國立臺灣大學資訊管理研究所

碩士論文

指導教授： 林永松 博士

顏宏旭 博士

考慮智慧型惡意攻擊下之
網路存活度最大化

Maximization of Network Survivability against Intelligent and Malicious Attacks

研究生：陳建宏 撰

中華民國九十四年七月

考慮智慧型惡意攻擊下之
網路存活度最大化

Maximization of Network Survivability against Intelligent and Malicious Attacks

本論文係提交國立台灣大學
資訊管理研究所作為完成碩士
學位所需條件之一部分

研究生：陳建宏　撰

中華民國九十四年七月

謝 誌

親手按下印表機的列印鍵，看著我的論文一頁一頁熱騰騰地印出，心中感觸實在良多。本篇論文能夠如期完成，要感謝的人實在是太多了。首先要感謝的是生我養我的父母：陳登科先生與余麗玲女士。感謝父母給我良好的環境與全力的支持，您們的言教、身教，帶給我很大的影響與啟發，也讓我能順利走完這趟恍如隔世的研究學習過程。

在研究所的求學過程中，感謝許多老師鼓勵與指導，使這篇論文能順利完成。首先感謝恩師林永松博士，在研究所這兩年，老師引領我進入網路最佳化的學術殿堂，並讓我學習到紮實的研究精神與待人接物的道理。顏宏旭博士在這兩年內，不厭其煩的指導我，讓我的論文內容更為精進，在此謝謝老師。感謝王柏堯博士適時的伸出援手，您的學術研究熱忱以及與學生互動的親和力讓我印象深刻。而口試期間，承蒙交大資科林盈達博士、清大電機趙啟超博士、輔大資工呂俊賢博士對學生論文的指正及提出建議，使本論文能更為嚴謹，成果更為豐碩。

感謝資安小組的成員：柏皓學長、中蓮、義倫，你們總是適時的提出許多寶貴建議，讓我的論文能更為完整精進，能夠與各位一起切磋研究，是我的榮幸。特別感謝旭成學長在這兩年內的幫忙，你的學術研究精神也讓我深感佩服。書平、琳智、明源、孝澤，與你們共同切磋，使我的論文更加完善。也謝謝弘翕、文政、勇誠，你們在我枯燥的研究生活中注入了許多樂趣與溫暖。

我還要感謝所有在這段時間內鼓勵我、支持我的朋友們，你們是讓我能夠繼續堅強走下去的動力。很高興認識你們這一群朋友。

陳建宏　謹識
于台大資訊管理研究所
民國九十四年七月

論文摘要

自從美國 911 攻擊事件發生之後，如何有效保護重要資訊基礎建設已成為一個重要的課題。而同為重要資訊基礎建設之一的網際網路，在近年來，隨著駭客入侵與攻擊重要主機事件層出不窮，網路安全議題亦逐漸受到專家重視。然而在理論與實務上，資訊安全都告訴我們，沒有任何系統是百分之百的安全。因此我們不應該問「這個系統安不安全」，而是要關心「這個系統有多安全」。量化的「存活度」概念便應運而生，成為網路安全專家衡量一個網路處於不正常（包含隨機錯誤與惡意攻擊）的狀態下，維持正常服務程度的效能指標。

另外，網路攻防也是網路安全專家所關心的議題。為了有效提升網路的存活度，網路營運者必須投資一筆固定預算並加以妥善配置。而相對的，攻擊者針對網路營運者所採用的資源配置策略，也會因應調整其攻擊方式，以最少的攻擊成本達成攻擊目的。

在本篇論文中，我們首先評估一個既有網路的存活度，也就是討論在給定的網路拓樸中，給定一種資源配置策略，一個攻擊者攻擊成功所需花費的最小成本；隨後我們討論：在一個給定的網路中，網路營運者（防禦者）投資一筆固定預算的情況下，應該如何有效的配置資源，才能使得攻擊者攻擊成功所花費的總成本最大。攻防的標的我們設定為：若干給定關鍵節點之間的正常連結。此時我們假設攻擊者是夠聰明的，在給定的防禦資源配置策略下，攻擊者總是能夠找到最小的攻擊成本策略，使得給定的關鍵節點之間無法連通。

