attacks, and prevent the core node from being compromised.

Table 2-1 Problem Description of the PSD Model

Given:

1. Network topology
2. Total budget of the defender
3. The cost of compromising a node is a function of the node's budget allocation

Objective:

To maximize the minimized total attack cost

Subject to:

1. Budget constraint of the defender

To determine:

1. The budget allocated to each node by the defender
2. Which nodes will be compromised by the attacker
3. Which routing path will be chosen to reach the core node

Table 2-2 Problem Assumptions of the PSD Model

Assumptions：

1. The attacker is on node *s*.
2. Only one node (node *t*, the core node) is the target of attack.
3. A node *i* is the subject of the attack only if a path exists from node *s* to node *i,* where all the intermediate nodes on the path have been compromised (they can be viewed as hop sites for attacking the target).
4. If $\hat{a}_i(b_i)$ attack cost or more is applied to node *i*, then the node will be compromised.
5. Both the attacker and defender have complete information about the network.
6. The attacker will always find the best strategy to reach the objective.
7. The defender is subject to the total budget constraint.
8. No link attacks are considered.
9. No random failures are considered.
10. The network is viewed at the AS level.

2.1.2 Notations

Given Parameters	
Notation	**Description**
B	Total budget of the defender
N	The index set of nodes in the network
w	The O-D pair (s, t)
P_w	The index set of candidate paths for O-D pair w
δ_{pi}	The indicator function, which is 1 if node i is on path p, and 0 otherwise; $i \in N$, $p \in P_w$
Decision Variables	
Notation	**Description**
y_i	1 if node i is compromised, and 0 otherwise; $i \in N$
x_p	1 if path p is selected as the attack path, and 0 otherwise; $p \in P_w$
b_i	The budget allocated to protect node i; $i \in N$
$\hat{a}_i(b_i)$	The attack cost applied against the budget of node i; $i \in N$

2.1.3 Problem Formulation

Objective function:

$$\max_{b_i} \min_{x_p} \sum_{i \in N} \hat{a}_i(b_i) \sum_{p \in P_w} x_p \delta_{pi} \qquad \text{(IP 1)}$$

subject to:

$$\sum_{i \in N} b_i \le B \qquad \text{(1-1)}$$

$$0 \le b_i \le B \qquad \forall\, i \in N \qquad \text{(1-2)}$$

$$\sum_{p \in P_w} x_p = 1 \qquad \text{(1-3)}$$

$$x_p = 0 \; or \; 1. \qquad \forall\, p \in P_w. \qquad \text{(1-4)}$$

The objective function (IP 1) to maximize the minimized total applied attack cost, where the defender manipulates the budget to maximize the value of the total applied attack cost, while the attacker minimizes it by choosing which path to attack. Constraint (1-1) is the total defense budget constraint for the defender. Constraint (1-2) requires that the budget allocated to each node should be between zero and the total budget *B*. Constraint (1-3) and Constraint (1-4) jointly enforce that exactly one path will be chosen between the given O-D pair.

2.1.4 Problem Reformulation

Objective function:

$$\min_{b_i} -\sum_{i\in N} y_i \hat{a}_i(b_i) \qquad \text{(IP 2)}$$

subject to:

$$\sum_{i\in N} y_i \hat{a}_i(b_i) \le \sum_{i\in N} \delta_{pi} \hat{a}_i(b_i) \qquad \forall\, p \in P_w \qquad \text{(2-1)}$$

$$\sum_{p\in P_w} x_p \delta_{pi} \le y_i \qquad \forall\, i \in N \qquad \text{(2-2)}$$

$$\sum_{p\in P_w} x_p = 1 \qquad \text{(2-3)}$$

$$x_p = 0 \; or \; 1 \qquad \forall\, p \in P_w \qquad \text{(2-4)}$$

$$y_i = 0 \; or \; 1 \qquad \forall\, i \in N \qquad \text{(2-5)}$$

$$\sum_{i\in N} b_i \le B \qquad \text{(2-6)}$$

$$0 \le b_i \le B \qquad \forall\, i \in N. \qquad \text{(2-7)}$$

From the defender’s perspective, we want to maximize the total applied attack cost through the budget allocation to each node. Therefore, we modify the objective function (IP 1) in the form of minimizing the attacker’s negative attack cost (IP 2). Constraint (2-1) requires that the selected path for the O-D pair should be the minimal attack cost path. Constraint (2-2) is the relation between y_i, x_p and δ_{pi}. We use y_i to replace the product of x_p and δ_{pi}, summing over all candidate paths. The substitution further simplifies the Lagrangean relaxation procedures. Constraint (2-3) and Constraint (2-4) jointly enforce exactly that one path will be chosen between the given O-D pair. Constraint (2-5) requires that each node is either compromised or not. Constraint (2-6) is the total budget constraint. Constraint (2-7) requires that the budget allocated to each node should be between zero and the total budget *B*.

2.2 Probabilistic Protection Strategy for Defenders (PPSD) Model

2.2.1 Problem Description and Assumptions

Based on the PSD model, we further assume that there is a probability that each node could be compromised under attack, and attacks on nodes are independent. Therefore, from the attacker's aspect, the probability of compromising the core node successfully is a product of the compromise probability of each node on the attack path between the given O-D pair.

From the defender's perspective, if the defender allocates more defense resources to a node, the compromise probability of the node will be reduced. With limited defense resources, defenders need to adopt a strategy that allocates the defense budget more effectively and economically, to minimize the probability of the core node being compromised.

In the worst case scenario, if the attacker can obtain complete information about the network and intelligent, he will try to find the most unreliable path to compromise the core node, which indicates that the product of the compromise probability of each node along the path is maximal. Meanwhile, the defender will try to make the network more secure by allocating a different budget for each node to minimize the probability that the core node will be compromised.

Table 2-3 Problem Description of the PPSD Model

Given:

1. Network topology
2. Total budget of the defender
3. The probability that a node will be compromised is a function of its budget allocation.

Objective:

To minimize the maximized compromise probability of the network

Subject to:

1. Budget constraint of the defender

To determine:

1. The budget allocated to each node by the defender
2. Which nodes will be attacked by the attacker
3. Which routing path will be chosen to reach the core node

Table 2-4 Problem Assumptions of the PPSD Model

Assumptions：

1. The attacker is on node *s*.
2. Only one node (node *t*, the core node) is the target of attack.
3. A node *i* is the subject of the attack only if a path exists from node *s* to node *i*.
4. Both the attacker and defender have complete information about the network.
5. The attacker will always find the best strategy to reach the objective.
6. The defender is subject to the total budget constraint.
7. No link attacks are considered.
8. No random failures are considered.
9. Attacks on nodes are independent.
10. The network is viewed at the AS level.

2.2.2 Notations

Given Parameters	
Notation	**Description**
B	Total budget of the defender
N	The index set of nodes in the network
w	The O-D pair (s, t)
P_w	The index set of candidate paths for O-D pair w
δ_{pi}	The indicator function, which is 1 if node i is on path p, and 0 otherwise; $i \in N$, $p \in P_w$
Decision Variables	
Notation	**Description**
y_i	1 if node i is compromised, and 0 otherwise; $i \in N$
x_p	1 if path p is selected as the attack path, and 0 otherwise; $p \in P_w$
b_i	The budget allocated to protect node i; $i \in N$
$P_i(b_i)$	The probability of node i being compromised by an attack; $i \in N$

2.2.3 Problem Formulation

Objective function:

$$\min_{b_i} \max_{x_p} \prod_{i \in N} P_i(b_i) \sum_{p \in P_w} x_p \delta_{pi} \qquad \text{(IP 3)}$$

subject to:

$$\sum_{i \in N} b_i \le B \qquad \text{(3-1)}$$

$$0 \le b_i \le B \qquad \forall\, i \in N \qquad \text{(3-2)}$$

$$\sum_{p \in P_w} x_p = 1 \qquad \text{(3-3)}$$

$$x_p = 0 \; or \; 1. \qquad \forall\, p \in P_w. \qquad \text{(3-4)}$$

The objective function (IP 3) is to minimize the maximized probability of compromising the core node, where the defender manipulates the budget to minimize the product of the probability of compromise, while the attacker maximizes it by choosing which path to attack. Constraint (3-1) is the total defense budget constraint for the defender. Constraint (3-2) requires that the budget allocated to each node should be between zero and the total budget *B*. Constraint (3-3) and Constraint (3-4) jointly enforce that exactly one path is chosen between the given O-D pair.

2.2.4 Problem Reformulation

Objective function:

$$\min_{b_i} \sum_{i \in N} \ln P_i(b_i) y_i \qquad \text{(IP 4)}$$

subject to:

$$\sum_{i \in N} -\ln P_i(b_i) y_i \le \sum_{i \in N} -\ln P_i(b_i) \delta_{pi} \qquad \forall\, p \in P_w \qquad (4\text{-}1)$$

$$\sum_{p \in P_w} x_p \delta_{pi} \le y_i \qquad \forall\, i \in N \qquad (4\text{-}2)$$

$$\sum_{p \in P_w} x_p = 1 \qquad (4\text{-}3)$$

$$x_p = 0 \; or \; 1 \qquad \forall\, p \in P_w \qquad (4\text{-}4)$$

$$y_i = 0 \; or \; 1 \qquad \forall\, i \in N \qquad (4\text{-}5)$$

$$\sum_{i \in N} b_i \le B \qquad (4\text{-}6)$$

$$0 \le b_i \le B \qquad \forall\, i \in N. \qquad (4\text{-}7)$$

To simplify this problem, we transform the compromise probability $P_i(b_i)$ of each node i into the weight $-\ln P_i(b_i)$. Therefore, from the defender's perspective, the objective function (IP 4) is to minimize the weight of compromising the core node. Constraint (4-1) requires that the selected path for the O-D pair should be a minimal weight path. Constraint (4-2) is the relation between y_i, x_p and δ_{pi}. We use y_i to replace the product of x_p and δ_{pi}, to sum over all candidate paths. Also, the substitution further simplifies the Lagrangean relaxation procedures. Constraint (4-3) and Constraint (4-4) jointly enforce that exactly one path is chosen between the given O-D pair. Constraint (4-5) stated that each node could be attacked. Constraint (4-6) is the total budget constraint. Constraint (4-7) requires that the budget allocated to each node should be between zero and the total budget *B*.

Chapter 3 Solution Approach

3.1 Lagrangean Relaxation Method

In the 1970s, many solution ideas were proposed to solve complicated integer programming problems [17]. One of them, called decomposition, states that many hard integer programming problems can be viewed as a set of several easier subproblems with side constraints, which are easier to solve. One well-known decomposition solution approach is the Lagrangean relaxation method. In recent years, Lagrangean relaxation has become one of the most popular tools for solving optimization problems, such as integer programming, linear programming, nonlinear programming, and combinational programming problems.

By applying the Lagrangean relaxation method [18], we can dismantle original models by removing some constraints and placing them in the objective function with associated multipliers. The new optimization problem with fewer constraints is called the Lagrangean relaxation problem. For minimization problems, the optimal value of the Lagrangean relaxation problem is always the lower bound of the original problem. To obtain the best lower bound, we have to tune the multipliers of the Lagrangean relaxation problem so that the optimal values of the Lagrangean relaxation subproblems are as large as possible. We can solve these subproblems in a variety of ways, of which the subgradient method would be the most popular technique [17][19].