我們將整個問題仔細地分析成最佳化數學模型，而這個問題在本質上是一個非線性混合整數規劃問題，具有高度的複雜度與困難度。我們採用以拉格蘭日鬆弛法為基礎的演算法來處理此一問題。在實驗設計方面，我們針對隨機網路、格狀網路與無尺度網路這三種不同網路拓樸，討論其網路的存活特性。

另外，我們針對這個問題的特性，提出了一個數學證明。我們也在最後提出許多豐富議題供後人從事相關研究。

關鍵詞：網路規劃、最佳化、拉格蘭日鬆弛法、數學規劃、存活度、資訊安全、網路攻防、資源配置、無尺度網路

THESIS ABSTRACT

GRADUATE INSTITUTE OF INFORMATION MANAGEMENT
NATIONAL TAIWAN UNIVERSITY
NAME: CHIEN-HUNG CHEN MONTH/YEAR: JULY, 2005
ADVISER: YEONG-SUNG LIN
HONG-HSU YEN

MAXIMIZATION OF NETWORK SURVIVABILITY AGAINST INTELLIGENT AND MALICIOUS ATTACKS

Since the 911 terrorist attacks in the United States, how to protect critical information infrastructures effectively has become an even more important topic. One critical information infrastructure, the Internet, has drawn increasing attention from network security experts because of the growing number of malicious attacks on it. However, experience tells us that, in both theory and practice, a system cannot be 100% secured. Therefore, we should not ask “Is the system secure?” but “How secure is the system?” A quantitative “survivability” concept has become an important performance metric for evaluating how a network sustains normal services under abnormal conditions, including random errors and malicious attacks.

Other issues of interest to network security experts are network attack and defense scenarios. To enhance network survivability effectively, a network operator needs to invest a fixed amount of budget and distribute it properly. However, a potential attacker will always adjust his attack strategies to compromise a network with the minimal cost, if he knows the resource allocation policy of a network operator.

In this thesis, we first evaluate the survivability of a given network. That is, we assess the minimal attack cost incurred by an attacker, under given network topologies and budget allocation policies. We then discuss how a network operator should allocate fixed budget resources such that the minimal attack cost incurred by an attacker can be maximized. The target of the attack and defense is assumed to be the connectivity of given critical OD-pairs. In cases of budget allocation decisions, we assume that an attacker is smart enough, so he can always find the strategy of minimal attack cost to disconnect critical OD-pairs.

We analyze the problems as optimization-based models, in which the problem structures are by nature nonlinear with mixed integer programming. To resolve such difficult problems, we adopt Lagrangean relaxation-based algorithms in conjunction with a number of optimization techniques. In the experimental design, we also evaluate the network survivability properties of different network topologies, including random networks, grid networks, and scale-free networks. In addition, we present a lemma based on the problem's properties.

We believe our work could provide the foundation for evaluating network survivability under various attack and defense scenarios. To this end, we conclude by indicating several interesting and challenging research directions.

Keywords: Information Security, Lagrangean Relaxation, Mathematical Programming, Network Attack and Defense, Network Planning, Optimization, Resource Allocation, Scale-free Networks, Survivability

Contents

List of Figures

List of Tables

Chapter 1 Introduction

1.1 Background

The events of 911 have led to a globally increasing focus on security and especially the protection of critical infrastructures, which encompass a wide array of physical assets, such as power plants, telecommunications, oil and gas pipelines, transportation networks, and computer data networks [2]. Specifically, the Internet has become a critical information infrastructure since 1980s. More and more people communicate with each other via this fascinating technological medium, and the prevailing Internet has made the world borderless. Moreover, many companies exploit the Internet to gain access to suppliers and customers, and also reduce transaction costs. E-commerce, for example, has emerged since the late 1990s, and has become a new business model attracting much attention.

Despite these advantages, the popularity of the Internet also caused potential problems. Since important messages and sensitive data flowing around the Internet may be eavesdropped or fabricated, information security experts have suggested different encryption algorithms and authenticated protocols to deal with the problems. Moreover, a potential attacker may discourage important servers from offering normal services. To handle malicious attack behaviors, information security experts have suggested different tools and strategies that focus on different network attack modes. For example, firewalls are used to filter illegal packets; intrusion detection systems (IDSs) are designed for detecting possible intrusion patterns; intrusion prevention systems (IPSs) are used to prevent intrusions of susceptible packets and reduce the probability of potential attack behaviors. Multi-function security gateways combine the above functions and have become widely adopted by network operators.

Despite the availability of various software and hardware tools, no one can be sure that a system is 100% robust against attacks. As this phenomenon is due to the imperfection of software programming and communication protocols, there is at least the possibility that malicious attackers could find the vulnerabilities of a system and deliver attacks to compromise it. However, through applying security mechanisms that have different levels for the systems, we can efficiently reduce the probability of being targeted by attackers and therefore enhance the level of robustness.

However, the robustness of a network consists in not only the availability of each component, but also the network's topological structure. The Internet topology has been shown to follow a power-law degree distribution [3] [4] [5], where empirical evidence has highlighted one major weakness in that the Internet is highly susceptible to attacks. Looked at in more detail, the average performance of the Internet would be cut in half if only 1% of the most highly-connected routers were incapacitated, and if 4% of the most connected routers succumbed to attacks, the integrity of the medium could be destroyed [2]. The secrets behind the Internet topology have drawn much attention from network researchers.

In addition, many researchers have focused their research on evaluating and enhancing the survivability of a network. Survivability is used to depict how a network adapts to abnormal conditions. An increasing number of researchers are engaged in network survivability issues, researching proper definitions of survivability, estimating suitable survivability metrics, and proposing solutions to different scenarios.

To enhance the survivability of a network, a network operator may invest a fixed amount of budget. However, there has been little theoretical research to enable a network operator to gain a global understanding on how to allocate limited budgets to components so that the overall survivability of a network can be maximized. Besides, we believe that a network operator's budget allocation strategies should consider responses from an attacker, due to the fact that an attacker may change his strategies to a better one if he finds other easier ways to attain his goals. It is therefore a challenging issue for a network operator to derive sensible defense strategies against attacks.

1.2 Motivation

From our survey of the literature, there has been little research on the issues of defense and attack based on mathematical programming models. To the best of our knowledge, no mathematical model that mentions defense and attack behavior in the context of survivability has been proposed. We therefore propose mathematical models under realistic scenarios to evaluate the network robustness for given defense resource allocation policies. We will also present a lemma to show the best resource allocation strategy for network operators under given scenarios.

1.3 Literature Survey

We will first introduce the concept of survivability, and then discuss the properties of scale-free networks in the literature survey.

1.3.1 From Information Security to Survivability

With the prevalence of the Internet, a great number of people have become highly relied on the convenient technological medium to communicate. However, new technologies also bring new problems. Due to the distributed and unsecured design of the Internet, data packets flowing around the nets may suffer from eavesdropping or packet drop. Therefore, issues such as confidentiality, availability, integrity, and privacy have become important topics, and many information security experts have proposed various encryption algorithms, authentication protocols, and so on, to secure communications. Moreover, other attack modes, such as Denial of Services (DoS) and Distributed Denial of Services (DDoS) focus on discouraging devices from providing normal services. Although information security experts continue proposing countermeasures to known attacks or intrusions, the war between network operators and attackers will never end since number of system vulnerabilities and possible attack modes are potentially infinite.

A key to defeat attackers is to think one more step than attackers. However, attackers may also think like this way. If both parties are smart enough, eventually there is equilibrium between them. A game theoretic framework would be helpful in describing this scenario: attackers try their best to attain a goal while network operators, or defenders, try their best to discourage it. By definition of game theories, it is a typical two person zero-sum game.