The fundamental principles of the Lagrangean relaxation method are to decompose the original problem into several easily solvable subproblems, each of which can be viewed as a standalone model. The solution approach permits us to exploit a substantial number of well-known algorithms to solve each subproblem. Therefore, we can locally optimize each subproblem, and then compose the subproblems with the global optimization.

The Lagrangean relaxation method has two main advantages. First, because we decompose the original complicated problem into several easily solvable subproblems, and choose well-known algorithms to solve each subproblem, Lagrangean relaxation is more flexible and the computational complexity of the original complicated problem is significantly reduced [17][19][20]. Second, given the nature of the Lagrangean relaxation method, it can help us obtain the bounds of the objective function, and we can evaluate the solution quality for implementing primal feasible solutions.

Figure 3-1 illustrates the general concepts of the Lagrangean relaxation method, while Figure 3-2 illustrates the detailed procedures of the method.

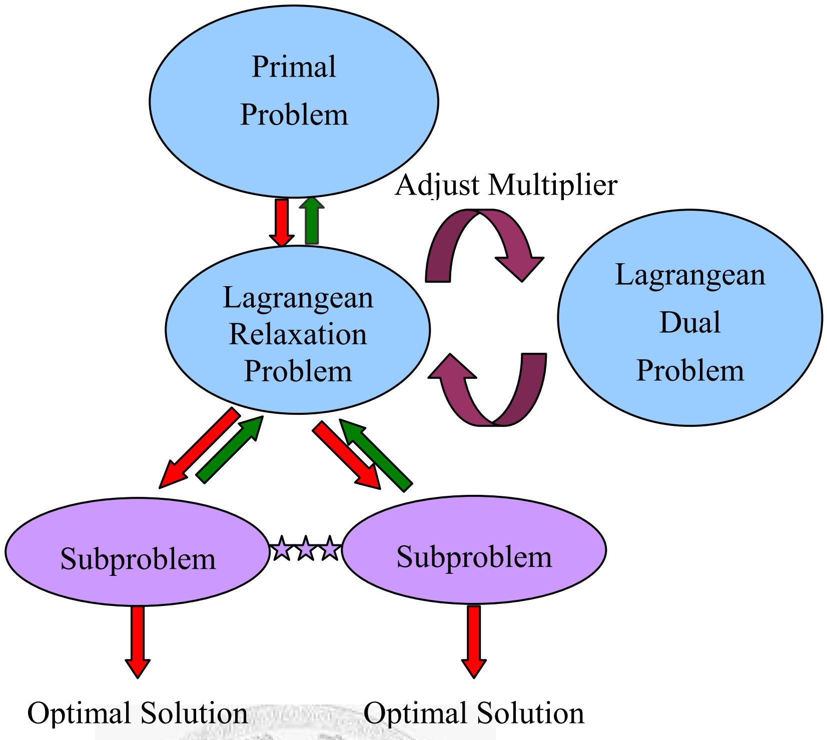

Figure 3-1 Illustration of the Lagrangean Relaxation Method

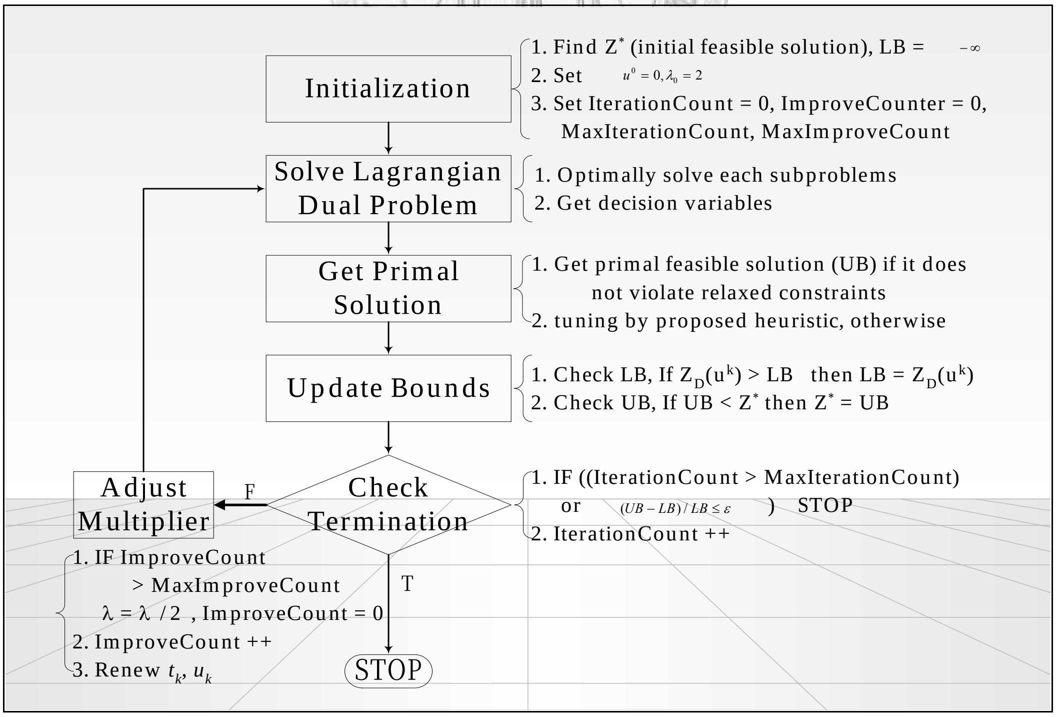
Initialization
1. Find Z* (initial feasible solution), LB = −∞
2. Set $u^0 = 0, \lambda_0 = 2$
3. Set IterationCount = 0, ImproveCounter = 0, MaxIterationCount, MaxImproveCount
Solve Lagrangian Dual Problem
1. Optimally solve each subproblems
2. Get decision variables
Get Primal Solution
1. Get primal feasible solution (UB) if it does not violate relaxed constraints
2. tuning by proposed heuristic, otherwise
Update Bounds
1. Check LB, If $Z_D(u^k)$ > LB then LB = $Z_D(u^k)$
2. Check UB, If UB < Z* then Z* = UB
Check Termination
1. IF ((IterationCount > MaxIterationCount) or $(UB - LB)/LB \le \varepsilon$) STOP
2. IterationCount ++
F
T
STOP
Adjust Multiplier
1. IF ImproveCount > MaxImproveCount λ = λ / 2 , ImproveCount = 0
2. ImproveCount ++
3. Renew t_k, u_k

Figure 3-2 Procedures of the Lagrangean Relaxation Method

3.2 PSD Model

3.2.1 Solution Approach

We transform the reformulation of the PSD model into the following Lagrangean relaxation problem (LR 1) by relaxing Constraints (2-1) and (2-2), with multipliers *u¹* and *u²* respectively. Furthermore, we assume that $\hat{a}_i(b_i)$ is equal to the concave function ln(b_i+1), which indicates that the marginal attack cost of the node will be reduced by the additional budget allocated to a node.

3.2.2 Lagrangean Relaxation

$$Z_{D1}(u^1,u^2) = \min - \sum_{i\in N} y_i \ln(b_i+1) + \sum_{p\in p_w} u_p^1 \sum_{i\in N} (y_i - \delta_{pi}) \ln(b_i+1) + \sum_{i\in N} u_i^2 (\sum_{p\in P_w} x_p \delta_{pi} - y_i) \qquad \text{(LR 1)}$$

subject to:

$$\sum_{p\in P_w} x_p = 1 \qquad \text{(5-1)}$$

$$x_p = 0 \; or \; 1 \qquad \forall\, p \in P_w \qquad \text{(5-2)}$$

$$y_i = 0 \; or \; 1 \qquad \forall\, i \in N \qquad \text{(5-3)}$$

$$\sum_{i\in N} b_i \le B \qquad \text{(5-4)}$$

$$0 \le b_i \le B \qquad \forall\, i \in N. \qquad \text{(5-5)}$$

We can decompose this optimization problem into the following two independent subproblems.

Subproblem 1-1 (related to decision variable x_p)

$$\min \sum_{i\in N}\ \sum_{p\in P_w} u_i^2 x_p \delta_{pi} \qquad \text{(SUB 1-1)}$$

subject to:

$$\sum_{p\in P_w} x_p = 1 \qquad (5\text{-}1)$$

$$x_p = 0\ or\ 1 \qquad \forall\ p \in P_w. \qquad (5\text{-}2)$$

(SUB 1-1) can be viewed as a shortest path problem with a node weight $u_i^2\delta_{pi}$. Because u_i^2 is non-negative, we apply Dijkstra's shortest path algorithm to optimally solve (SUB 1-1). The time complexity is $O(|N|^2)$.

Subproblem 1-2 (related to decision variables y_i, b_i)

$$\min\ (\sum_{p\in p_w} u_p^1 - 1)\sum_{i\in N} y_i \ln(b_i+1) - \sum_{p\in p_w}\ \sum_{i\in N} u_p^1 \delta_{pi} \ln(b_i+1) - \sum_{i\in N} u_i^2 y_i \qquad \text{(SUB 1-2)}$$

subject to:

$$y_i = 0\ or\ 1 \qquad \forall\ i \in N \qquad (5\text{-}2)$$

$$\sum_{i\in N} b_i \le B \qquad (5\text{-}3)$$

$$0 \le b_i \le B \qquad \forall\ i \in N. \qquad (5\text{-}4)$$

(SUB 1-2) can be further decomposed into $|N|$ subproblems. For each node i,

$$\min \ (\sum_{p \in p_w} u_p^1 - 1) y_i \ln(b_i + 1) - \sum_{p \in p_w} u_p^1 \delta_{pi} \ln(b_i + 1) - u_i^2 y_i$$

subject to:

$$y_i = 0 \; or \; 1$$

$$\sum_{i \in N} b_i \le B$$

$$0 \le b_i \le B.$$

To optimally solve (SUB 1-2), we must consider the following three cases:

Case 1, $\sum_{p \in p_w} u_p^1 = 1$. For a node that is not on the selected path X_p (δ_{pi} = 0), we assign b_i = 0. Furthermore, if u_i^2 of the node is more than zero, we assign y_i = 1, and 0 otherwise. For a node that is on the selected path X_p (δ_{pi} = 1), we assign y_i = 1, b_i = B/P, where B denotes the total budget, and P denotes the number of nodes on the selected path X_p.

Case 2, $0 \le \sum_{p \in p_w} u_p^1 < 1$. Initially, we assign all nodes y_i = 1. After applying calculus, if $Pd<B$, then for a node with δ_{pi} = 1, we assign b_i = d; and for a node with δ_{pi} = 0, we assign $b_i = \frac{B - Py}{N - P}$, where $d = \frac{B + (N - P)\sum_{p \in p_w} u_p^1}{P - (\sum_{p \in p_w} u_p^1 - 1)(N - P)}$, and N denotes the number of nodes. If $Pd \ge B$, then for a node with δ_{pi} = 1, we assign b_i = B/P; and for a node with δ_{pi} = 0, we assign b_i = 0. Furthermore, if u_i^2 of the node is equal to zero, we assign y_i = 0.