In [6], the authors consider the problem of detecting an intruding packet in a communication network. Detection is accomplished by sampling a portion of the packets, due to the high cost for real-time packet sampling and packet examination software. Network operators would like to effectively sample network intrusions by maximizing the chance of detection while not exceeding a given total sampling budget. However, a smart intruder would select paths in order to minimize chances of detection. The authors further well-describe the problem through mathematical formulation methods. The objective of an intruder is to minimize the maximal detection probability where that of a service provider is to maximize the minimal detection probability. According to the theorem in this paper, the two values will be the same. That is to say, $\theta = \min_{q \in V} \max_{p \in U} \sum_{P \in P_a^t} q(P)[\sum_{e \in P} P_e] = \max_{p \in U} \min_{q \in V} \sum_{P \in P_a^t} q(P)[\sum_{e \in P} P_e]$, where *q(P)* is a probability distribution function that path *P* is selected by an intruder, and P_e is a probability of detecting a malicious packet on link *e*.

In summary, the game theoretic framework provides us with an insight that a minimization of maximization or a maximization of a minimization objective is useful in describing the interaction between the two parties, an attacker and a defender.

The concept of security has been generalized as survivability in recent years.

Since there are only two states, safe and compromised, in the context of security, it is definitely insufficient to well-describe how likely a system remains functional under different failure scenarios. Moreover, with the popularity of the Internet, a system or a network is inevitably connected to the unbounded Internet, leading to more risk suffering from undesired failures. We should therefore focus more on the system recoverability and the ability of maintaining normal services when failures occur.

The concept of survivability is proposed accordingly. Survivability is roughly defined as the ability a system can fulfill a mission in a timely manner, under attacks, errors, or catastrophic failures [7]. Note that the survivability of a system is not only determined by any single component of it, but depends on a global cooperative effort. That means we have to pay attention to not only the reliability of each component, but also the global topological information, such that we can find a substitution once any component is failed for some reason.

According to the author of [8], the definitions of survivability in the literature vary case by case. Roughly speaking, survivability can be defined as how well a network or a system can be sustained under random errors or malicious attacks, or both. Survivability can be further measured by means of time sustainability during accidents, the probability of functioning normally, and other interesting performance metrics. The inconsistency of definitions for survivability causes many variations in describing and modeling behavior of information systems under attack or failure. A detailed illustration of different descriptions of survivability is shown in **Table 1-1** [8].

Table 1-1 Different Definitions of Survivability

Terminology	*Description*
Availability	The degree to which software remains operable in the presence of system failures.
Architectural	The degree to which software does not depend on specific

design hardware dependence	hardware environments; or the degree to which hardware does not depend on specific software environments.
Connectivity	The degree to which a system will perform reliably when all nodes and links are available.
Correctness	The degree to which all software functions are specified.
Dependability	The degree to which the system can provide services, even in the event of a threat.
Endurability	The degree to which a system can tolerate a threat and still provide service.
Fairness	The ability of a network system to organize and route information without failure.
Fault tolerance	The degree to which the software will continue to work without a system failure that would cause damage to users. Also, the degree to which software includes degraded operation and recovery functions.
Interoperability	The degree to which software can be connected easily with other systems and operated.
Modifiability	The degree of effort required to improve or modify the efficiency of functions of the software.
Performance	Composed of quality factors, such as Efficiency, Integrity, Reliability, Survivability, and Usability.
Predictability	The degrees of providing countermeasures to system failures in the event of a threat.
Recoverability	The ability to restore services in a timely manner.
Reliability	A set of attributes that bear on the capability of software to maintain its level of performance under stated conditions for a stated period of time.
Restorability	The ability of a system to recover from threat and provide services in a timely manner.
Reusability	The degree to which software can be reused in applications

	other than the original application.
Safety	The ability of the system not to cause harm to the network or personnel.
Security	The degree to which software can detect and prevent information leaks, information loss, illegal use, and system resource destruction.
Testability	The effort required to test software.
Verifiability	Relative efforts to verify the specified software operation and performance.

There are some similar terms related to survivability. In [1], the author compares survivability with reliability and availability. The definition of reliability is the probability that an object will work normally under specific conditions and specific time intervals. To be more specific, one can estimate a mean error rate, λ, of the object in its life time through statistical methods for forecasting the probability of normal functionality under given situations. By definition, reliability is a function of time and the error rate, which can be described as $R(t) = e^{-\lambda t}$ if Poisson distribution is assumed.

Availability, on the other hand, is defined as the time ratio an object operates under normal conditions. The definition of availability also implies possibilities of malfunctions, but it concerns the ratio $A = \frac{uptime}{uptime + downtime}$. A high availability index indicates high reliability of the object and that there are sufficient maintenance resources to quickly offer services again if the object should be out of order in the future.

After reviewing the rough definitions of survivability, one may ask: “How can survivability be measured?” In fact, measurement of survivability differs case by case. For example, survivability can be defined in terms of the degree to which software remains operable in the presence of system failures. It can also be measured as the ability to restore services in a timely manner.

Computations and calculations of survivability are also diverse. Our broad survey concludes that quantitative survivability can be divided into two categories: connectivity and performance. The connectivity issue has been intensely researched by graph theorists for a long time, and several papers that consider connectivity as a metric have been published. In [9], the node connectivity factor (NCF) is proposed to evaluate the level of robustness of a given network. The NCF quantifies the physical stability of a network in terms of the expected number of critical nodes that must be removed from a network to eliminate all communication links. By definition, the NCF of a connected graph G is defined recursively as:

$$NCF(G) = K(G) + \sum_{i=1}^{C(G)} [P(i) * NCF(G(i))],$$

where

$C(G) =$ number of minimum cut-vertex sets for G_i

$K(G) =$ number of vertices in each minimum cut-vertex set of the graph G_i

$P(i) =$ likelihood of occurrence for the i^{th} minimum cut-vertex set

$G(i) =$ i^{th} subgraph of G induced by the removal of the i^{th} minimum cut-vertex set

For a disconnected graph, G, composed of m components, G_j ,

$$NCF(G) = \sum_{j=1}^{m} NCF(G_j).$$

The introduction of NCF describes how robust and stable a given network topology is. However, the computation of NCF value is a recursive procedure, which incurs an exponential computation time with the growth of network size. Therefore, some papers, [10], for example, further try to lower the computational complexity using special data structures, such as knowledge-based look-ups. In any case, NCF is a method to describe topological properties with the consideration of how many expected number of critical nodes should be removed from the network, such that all communication links are eliminated. The concept of NCF is definitely worthy of consideration.

Another paper, [11], proposes a different survivability measure (SM) in the context of connectivity and, through simulations, shows a high correlation between the SM value and the probability that rest nodes in a network are still connected. A significant contribution made by [11] is the worst case assumption from a network operator's perspective, i.e., each time the most important node is removed. Through simulations, the authors conclude that the proposed measure is even more useful while considering malicious attack, which is regarded as an important issue in military networks. Moreover, the authors show that a balanced network topology yields the highest SM value, which suggests network planners should not create super important nodes in a network. However, we will show that it is not this case in the real world in the "scale-free networks" section.

We also note that several papers discuss survivability in the context of performance. The main idea of considering performance rather than connectivity as a survivability metric lies in the fact that connectivity metrics focus on topology information, where as performance metrics require more, such as traffic flows, average end-to-end delay, and mean delay jitters. For example, traffic flows are used in [12] and [13] as survivability metrics. Specifically, remaining traffic flow as a percentage of original traffic under destruction of nodes or links is discussed in [12]. Meanwhile, in [14], the authors emphasize that users' perceptions should be included as a kind of performance metric. If the time to gain access to a resource, for example, an http request for a webpage, is longer than an end user's endurable time period, the network is regarded as non-survivable.

1.3.2 Scale-free Networks

Network researchers have focused on random networks for a long time. However, a growing number of evidences have shown that most real network topologies are not random. The concept of a small-world model was then proposed, followed by another scale-free model, to describe topological properties of real networks.

Paul Erdos and A. Renyi proposed a random graph model, which is also well-known as an ER model, in 1950s [15]. In a random graph model, connectedness of each pair of nodes is determined by a given probability, which makes a constructed network balanced in terms of degrees of connectivity. Many previous computer network topologies were created in simulations and discussed based on an assumption of an ER model. An example of an ER model is shown in **Figure 1-1**.