Case 3, $\sum_{p\in p_w} u_p^1 > 1$. For a node with δ_{pi} = 0, we assign b_i = 0. Furthermore, if u_i^2 of the node is more than zero, we assign y_i = 1 and 0 otherwise. For nodes with δ_{pi} = 1, initially, we assign y_i = 1, and sort them in ascending order, depending on u_i^2. Step by step, we assign the first Q nodes in the order y_i = 0, where Q = 0, 1, 2, …, P. If Q = 0 or P, we assign $b_i = B/P$ to all nodes in that order. If 0 < Q < 0, after applying calculus, the proper value of b_i for the first Q elements in the order is $\frac{B+(P-Q)(1-\sum_{p\in p_w} u_p^1)}{(P-Q)\sum_{p\in p_w} u_p^1+Q}$, and we assign the value to e. If e < 0, we modify e to 0; if Qe > B, then we modify e to B/Q. Therefore, we assign b_i = e to the fist Q nodes in the order, and assign $b_i = \frac{B-Qe}{P-Q}$ to the other nodes in the order. We obtain $(\sum_{p\in p_w} u_p^1 - 1)\sum_{i\in N} y_i \ln(b_i+1) - \sum_{p\in p_w}\sum_{i\in N} u_p^1\delta_{pi}\ln(b_i+1) - \sum_{i\in N} u_i^2 y_i$ after assigning proper values of b_i and y_i to each node. Therefore, we can obtain P+1 values of the above function, and choose the minimal one to optimally solved (SUB 1-2). The time complexity is $O(|N|^2)$.

3.2.3 The Dual Problem and the Subgradient Method

Based on the weak Lagrangean duality theorem [21], the objective value of $Z_{D1}(u^1,u^2)$ is a lower bound of Z_{IP2}. Therefore, we construct the following dual problem (D1) and obtain the tightest lower bound by applying the subgradient method [21].

Dual Problem (D1):

$Z_{D1} = \max Z_{D1}(u^1, u^2)$

subject to:

$u^1, u^2 \geq 0.$

Let the vector S be the subgradient of $Z_{D1}(u^1, u^2)$. Then, in iteration k of the subgradient optimization procedure, the multiplier vector $m^k = (u^{1k}, u^{2k})$ is updated by $m^{k+1} = m^{k+1} + \alpha^k S^k$. The step size α^k is determined by $\rho \frac{{Z_{IP2}}^k - Z_{D1}(m^k)}{\| S^k \|^2}$, where ${Z_{IP2}}^k$ is the best primal objective function value obtained by iteration k, and ρ is a constant where $0 \leq \rho \leq 2$.

3.2.4 Getting Primal Feasible Solution

To obtain a heuristic that solves the problem, information provided by multipliers is very helpful. In this problem, the multiplier vector u_i^2 is adjusted by the function $\sum_{i \in N} (y_i - \delta_{pi}) \hat{a}_i(b_i)$ for each node *i*, which implies the importance of each node *i*. This gives a hint about how to allocate the budget.

In addition, we construct a minimal defense region to improve the solution quality. First, we obtain the minimal number of nodes that need to be compromised by applying Dijkstra’s shortest path algorithm. Then, by applying a labeling process, we obtain an initial defense region. However, as some nodes of the outer layer may be unnecessary, we remove them from the region. Finally, we obtain the minimal defense region, and allocate b_i, where $b_i \sim r_i = \frac{u_i^2}{\text{total } u_i^2}$. If a node has $r_i > 0$, and it is not in the minimal defense region, we allocate its budget to the source and destination node without allocating any budget to the node.

The tuning process allocates the epsilon budget from the source and core node to the other nodes in the minimal defense region. Then, we test if the objective function value is less than the previous state. If it is, we continue the tuning process until the objective function value is no less than the previous state. The time complexity of the heuristic is $O(|N|^2)$.

Table 3-1 Heuristic for the PSD Model

Step 1. Construct a minimal defense region by applying the labeling and the removal processes. The labeling process is based on a breadth-first search, and the removal process tests whether each outer layer node is necessary or not.

Step 2. Allocate b_i to each node, where $b_i \sim r_i = \frac{u_i^2}{\text{total } u_i^2}$, $i \in N$. If a node has $r_i > 0$, and it is not in the minimal defense region, allocate its budget to the source and destination node without allocating any budget to the node.

Step 3. Tune the epsilon budget from the source and core node to the other nodes in the minimal defense region. If the objective function value is less than the previous state, we continue the tuning process recursively.

3.3 PPSD Model

3.3.1 Solution Approach

We can transform the reformulation of the PPSD model into the following Lagrangean relaxation problem (LR 2) by relaxing Constraints (4-1) and (4-2), with multipliers u^1 and u^2 respectively. Furthermore, we assume that $P_i(b_i)$ follows an exponential distribution with λ, which indicates that the compromise probability will be rapidly reduced by the additional budget allocation to a node.

3.3.2 Lagrangean Relaxation

$$Z_{D2} = \min \sum_{i\in N} \ln \lambda e^{-\lambda bi} y_i + \sum_{p\in p_w} u_p^1 \sum_{i\in N} \ln \lambda e^{-\lambda bi} (\delta_{pi} - y_i) + \sum_{i\in N} u_i^2 (\sum_{p\in P_w} x_p \delta_{pi} - y_i) \qquad \text{(LR 2)}$$

subject to:

$$\sum_{p\in P_w} x_p = 1 \qquad (6\text{-}1)$$

$$x_p = 0 \; or \; 1 \qquad \forall \; p \in P_w \qquad (6\text{-}2)$$

$$y_i = 0 \; or \; 1 \qquad \forall \; i \in N \qquad (6\text{-}3)$$

$$\sum_{i\in N} b_i \le B \qquad (6\text{-}4)$$

$$0 \le b_i \le B \qquad \forall \; i \in N. \qquad (6\text{-}5)$$

We can decompose this optimization problem into the following two independent subproblems.

Subproblem 2-1 (related to decision variable *x*$_p$)

$$\min \sum_{i\in N}\ \sum_{p\in P_w} u_i^2 x_p \delta_{pi} \qquad \text{(SUB 2-1)}$$

subject to:

$$\sum_{p\in P_w} x_p = 1 \qquad \text{(6-1)}$$

$$x_p = 0 \; or \; 1 \qquad \forall\ p \in P_w. \qquad \text{(6-2)}$$

(SUB 2-1) can be viewed as a shortest path problem with a node weight $u_i^2\delta_{pi}$. Because u_i^2 is non-negative, we apply Dijkstra's shortest path algorithm to optimally solve (SUB 2-1). The time complexity is $O(|N|^2)$.

Subproblem 2-2 (related to decision variables y_i, b_i)

$$\min\ (1-\sum_{p\in p_w} u_p^1)\sum_{i\in N}\ln \lambda e^{-\lambda bi} y_i + \sum_{p\in p_w} u_p^1 \sum_{i\in N}\ln \lambda e^{-\lambda bi}\delta - \sum_{i\in N} u_i^2 y_i \qquad \text{(SUB 2-2)}$$

subject to:

$$y_i = 0 \; or \; 1 \qquad \forall\ i \in N \qquad \text{(6-2)}$$

$$\sum_{i\in N} b_i \le B \qquad \text{(6-3)}$$

$$0 \le b_i \le B \qquad \forall\ i \in N. \qquad \text{(6-4)}$$

(SUB 2-2) can be further decomposed into $|N|$ subproblems. For each node i,

$$\min \ (1-\sum_{p\in p_w} u_p^1)\ln \lambda e^{-\lambda bi} y_i + \sum_{p\in p_w} u_p^1 \ln \lambda e^{-\lambda bi} \delta_{pi} - u_i^2 y_i$$

subject to:

$y_i = 0 \ or\ 1$

$\sum_{i\in N} b_i \le B$

$0 \le b_i \le B.$

To optimally solve (SUB 2-2), we have to consider the following three cases:

Case 1, $\sum_{p\in p_w} u_p^1 = 1$. For a node that is not on the selected path X_p (δ_{pi} = 0), we assign b_i = 0. Furthermore, if u_i^2 of the node is more than zero, we assign y_i = 1 and 0 otherwise. For a node that is on the selected path X_p (δ_{pi} = 1), we assign y_i = 1, and record its λ. Therefore, we assign b_i = B to the node with the maximal λ, and assign the other nodes b_i = 0.

Case 2, $0 \le \sum_{p\in p_w} u_p^1 < 1$. Initially, we assign all nodes y_i = 1. For a node with δ_{pi} = 0, we record the value $(\sum_{p\in p_w} u_p^1 - 1)\lambda$; and for a node with δ_{pi} = 1, we record the value $-\lambda$. Therefore we assign b_i = B to the node with minimal value, and b_i = 0 to the other nodes.

Case 3, $\sum_{p\in p_w} u_p^1 > 1$. For a node with δ_{pi} = 0, we assign b_i = 0. Furthermore, if $(1-\sum_{p\in p_w} u_p^1)\ln \lambda - u_i^2$ of the node is less than zero, we assign y_i = 1, and 0 otherwise.

For a node with δ_{pi} = 1, we compute the critical point $C.P. = \frac{(1-\sum_{p\in p_w} u_p^1)\ln\lambda - u_i^2}{(1-\sum_{p\in p_w} u_p^1)\lambda}$. If $C.P. < 0$, we record the value $-\sum_{p\in p_w} u_p^1\lambda$; if $C.P. \geq B$, we record the value -λ; and if $0 \leq C.P. < B$, we record the value $\frac{-\sum_{p\in p_w} u_p^1\lambda B + (\sum_{p\in p_w} u_p^1 - 1)\ln\lambda + u_i^2}{B}$. After recording the values of all nodes with δ_{pi} = 1. We assign $b_i = B$ to the node with minimal value, and b_i = 0 to the other nodes. For the node with minimal value, if its value is equal to –λ, we assign y_i = 1, and 0 otherwise. For the other nodes with δ_{pi} = 1, if $\sum_{p\in p_w} u_p^1 \ln\lambda < \ln\lambda - u_i^2$, we assign y_i = 0, and 1 otherwise. After assigning appropriate values of b_i, y_i to each node, we can optimally solve (SUB 2-2). The time complexity is $O(|N|)$.

3.3.3 The Dual Problem and the Subgradient Method

Based on the weak Lagrangean duality theorem [21], the objective value of $Z_{D2}(u^1, u^2)$ is a lower bound of Z_{IP4}. Therefore, we construct the following dual problem (D2) and obtain the tightest lower bound by applying the subgradient method [21].

Dual Problem (D2):

$Z_{D2} = \max Z_{D2}(u^1, u^2)$

subject to:

$u^1, u^2 \geq 0.$

Let the vector S be the subgradient of $Z_{D2}(u^1, u^2)$. Then, in iteration k of the subgradient optimization procedure, the multiplier vector $m^k = (u^{1k}, u^{2k})$ is updated by $m^{k+1} = m^{k+1} + \alpha^k S^k$. The step size α^k is determined by $\rho \frac{Z_{IP4}{}^k - Z_{D2}(m^k)}{\| S^k \|^2}$, where $Z_{IP4}{}^k$ is the best primal objective function value obtained by iteration k, and ρ is a constant where $0 \le \rho \le 2$.

3.3.4 Getting Primal Feasible Solution

Based on the getting primal feasible solution for the PSD model, we construct a minimal defense region to improve the solution quality. Then we adopt the multiplier vector u_i^2 as a hint to allocate b_i, where $b_i \sim r_i = \frac{u_i^2}{\text{total } u_i^2}$. If a node with $r_i > 0$ is not in the minimal defense region, we allocate its budget to the source or destination node, depending on which one has the bigger λ.

The tuning process extracts the epsilon budget from the source or core node that has the bigger λ, and allocates it to the nodes in the minimal defense region, one by one. Then we can determine which of the nodes we allocated the epsilon budget to will result in the most negative effect of the objective value. If the value of the objective function is less than the previous state, we continue the tuning process until that value is no less than the previous state.

After finishing the tuning process, we compare the objective function’s value with another heuristic that is based on the primal variable b_i. By applying the LR method, we can obtain the value of the primal variable b_i for each node. Therefore, we can derive a primal-based heuristic, which allocates the budget to each node according to the value of the primal variable b_i when we solve (SUB 2-2). Then we compare the primal-based heuristic with the original heuristic, and obtain the minimal objective value of the heuristics. The time complexity of the entire heuristic is O($|N|^3$).

Table 3-2 Heuristic for the PPSD Model

Step 1. Construct a minimal defense region by applying the labeling and the removal process. The labeling process is based on a breadth-first search, and the removal process tests whether each outer layer node is necessary.

Step 2. Allocate b_i to each node, where $b_i \sim r_i = \frac{u_i^2}{\text{total } u_i^2}, i \in N$. If a node with $r_i > 0$ is not in the minimal defense region, we allocate its budget to the source or destination node, depending on which one has the bigger λ.

Step 3. Tune the epsilon budget from the source and core node to the node in the minimal defense region, which has the most negative effect of the objective value. If the value of the objective function value is less than the previous state, we continue the tuning process recursively.

Step 4. Compare with the primal-based heuristic, which allocates the budget to each node according to the value of the primal variable $b_{i.}$ Then we determine the minimal objective value of the heuristics.

Chapter 4 Computational Experiments

4.1 Computational Experiments on the PSD Model

4.1.1 Experiment Environments

The algorithm we propose is written in C, and implemented on a notebook with an INTEL$^{\text{TM}}$ Pentium-M 1.5GHz environment; the other experimental parameters are shown in **Table 4-1**. In this model, to present a homogenous network, we assume that $\hat{a}_i(b_i)$ is the same for each node. The LR denotes the attack costs of the algorithm we propose, and the LB indicates the theoretical attack costs

In addition, we propose two simple and one primal-based algorithms to compare the attack costs of different defense resource allocation strategies. Simple algorithm 1 allocates b_i uniformly, and the SA1 denotes the attack costs of the algorithm. In simple algorithm 2, the allocation of b_i is proportionate to the ratio $\frac{\text{Links of a node}}{\text{Total Links}}$, and the SA2 denotes the attack costs of simple algorithm 2. In the primal-based algorithm, the budget allocation for each node is according to the value of primal variable b_i, which is obtained by solving (SUB 1-2). HE3 denotes the attack costs of the primal-based heuristic. In addition, the gap is computed by $\frac{\text{LB-LR}}{\text{LR}}*100\%$; the survivability factor is calculated by $\frac{\text{LR}}{\text{LB}}$; and the improvement ratio is calculated by $\frac{\text{LR-Attack Costs of an Algorithm}}{\text{Attack Costs of an Algorithm}}*100\%$; Finally, we transform the objective value into being positive by obtaining the absolute value of it for easy illustration.

Table 4-1 Experimental Parameter Settings for the PSD Model

Parameter	Value
Number of Nodes	16~361
Number of Links	60~1440
Network Topology	Grid, Random, and Scale-Free Networks
Number of Iterations	2000
Improvement Counter	100
Initial Scalar of Step Size	1
Initial Upper Bound	The 1st Getting Primal Feasible Solution
Test Platform	CPU: INTEL$^{\text{TM}}$ Pentium-M 1.5GHz RAM: 768MB OS: Microsoft Windows XP

4.1.2 Experiment Results

In **Figure 4-1**, the attack costs determined by our proposed algorithm are always higher than those of the other algorithms. In the large networks, the differences are particularly significant. In addition, the proposed algorithm provides a stable level of protection for the core node, even in different-sized networks and topologies. **Figure 4-2** shows the survivability factor of scale-free networks. The survivability factor of the proposed algorithm is consistently higher than that of the other algorithms. Thus, by applying the proposed algorithm, the core node will be more robust and secure.

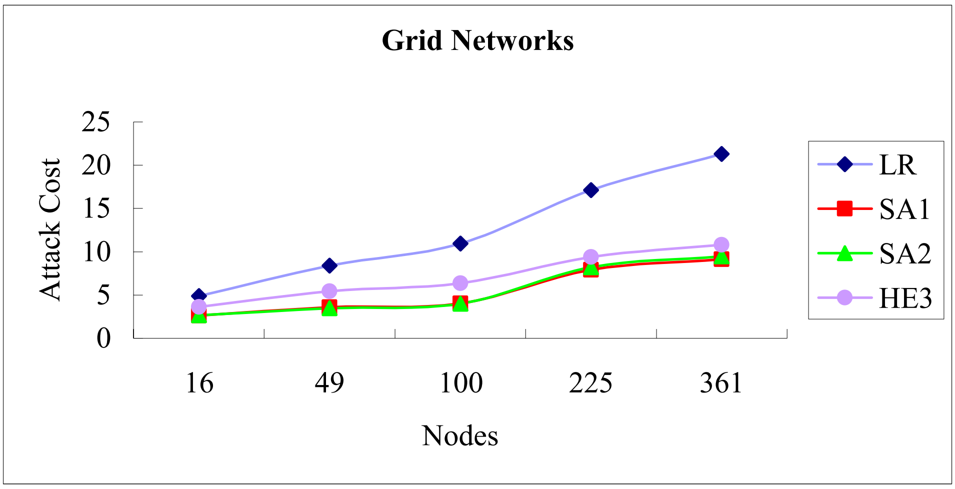

Figure 4-1 Experiment Results for Grid Networks

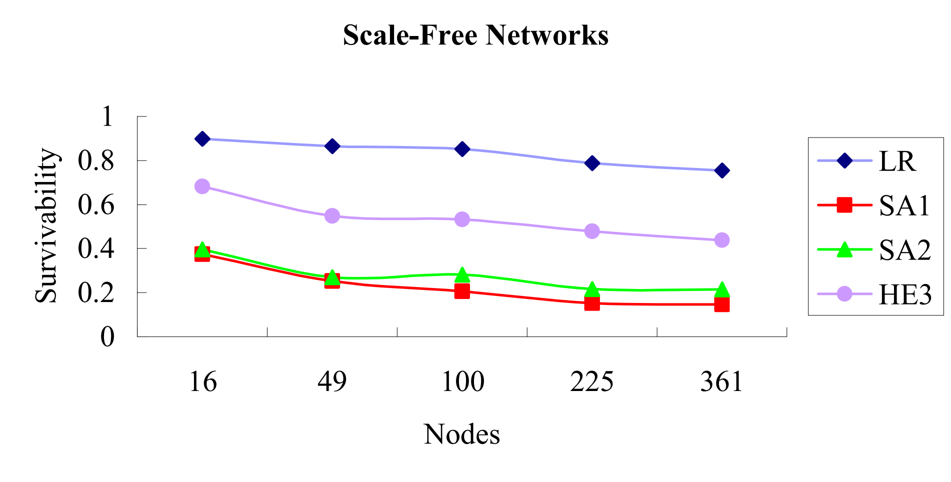

Figure 4-2 Survivability of Scale-Free Networks

After experimenting with the proposed algorithm in different-sized network topologies, we find the interesting phenomenon illustrated in **Figure 4-3**. When the network size is large, the attack costs in grid networks are higher than those in random and scale-free networks. To determine the reason for this phenomenon, we initially select an O-D pair in a network at random, and apply Dijkstra's shortest path algorithm to determine the minimal number of nodes that must be compromised between the O-D pair. We execute the above process one hundred times and draw the probability distribution of the average number of nodes that must be compromised between an O-D pair. We observe that the average number of nodes that must be compromised in a grid network is much more than in a random or scale-free network, as shown in **Figure 4-4**. This is due to the small-world phenomenon. Therefore, we can conclude that the depths of defense are the important factor about survivability. The detail experiment results are summarized in **Table 4-2.**