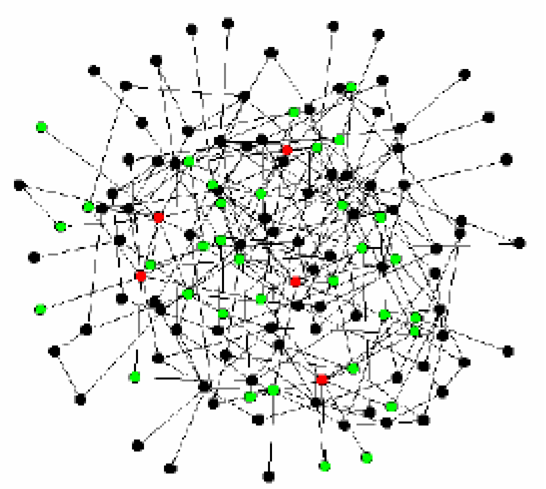

Figure 1-1 An Example of an ER Model [16]

However, evidences have shown that most of the existing networks are not randomly constructed. In 1998, Duncan Watts and Steve Strogatz discovered a new model after many observations and experiments: the small-world model [17]. The small-world model is nominated for its introduction of rewiring probability. That is, given a random graph, each link is rewired with certain probability *p*. The main contribution of the small-world model is its brand-new discovery of secrets and rules hidden behind general networks, which is believed to be applicable to many different fields. For example, biologists find it useful in describing the evolution of nerve systems of nematode; sociologists model interpersonal relationships as six degrees of separation. Experiments approve that the small-world model best fits some realistic situations.

However, characteristics of some large networks, such as the Internet and World Wide Web (WWW), still cannot be well-described by the small-world model [18]. In 1999, the Faloutsos et al. published their discovery of the Internet [3]. They found that the degree of connectivity of the Internet follows a power-law distribution, which means that the connectivity distribution *P(k)* is logarithmically proportional to $k^{-\gamma}$, with different constant *r* for different networks. In other words, there are relatively small numbers of nodes with high degrees of connectivity; whereas a majority of nodes are relatively low degrees. However, it was not until the introduction of the scale-free networks could we realize the secrets behind the Internet.

Albert-Laszlo Barabasi and Reka Albert proposed a scale-free model in year 2000 [16] [19]. There are two properties in a scale-free network: growth and preferential attachment. These kinds of networks are assumed to have a growth tendency; moreover, a new node joining such a network has preferential interest in connecting with nodes of high degree of connectivity. Due to the phenomenon of the preferential attachment, a node with higher degree of connectivity could attract more new nodes, while a lower degree one has lower probability of linking with new nodes. It is these two properties that results in a power-law distribution of nodes' degree of connectivity. **Figure 1-2** is an example of a scale-free model.

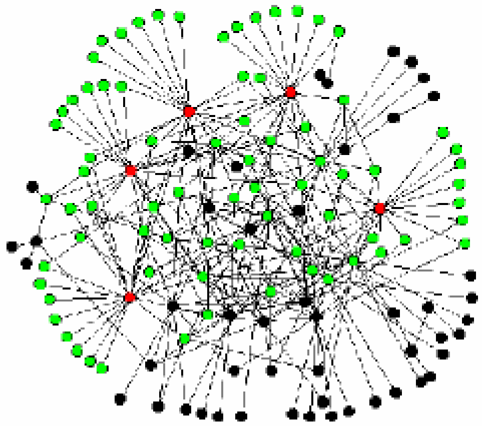

Figure 1-2 An Example of a Scale-free Network [16]

Reka Albert, Albert-Laszlo Barabasi, and Hawoong Jeong also showed important characteristics of scale-free networks [16]. Scale-free networks, such as the Internet and WWW, are capable of enduring high rate of random errors but are vulnerable to malicious attacks. Simulations by Faloutsos et al. [3] investigated the topological properties of the Internet at the router and inter-domain level, finding that the diameter of the Internet remains unaffected by the random removal of as high as 2.5% of the nodes, whereas if the same percentage of the most connected nodes are eliminated (i.e. malicious attacks), the diameter grows more than triples [16].