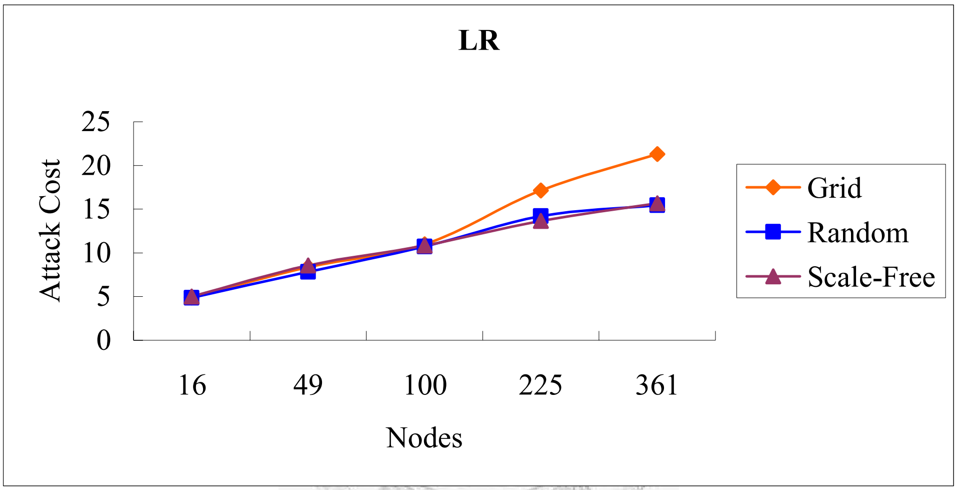

Figure 4-3 Experiment Results for Different Network Topologies

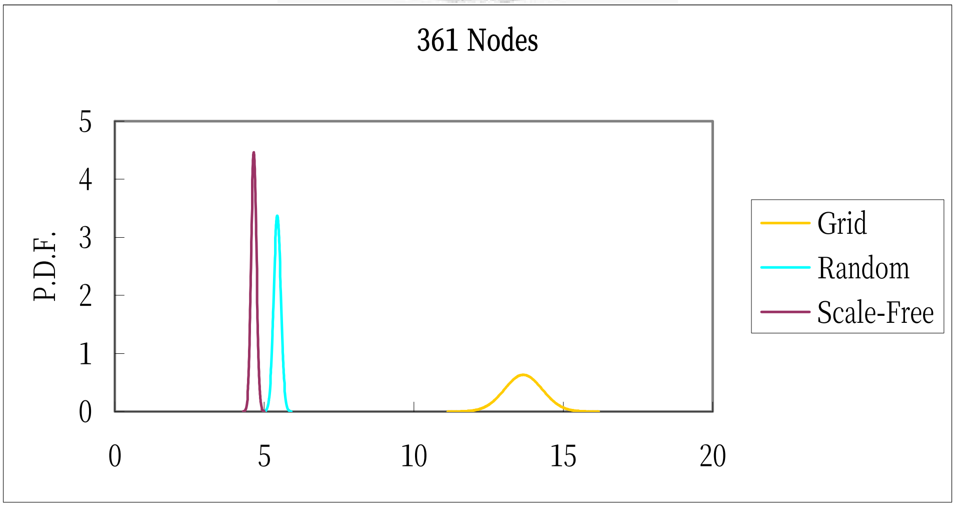

Figure 4-4 Average Number of Nodes Must be Compromised Distribution

Table 4-2 Experiment Results for the PSD Model

Topology	No. of Nodes	LB	LR	Gap (%)	Surv.	SA1	Imp. Ratio to SA1 (%)	SA2	Imp. Ratio to SA2 (%)	HE3	Imp. Ratio to HE3 (%)
Grid Networks	16	6.23	4.89	27.37	0.79	2.63	85.84	2.67	83.12	3.62	35.37
	49	12.18	8.40	45.05	0.69	3.60	132.92	3.46	142.54	5.43	54.65
	100	16.80	10.96	53.26	0.65	4.02	172.70	3.99	174.73	6.37	72.13
	225	36.08	17.14	110.51	0.48	7.90	116.92	8.22	108.55	9.38	82.77
	361	46.51	21.29	118.51	0.46	9.15	132.65	9.48	124.45	10.79	97.26
Random Networks	16	5.74	4.87	17.99	0.85	2.22	119.45	2.40	102.49	3.97	22.53
	49	9.36	7.84	19.34	0.84	2.36	232.78	2.52	211.70	5.53	41.90
	100	15.50	10.71	44.70	0.69	3.33	221.96	3.53	203.68	6.76	58.37
	225	21.30	14.22	49.82	0.67	3.47	310.31	3.84	270.24	8.40	69.21
	361	25.65	15.43	66.22	0.60	3.60	328.21	4.29	260.06	8.52	81.19
Scale-Free Networks	16	5.56	5.00	11.31	0.90	2.08	140.36	2.20	127.00	3.79	31.83
	49	9.90	8.56	15.65	0.86	2.50	242.94	2.66	221.13	5.42	57.82
	100	12.74	10.85	17.41	0.85	2.63	311.93	3.58	203.13	6.79	59.81
	225	17.32	13.65	26.86	0.79	2.63	418.34	3.74	265.27	8.30	64.57
	361	20.77	15.66	32.62	0.75	3.05	413.47	4.47	250.35	9.11	71.97

4.2 Computational Experiments on the PPSD Model

4.2.1 Experiment Environments

The algorithm we propose is written in C, and implemented on a PC with an INTEL^{TM} Pentium-4 2.0GHz environment, and the other experimental parameters are shown in **Table 4-3**. In this model, to present a heterogeneous network, we assume that $P_i(b_i)$ is different for each node.

In the PPSD model scenario 1, by the 20/80 rule, we assume that 20% of the nodes in the network are more important than the other 80%. Therefore, we assume that $P_i(b_i)$ for these 20% nodes follows an exponential distribution with the smaller $\lambda(\lambda_1)$, and the other 80% of nodes follow an exponential distribution with the larger $\lambda(\lambda_2)$. Note that the λ represents the initial compromise probability of each node. In the PPSD model scenario 2, we assume that $P_i(b_i)$ for an O-D pair follows an exponential distribution with a randomly selected λ between [0, 0.5]. Because the source node and the core node are important, we assume that the O-D pair has a certain level of protection initially. For the other nodes, we assume that $P_i(b_i)$ follows an exponential distribution with a randomly selected λ between [0, 1]. The LR denotes the attack costs of the proposed algorithm, and the other symbols are still the same as we have mentioned in the section 4.1.1.

Table 4-3 Experimental Parameter Settings for the PPSD Model

Parameter	Value
Number of Nodes	16~361
Number of Links	60~1440
Network Topology	Grid, Random, and Scale-Free Networks

Set of $(\lambda_{1,} \lambda_2)$	(0.1, 0.2), (0.1, 0.3), (0.1, 0.4);
	(0.2, 0.4), (0.2, 0.6), (0.2, 0.8);
	(0.3, 0.5), (0.3, 0.7), (0.3, 0.9)

Number of Iterations	2000
Improvement Counter	50
Initial Scalar of Step Size	1
Initial Upper Bound	The 1st Getting Primal Feasible Solution
Test Platform	CPU: INTEL^{TM} Pentium-4 2.0GHz RAM: 1GB OS: Microsoft Windows 2000

4.2.2 Experiment Results

In the PPSD model scenario 1, for comparison with other two simple algorithms, the proposed algorithm incurs much higher attack costs, and maintains a high level of protection in different-sized network topologies, as shown in **Figures 4-5 and 4-6**.

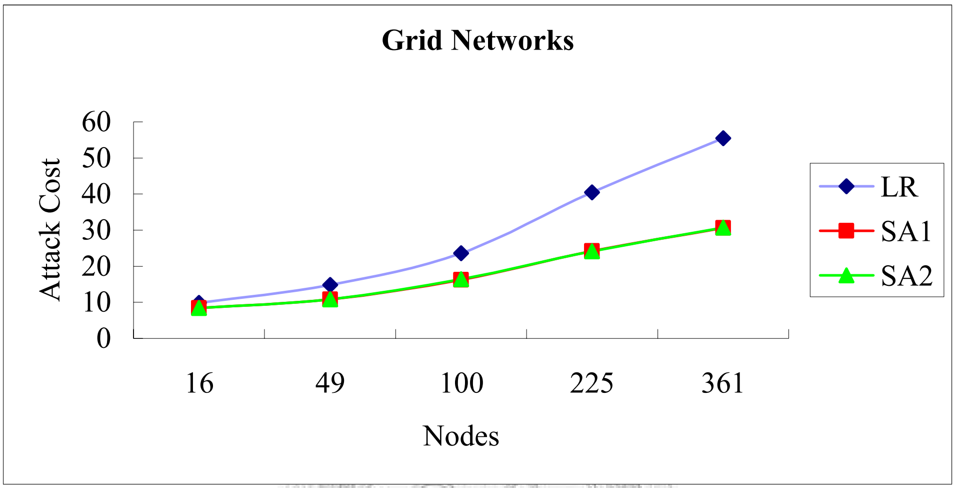

Figure 4-5 Experiment Results for the PPSD Model Scenario 1 in Grid Networks (λ_1=0.1, λ_2=0.2)

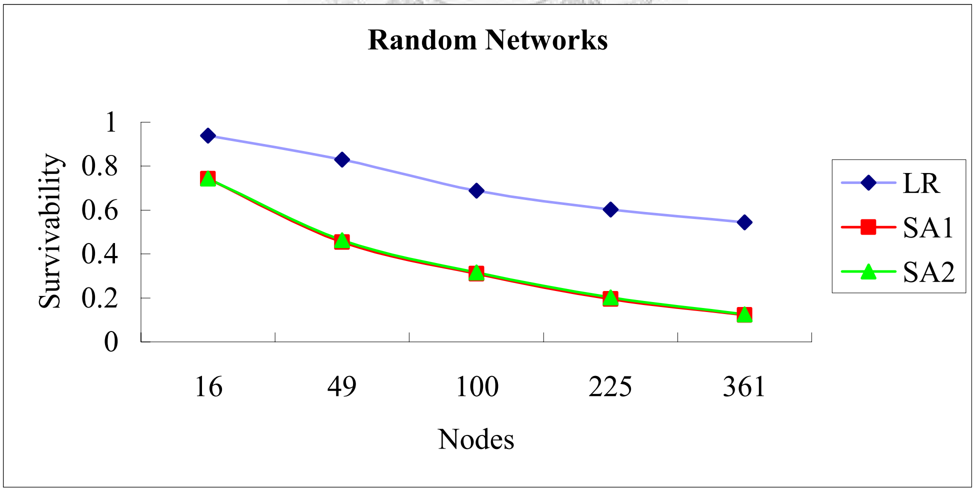

Figure 4-6 Survivability of the PPSD Model Scenario 1 in Random Networks (λ_1=0.1, λ_2=0.2)

In the PPSD model scenario 1, if we assume that the similar λ_1, λ_2 to the more important nodes and other nodes respectively, the network is similar to a homogeneous network. Therefore, the depths of defense have a strong influence on the attack costs. In grid networks, the attacker has to compromise more nodes than in the other two network topologies, which increases his attack costs. The phenomenon is significant, especially if the network size is large, as shown in **Figure 4-7**.

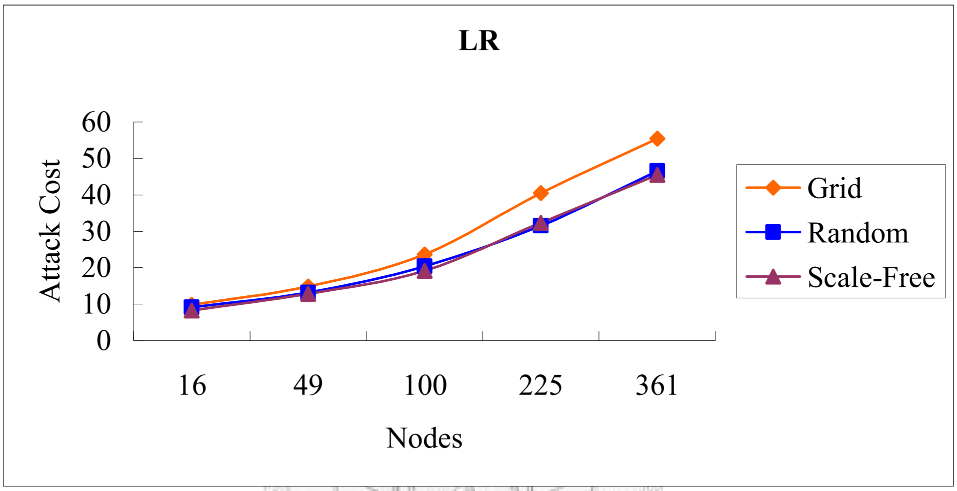

Figure 4-7 Experiment Results for the PPSD Model Scenario 1 in Different Network Topologies (λ_1=0.1, λ_2=0.2)

However, if λ_1 is different from λ_2, we must consider more about the node characteristics, such as the importance and the $P_i(b_i)$ function of each node. For example, a node with a substantial number of links that provides short cuts from the source node to the destination node is very important in a scale-free network. If the node is vulnerable (especially with a bigger λ), we should allocate the defense resources to reduce the risk of the node being compromised, which would improve the protection of the core node. In a random network, we focus on the vulnerable nodes that have short cuts to the core node, and allocate the defense resources so that the protection of the core node is improved. Because the effects of the node characteristics are more than those of the depths of defense, the attack costs in scale-free networks are higher than those in the other two network topologies, especially if the network size is large, as shown in **Figure 4-8**. After testing several combinations of λ_1 and λ_2, we observe that if the difference between λ_1 and λ_2 is significant, the defender has to consider more about the node characteristics, instead of the depths of defense. The more the difference between λ_1 and λ_2 is, the more the impact of node characteristics, as shown in **Figure 4-9**, **Figure 4-10**.

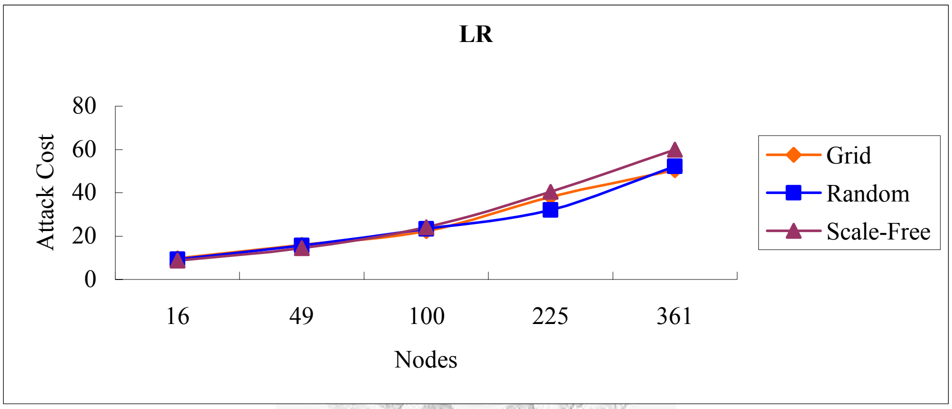

Figure 4-8 Experiment Results for the PPSD Model Scenario 1 in Different Network Topologies (λ_1=0.1, λ_2=0.4)

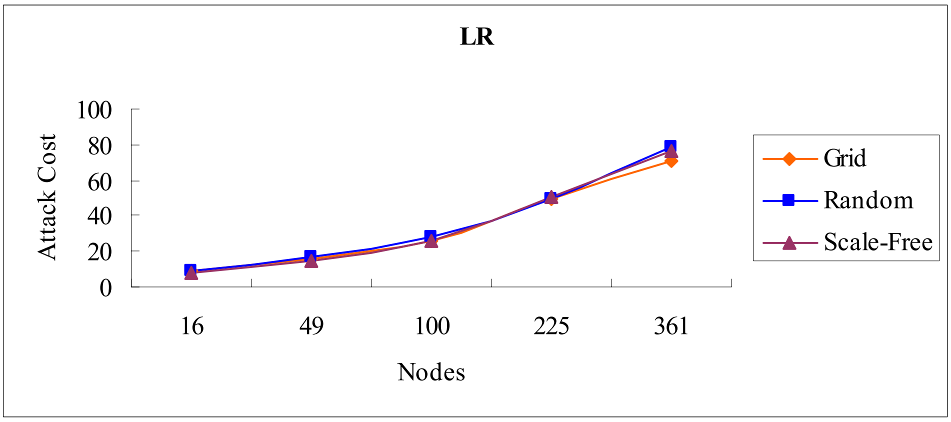

Figure 4-9 Experiment Results for the PPSD Model Scenario 1 in Different Network Topologies (λ_1=0.2, λ_2=0.4)

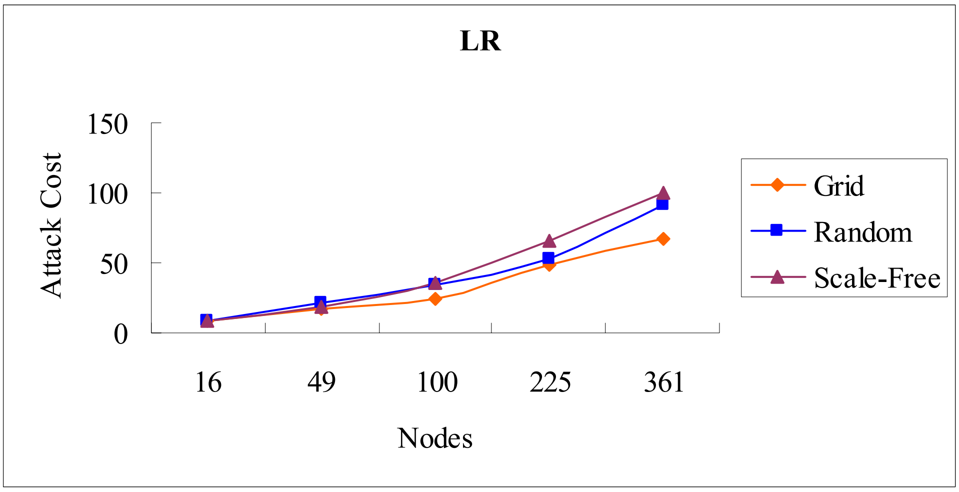

Figure 4-10 Experiment Results for the PPSD Model Scenario 1 in Different Network Topologies (λ_1=0.2, λ_2=0.8)

In the PPSD model scenario 2, we assume that the O-D pair initially has a certain level of protection, and the other nodes have random protection. In different-sized network and topologies, the proposed algorithm incurs more attack costs and maintains a higher level of survivability than that of the other algorithms, as shown in **Figure 4-11** and **Figure 4-12**.

Considering both the depths of defense and node characteristics, the attack costs of the proposed algorithm are approximately equal in different-sized networks and topologies, as shown in **Figure 4-13**. This implies the proposed protection strategy is very adaptive, and we can obtain almost the same effects even in different network sizes and topologies.

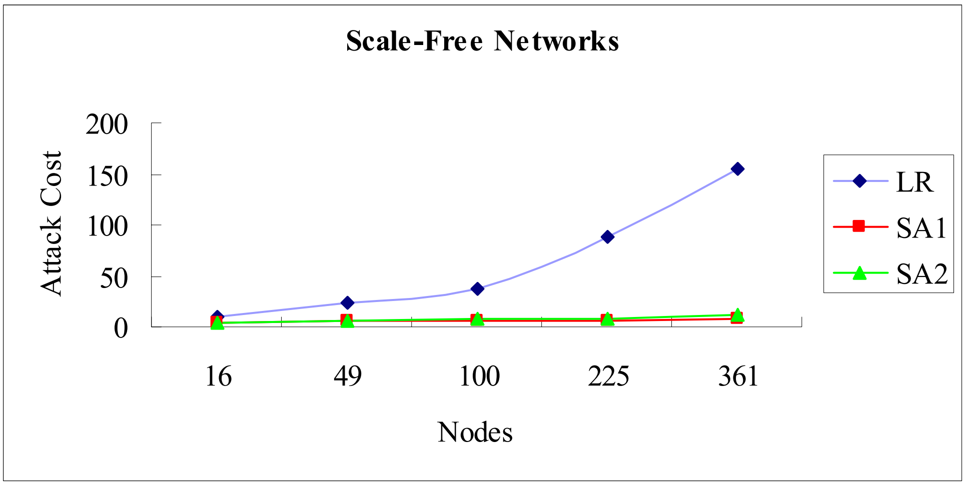

Figure 4-11 Experiment Results for the PPSD Model Scenario 2 in Scale-Free Networks

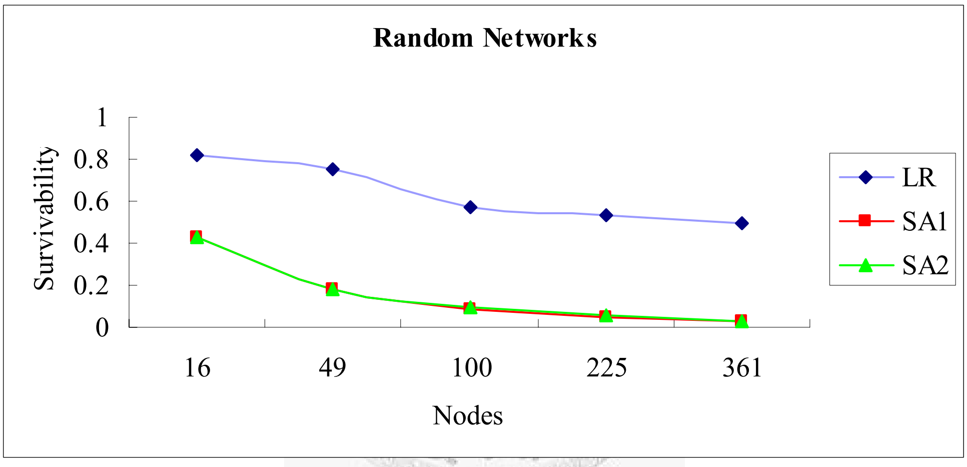

Figure 4-12 Survivability of the PPSD Model Scenario 2 in Random Networks

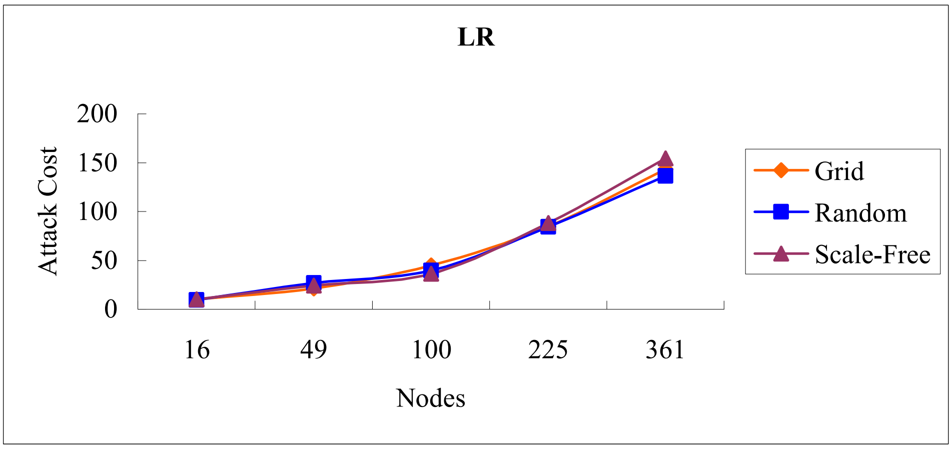

Figure 4-13 Experiment Results for the PPSD Model Scenario 2 in Different Network Topologies

Table 4-4 Experiment Results for the PPSD Model Scenario 1 (λ_1=0.1, λ_2=0.2)

Topology	No. of Nodes	LB	LR	Gap (%)	Surv.	SA1	Imp. Ratio to SA1 (%)	SA2	Imp. Ratio to SA2 (%)
Grid Networks	16	11.05	9.81	12.63	0.89	8.42	16.49	8.43	16.40
	49	20.18	14.86	35.81	0.74	10.83	37.17	10.83	37.18
	100	34.47	23.61	46.02	0.68	16.26	45.20	16.39	44.06
	225	69.56	40.50	71.72	0.58	24.22	67.22	24.18	67.50
	361	104.31	55.46	88.08	0.53	30.61	81.17	30.75	80.34
Random Networks	16	9.71	9.12	6.46	0.94	7.21	26.49	7.22	26.32
	49	15.87	13.18	20.46	0.83	7.21	82.66	7.35	79.18
	100	29.55	20.35	45.19	0.69	9.15	122.47	9.34	117.95
	225	52.37	31.54	66.03	0.60	10.23	208.23	10.57	198.36
	361	85.57	46.55	83.81	0.54	10.46	344.85	10.71	334.67
Scale-Free Networks	16	8.81	8.29	6.17	0.94	6.25	32.64	6.33	30.94
	49	17.74	12.86	37.93	0.72	8.18	57.23	8.74	47.18
	100	28.95	19.12	51.43	0.66	8.90	114.69	9.53	100.63
	225	56.68	32.37	75.12	0.57	10.47	209.10	11.61	178.81
	361	85.76	45.48	88.58	0.53	10.71	324.72	11.86	283.56

Table 4-5 Experiment Results for the PPSD Model Scenario 1 (λ_1=0.1, λ_2=0.3)

Topology	No. of Nodes	LB	LR	Gap (%)	Surv.	SA1	Imp. Ratio to SA1 (%)	SA2	Imp. Ratio to SA2 (%)
Grid Networks	16	11.84	9.68	22.22	0.82	7.81	23.95	7.82	23.84
	49	23.94	15.38	55.68	0.64	9.98	54.15	9.98	54.16
	100	40.60	22.80	78.09	0.56	14.49	57.34	14.68	55.34
	225	88.11	38.64	128.03	0.44	21.11	83.07	21.05	83.58
	361	135.63	52.13	160.16	0.38	26.58	96.14	26.79	94.61
Random Networks	16	10.70	9.20	16.31	0.86	6.97	31.96	6.99	31.58
	49	19.50	14.39	35.55	0.74	6.97	106.42	7.16	100.94
	100	38.67	21.62	78.90	0.56	8.41	156.87	8.69	148.75
	225	69.56	31.10	123.66	0.45	9.32	233.79	9.81	216.96
	361	120.77	49.35	144.72	0.41	9.91	397.75	10.26	381.01
Scale-Free Networks	16	9.74	8.48	14.95	0.87	6.01	41.09	6.12	38.51
	49	22.02	13.39	64.40	0.61	7.69	74.11	8.52	57.12
	100	38.31	21.56	77.73	0.56	8.29	159.92	9.20	134.20
	225	78.65	35.63	120.75	0.45	9.68	268.20	11.28	215.79
	361	120.76	50.73	138.03	0.42	10.04	405.53	11.38	346.02

Table 4-6 Experiment Results for the PPSD Model Scenario 1 (λ_1=0.1, λ_2=0.4)

Topology	No. of Nodes	LB	LR	Gap (%)	Surv.	SA1	Imp. Ratio to SA1 (%)	SA2	Imp. Ratio to SA2 (%)
Grid Networks	16	12.85	9.76	31.58	0.76	7.44	31.25	7.44	31.13
	49	28.04	15.93	76.04	0.57	9.45	68.52	9.45	68.54
	100	47.34	22.23	113.00	0.47	13.40	65.86	13.65	62.87
	225	108.11	38.11	183.68	0.35	19.19	98.56	19.12	99.36
	361	168.33	50.46	233.60	0.30	24.10	109.35	24.38	106.97
Random Networks	16	11.63	9.28	25.39	0.80	6.82	36.02	6.85	35.43
	49	23.19	15.70	47.73	0.68	6.82	130.20	7.06	122.38
	100	48.04	23.37	105.51	0.49	7.96	193.50	8.32	180.80
	225	86.89	32.01	171.40	0.37	8.75	265.70	9.38	241.25
	361	156.52	52.18	199.93	0.33	9.58	444.89	10.02	420.70
Scale-Free Networks	16	10.78	8.66	24.52	0.80	5.86	47.76	6.00	44.26
	49	26.29	14.45	81.99	0.55	7.39	95.44	8.49	70.06
	100	47.64	24.05	98.13	0.50	7.92	203.68	9.12	163.77
	225	100.66	40.37	149.36	0.40	9.19	339.34	11.23	259.60
	361	156.68	59.93	161.44	0.38	9.62	522.76	11.05	442.15

Table 4-7 Experiment Results for the PPSD Model Scenario 1 (λ_1=0.2, λ_2=0.4)

Topology	No. of Nodes	LB	LR	Gap (%)	Surv.	SA1	Imp. Ratio to SA1 (%)	SA2	Imp. Ratio to SA2 (%)
Grid Networks	16	11.54	8.50	35.67	0.74	6.25	36.03	6.26	35.74
	49	26.38	15.98	65.02	0.61	8.03	99.09	8.03	99.13
	100	46.93	25.60	83.30	0.55	11.98	113.75	12.22	109.58
	225	105.89	49.77	112.77	0.47	17.77	180.08	17.69	181.37
	361	165.34	71.01	132.83	0.43	22.44	216.44	22.72	212.51
Random Networks	16	10.38	8.69	19.53	0.84	5.40	61.02	5.42	60.43
	49	22.51	16.62	35.45	0.74	5.40	207.97	5.68	192.77
	100	46.51	28.23	64.78	0.61	6.78	316.44	7.16	294.34
	225	89.58	49.11	82.40	0.55	7.57	548.98	8.11	505.85
	361	154.10	78.26	96.89	0.51	7.80	903.69	8.29	844.35
Scale-Free Networks	16	9.71	7.68	26.47	0.79	4.67	64.37	4.83	58.84
	49	24.81	14.99	65.51	0.60	6.09	146.27	7.20	108.15
	100	46.24	25.86	78.82	0.56	6.61	291.03	7.84	229.68
	225	98.72	50.10	97.04	0.51	7.77	545.25	9.88	407.29
	361	154.63	76.07	103.29	0.49	7.96	855.32	9.57	694.84

Table 4-8 Experiment Results for the PPSD Model Scenario 1 (λ_1=0.2, λ_2=0.6)

Topology	No. of Nodes	LB	LR	Gap (%)	Surv.	SA1	Imp. Ratio to SA1 (%)	SA2	Imp. Ratio to SA2 (%)
Grid Networks	16	13.98	8.38	66.78	0.60	5.84	43.54	5.85	43.21
	49	35.04	16.62	110.88	0.47	7.45	122.95	7.45	123.00
	100	60.95	25.23	141.55	0.41	10.79	133.97	11.13	126.64
	225	147.08	47.94	206.76	0.33	15.67	205.90	15.56	208.22
	361	232.84	68.74	238.72	0.30	19.73	248.42	20.15	241.18
Random Networks	16	12.52	8.88	41.00	0.71	5.23	69.69	5.27	68.40
	49	30.02	19.17	56.62	0.64	5.23	266.43	5.61	241.61
	100	65.62	30.95	112.05	0.47	6.28	392.38	6.83	352.76
	225	124.61	48.47	157.11	0.39	6.95	597.22	7.72	527.73
	361	225.49	83.95	168.60	0.37	7.43	1030.21	8.12	934.14
Scale-Free Networks	16	11.97	8.22	45.60	0.69	4.51	82.44	4.73	73.82
	49	34.01	16.33	108.26	0.48	5.76	183.63	7.13	129.02
	100	65.37	31.13	109.98	0.48	6.20	401.95	7.77	300.59
	225	142.83	57.34	149.10	0.40	7.23	692.99	9.92	478.00
	361	226.23	89.28	153.40	0.39	7.51	1088.73	9.43	846.78

Table 4-9 Experiment Results for the PPSD Model Scenario 1 (λ_1=0.2, λ_2=0.8)

Topology	No. of Nodes	LB	LR	Gap (%)	Surv.	SA1	Imp. Ratio to SA1 (%)	SA2	Imp. Ratio to SA2 (%)
Grid Networks	16	16.48	8.62	91.22	0.52	5.67	52.15	5.68	51.79
	49	44.04	17.47	152.14	0.40	7.21	142.32	7.21	142.37
	100	75.69	24.64	207.13	0.33	10.28	139.80	10.71	130.06
	225	189.37	48.32	291.91	0.26	14.78	226.96	14.62	230.41
	361	301.64	67.45	347.24	0.22	18.57	263.16	19.13	252.63
Random Networks	16	14.71	9.17	60.45	0.62	5.16	77.61	5.22	75.57
	49	37.48	21.77	72.18	0.58	5.16	321.72	5.64	285.84
	100	84.84	34.78	143.89	0.41	6.07	472.64	6.79	411.96
	225	159.92	52.45	204.88	0.33	6.69	684.25	7.63	587.20
	361	296.79	90.91	226.45	0.31	7.27	1150.55	8.16	1014.15
Scale-Free Networks	16	14.29	8.86	61.33	0.62	4.44	99.64	4.72	87.63
	49	43.15	18.90	128.28	0.44	5.62	236.46	7.22	161.82
	100	84.78	36.34	133.26	0.43	6.03	503.03	7.83	364.14
	225	187.12	65.97	183.64	0.35	7.00	842.05	9.93	564.53
	361	297.63	100.19	197.07	0.34	7.32	1269.19	9.54	950.73

Table 4-10 Experiment Results for the PPSD Model Scenario 1 (λ_1=0.3, λ_2=0.5)

Topology	No. of Nodes	LB	LR	Gap (%)	Surv.	SA1	Imp. Ratio to SA1 (%)	SA2	Imp. Ratio to SA2 (%)
Grid Networks	16	11.83	8.74	35.28	0.74	5.39	62.11	5.41	61.51
	49	29.68	19.24	54.27	0.65	6.95	176.79	6.95	176.89
	100	54.44	30.59	77.99	0.56	10.53	190.47	10.77	184.06
	225	124.81	61.77	102.07	0.49	15.78	291.44	15.64	294.97
	361	197.19	92.03	114.26	0.47	19.96	361.06	20.32	352.99
Random Networks	16	10.83	9.04	19.86	0.83	4.56	97.98	4.58	97.11
	49	26.26	20.19	30.04	0.77	4.56	342.37	4.93	309.20
	100	55.13	35.99	53.17	0.65	5.87	513.01	6.36	466.24
	225	110.49	68.40	61.54	0.62	6.59	938.32	7.17	854.39
	361	188.53	111.45	69.16	0.59	6.66	1573.54	7.29	1427.86
Scale-Free Networks	16	10.32	8.08	27.76	0.78	3.96	103.93	4.18	93.49
	49	28.56	18.51	54.26	0.65	5.22	254.78	6.49	185.45
	100	54.74	33.73	62.30	0.62	5.70	492.26	7.06	377.53
	225	119.60	69.51	72.06	0.58	6.71	935.64	9.28	648.78
	361	189.16	108.85	73.79	0.58	6.84	1492.24	8.72	1147.55

Table 4-11 Experiment Results for the PPSD Model Scenario 1 (λ_1=0.3, λ_2=0.7)

Topology	No. of Nodes	LB	LR	Gap (%)	Surv.	SA1	Imp. Ratio to SA1 (%)	SA2	Imp. Ratio to SA2 (%)
Grid Networks	16	14.41	8.36	72.31	0.58	5.12	63.25	5.14	62.62
	49	38.54	18.93	103.57	0.49	6.57	188.22	6.57	188.33
	100	68.73	30.34	126.56	0.44	9.74	211.53	10.07	201.20
	225	166.83	60.68	174.92	0.36	14.39	321.78	14.20	327.28
	361	265.42	90.52	193.21	0.34	18.16	398.48	18.65	385.34
Random Networks	16	13.03	9.29	40.24	0.71	4.45	108.60	4.49	106.74
	49	33.83	22.34	51.40	0.66	4.45	401.53	4.92	353.67
	100	74.38	38.78	91.81	0.52	5.54	599.46	6.20	525.55
	225	145.46	67.88	114.30	0.47	6.18	998.67	6.95	876.36
	361	259.77	113.73	128.41	0.44	6.41	1673.21	7.25	1468.95
Scale-Free Networks	16	12.64	8.26	53.04	0.65	3.85	114.33	4.13	100.07
	49	37.64	18.88	99.43	0.50	5.00	277.54	6.51	189.82
	100	74.15	35.89	106.61	0.48	5.42	561.87	7.08	406.58
	225	163.86	72.03	127.48	0.44	6.36	1033.13	9.29	675.56
	361	260.66	111.65	133.47	0.43	6.54	1608.23	8.76	1174.39

Table 4-12 Experiment Results for the PPSD Model Scenario 1 (λ_1=0.3, λ_2=0.9)

Topology	No. of Nodes	LB	LR	Gap (%)	Surv.	SA1	Imp. Ratio to SA1 (%)	SA2	Imp. Ratio to SA2 (%)
Grid Networks	16	17.02	8.14	109.06	0.48	5.02	62.24	5.04	61.60
	49	47.63	19.26	147.28	0.40	6.42	199.83	6.42	199.95
	100	83.67	29.53	183.28	0.35	9.44	212.85	9.85	199.73
	225	209.44	60.19	247.96	0.29	13.86	334.15	13.59	342.90
	361	333.86	89.76	271.96	0.27	17.48	413.43	18.11	395.64
Random Networks	16	15.29	9.60	59.21	0.63	4.41	117.57	4.47	114.65
	49	41.35	24.95	65.72	0.60	4.41	465.32	4.98	400.66
	100	93.84	41.70	125.04	0.44	5.42	669.21	6.25	567.61
	225	180.99	67.55	167.91	0.37	6.02	1021.41	6.96	870.82
	361	331.77	121.30	173.52	0.37	6.32	1818.81	7.36	1548.85
Scale-Free Networks	16	14.98	8.94	67.61	0.60	3.81	134.46	4.15	115.51
	49	46.93	20.37	130.39	0.43	4.92	314.24	6.59	209.21
	100	93.66	41.42	126.13	0.44	5.32	678.68	7.16	478.52
	225	208.01	79.83	160.55	0.38	6.22	1182.77	9.35	753.90
	361	332.48	121.77	173.05	0.37	6.42	1795.79	8.97	1256.87

Table 4-13 Experiment Results for the PPSD Model Scenario 2

Topology	No. of Nodes	LB	LR	Gap (%)	Surv.	SA1	Imp. Ratio to SA1 (%)	SA2	Imp. Ratio to SA2 (%)
Grid Networks	16	14.42	10.16	41.94	0.70	6.48	56.73	6.76	50.25
	49	36.52	21.35	71.08	0.58	6.92	208.31	7.00	205.13
	100	88.08	44.82	96.52	0.51	10.07	345.24	10.33	333.77
	225	177.25	84.61	109.49	0.48	8.92	848.95	9.07	832.54
	361	329.29	143.17	129.99	0.43	15.84	804.07	16.18	784.67
Random Networks	16	11.79	9.65	22.24	0.82	5.05	91.03	5.07	90.12
	49	35.78	26.84	33.29	0.75	6.47	315.02	6.60	306.45
	100	69.09	39.65	74.25	0.57	6.06	553.77	6.36	523.22
	225	159.10	84.18	89.00	0.53	8.25	919.80	8.97	838.00
	361	275.29	136.34	101.92	0.50	7.86	1634.07	8.18	1565.90
Scale-Free Networks	16	11.56	10.08	14.63	0.87	4.45	126.51	4.65	117.01
	49	36.98	24.32	52.05	0.66	5.72	325.06	6.56	270.59
	100	57.41	36.36	57.90	0.63	6.61	450.19	7.60	378.44
	225	153.33	88.17	73.90	0.58	6.49	1258.63	8.70	912.94
	361	284.94	154.44	84.50	0.54	7.86	1865.08	11.22	1277.05

Chapter 5 Conclusion

5-1 Summary

In this thesis, we clearly formulate the attack-defense behavior, and propose an effective and adaptive defense resource allocation strategy. It works very well, even in different-sized networks and topologies. In addition, we propose a survivability factor to quantitatively analyze the protection of the network. The higher the factor, the more protection the network has.

In a homogeneous network, the most important issue for the defender to allocate the budget is the depth of defense. Because the grid network doesn't have the short cuts, the attacker has to compromise more nodes than in an attack on random or scale-free network. Therefore, the defender can obtain more depths of defense to deploy the defense resources, while the attacker has to overcome more obstacles established by the defender. The defense in depth protection strategy conducts that the attack costs in a grid network are higher than in random and the scale-free networks, especially if the network size is large.

However, if the network is heterogeneous, the defender should pay more attention to the node characteristics. In random and scale-free networks, we focus on the nodes that provide short cuts and are vulnerable. We then allocate the budgets to them to improve the protection of the core node. It conducts that the attack costs in scale-free network are higher than in gird and random networks, especially if the network size is large. The more the differences between nodes are, the more impacts of node characteristics. The proposed solution approach is very effective and adaptive in different scenarios.

In addition, by applying the proposed protection strategy, we can obtain a threshold of the attack cost a_t. Therefore, if we know the probability distribution of the total attack power A of the attacker, we can obtain another novel survivability factor, which is equal to $P(A|A>a_t)$.

5-2 Future Work

Until now, there has been little research on the functions $\hat{a}_i(b_i)$, $P_i(b_i)$. In our experiments, we assume that $\hat{a}_i(b_i)$ follows a concave function $\ln(b_i+1)$, and $P_i(b_i)$ follows an exponential distribution with different λ. The $\hat{a}_i(b_i)$ and $P_i(b_i)$ functions will be an interesting research topic in the future.

In this thesis, we only consider single core node. However, enterprises and organizations may have more than one core node to protect. For example, a bank with many branches may store its transaction data in different places. Therefore, in the future, we may consider multiple core nodes, and propose a good solution approach for defenders to allocate their defense resources.

A vulnerable choke point can be viewed as another important node in a network. In the PPSD model, if a choke point exists and is vulnerable, the best protection strategy is to allocate the budget to that node. Therefore, finding vulnerable choke points is a very interesting topic in the future. In **Figure 5-1**, the pink node denotes the vulnerable choke point.

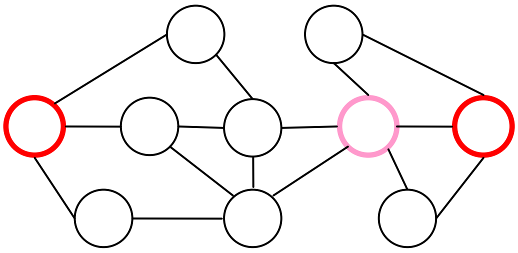

Figure 5-1 Choke Point Example

The total attack power distribution is another interesting research topic that we know very little about. If we can learn more about it, we may adopt it and propose a more effective protection strategy to help defenders against attacks.

In addition, game theory could be considered. In this thesis, we formulate the attack-defense behavior as a mathematical model. However, with the rapid development of game theory, we may adopt it to solve network attack-defense problems in the future.

In this thesis, the network topology is given. However, if the defender can decide how to construct the network, it will be more helpful for him to develop the protection strategy against targeted attacks. For example, if the defender can construct a linear defense region, with deep depths of defense. Therefore, the attacker has to overcome more obstacles than other network topologies. However, the availability of the network is limited, e.g., the delay of the network is significant because the packet has to cross much more hops. The network structure is another aspect we could consider, and it is a trade-off between availability and security.

References

[1] http://www.cert.org/stats/cert_stats.html

[2] Simon Hansman, Ray Hunt, "A Taxonomy of Network and Computer Attacks," *Computers and Security*, Elsevier, U.K., Vol 24, No 1, 2005, pp31-43.

[3] Michael Faloutsos, Petros Faloutsos , and Christos Faloutsos , "On Power-Law Relationships of the Internet Topology," *Computer Communications Review* 29, pp. 251-263, 1999.

[4] Westmark V. R, "A Definition for Information System Survivability," in *Proceedings of the 37th Hawaii Internal Conference on System Sciences* (HICSS'04), Track 9, 2004.

[5] Ellison, R. J., R. C. Linger, T. Longstaff, N. R. Mead, "A Case Study in Survivable Network System Analysis," SEI, Sep 1998.

[6] U.S. Department of Commerce, National Telecommunications and Information Administration, Institute for Telecommunications Services, Federal Standard 1037C.

[7] Nicol, DM; Sanders, WH; Trivedi, KS, "Model-Based Evaluation: from Dependability to Security", *Dependable and Secure Computing*, IEEE Transactions on Volume 1, Issue 1, Jan 2004.

[8] J. C. Knight and K. J. Sullivan, "On the definition of survivability," Technical Report CS-TR-33-00, University of Virginia, Department of Computer Science, 2000.

[9] D. Y. Chen, S. Garg, and K. S. Trivedi, "Network Survivability Performance Evaluation: A Quantitative Approach with Applications in Wireless Ad-hoc

Networks," *MSWiM'02*, page 61-68, September 28, 2002.

[10] Molisz, W., "Survivability Function - a Measure of Disaster-Based Routing Performance," *Selected Areas in Communications*, IEEE Journal on Volume 22, Issue 9, Nov. 2004 pp. 1876 – 1883.

[11] J.C. Knight, K. Sullivan, M.C. Elder, and C. Wang, "Survivability Architectures: Issues and Approaches," in *Proceedings of the DARPA Information Survivability Conference and Exposition*, pages 157–171, Los Alamitos, California, January 2000. IEEE Computer Society Press.

[12] Erdos, P. & Renyi A., "On the evolution of random graphs," *Publ. Math. Inst. Sci.* 5, pp. 17-60, 1960.

[13] Albert-Laszlo Barabasi and E. Bonabeau, "Scale-Free Networks," *Scientific American* 288, 60-69 (2003).

[14] Duncan J. Watts and Steven H. Strogatz, "Collective Dynamics of 'Small-World' Networks," *Nature* 393, pp. 440-442, 1998.

[15] Reka Albert, Hawoong Jeong, and Albert-Laszlo Barabasi, "Diamater of the World Wide Web," *Nature* 401, pp. 130-131, 1999.

[16] Reka Albert, Hawoong Jeong, and Albert-Laszlo Barabasi, "Error and Attack Tolerance of Complex Networks," *Nature* 406, pp. 378-381, 2000.

[17] M. L. Fisher, "The Lagrangean Relaxation Method for Solving Integer Programming Problems," *Management Science*, Volume 27, Number 1, pp. 1-18, January 1981.

[18] M. L. Fisher, "An Application Oriented Guide to Lagrangean Relaxation," *Interfaces*, Volume 15, Number 2, pp. 10-21, April 1985.

[19] A. M. Geoffrion, "Lagrangean Relaxation and its Use in Integer Programming,"

Mathematical Programming Study, Volume 2, pp. 82-114, 1974.

[20] M.S. Bazaraa, H.D. Sherali, and C.M. Shetty, “Lagrangian Duality and Saddle Point Optimality Conditions,” *Nonlinear Programming: Theory and Algorithms*, 2nd Edition, pp. 199-242, John Wiley & Sons, Inc, Singapore, 1993.

[21] M. Held, *et al.*, “Validation of subgradient optimization,” *Math. Programming*, vol. 6, pp. 62-88, 1974.

簡　　歷

姓　　名：林義倫

出 生 地：臺灣省臺北市

出 生 日：中華民國七十一年三月二十五日

學　　歷：

學　士　八十九年九月至九十三年六月

國立中正大學資訊管理學系

碩　士　九十三年九月至九十五年七月

國立臺灣大學資訊管理學研究所