Since most of the large scale networks are proven to be scale-free networks, we will consider scale-free network topologies in our experiments, in addition to random networks and grid networks.

1.4 Proposed Approach

We model the attack and defense problem as optimization problems. Due to the high complexities of the problems, our proposed mathematical programming models are nonlinear and mixed integer-programming ones. As we expected, the problems are by nature highly complicated and difficult.

To the best of our knowledge, our proposed approach is the first attempt to solve an attack and defense problem considering survivability issues in general networks via mathematical programming techniques. We then apply the Lagrangean relaxation method [20] [21] and the subgradient method [22] to solve the problem.

Chapter 2 Problem Formulation

In this chapter, we propose two mathematical models with specific assumptions and problem objectives. In Model 1, we consider how attackers might attack the network under given budget allocation scenarios. In Model 2, we discuss how a defender should allocate a budget under such attack scenarios.

2.1 Model 1

2.1.1 Problem Description and Assumptions

The objective of this problem is to decide the minimal attack cost for an attacker, in order to “compromise” a network.

Here, we discuss survivability in the domain of connectivity. Network connectivity has been researched by computer network experts for many years, yielding many different metrics for measuring the connectivity of a given network. We focus on the connectivity of important node pairs. Given several critical origin-destination pairs (OD-pairs), it is important to ensure at least one functional path for each OD-pair making communications. In order to report the worst case scenario for a defender, we research the strategies of applying the minimal attack cost from the perspective of an attacker, such that there is no available path for critical OD-pairs to communicate.

In this model, we assume that both the attacker and the defender have the complete information about the targeted network topology. Moreover, the attacker has complete information about the defender’s budget allocation. However, in the real world, the defender can take advantage of information asymmetry by concealing or confusing critical information, so that the attacker has to speculate about the real situation; therefore, the attacker may waste attack resources in order to compromise the network. Consequently, we consider the worst case for the defender here.

The defender's budget allocation strategy may greatly influence the difficulty that the attacker experiences in compromising a network. Naturally, it is more difficult to attack a node if more budgetary resources are allocated to it.

Note that, for simplicity we do not take relatively infrequent link attacks into account, whereas node attacks, which result in worse case scenarios, are more common in real computer networks. Also, if a node is attacked, all of its outgoing links are no longer available. In addition, we do not consider random errors here because we want to focus on the effects of malicious attacks.

Table 2-1 Problem Assumptions of Model 1

Problem assumptions:

1. The survivability metric is measured as the connectivity of the given critical OD-pairs.

2. The attacker and the defender have complete information about the targeted network topology.

3. The defender's budget allocation strategy is a given parameter.

4. The objective of the attacker is to minimize the total attack cost of destroying all paths between given critical OD-pairs.

5. We consider node attacks only. (No link attacks are considered). If a node is attacked, its outgoing links are not functional.

6. We consider malicious attacks only. (No random errors are considered.)

Table 2-2 Problem Descriptions of Model 1

Given:

1. The network topology and the network size

2. The defender's budget allocation policy
3. A set of critical OD-pairs
4. The minimal attack cost to compromise a node is a given function of the budget allocation for it.

Objective:

To minimize the total cost of an attack

Subject to:

1. There is no available path for each given critical OD-pair to communicate.

To determine:

1. Which nodes will be attacked

To describe the constraints mathematically, we adopt the following concepts. For each OD-pair, we select exactly the shortest cost path and enforce it to be a non-available path. The "cost" of a path is defined as the sum of the link costs along that path, where the cost of a link is very large if that link is not functional and very small otherwise.

The argument is that if there is at least one disconnected link along the shortest cost path, then there is no available path for that OD-pair to communicate.

2.1.2 Notation

Given Parameters	
Notation	Description
V	The index set of all nodes
L	The index set of all links
W	The index set of all given critical origin-destination pairs
OUT^i	The index set of outgoing links of node *i,* where $i \in V$
M	A large number that represents the link disconnection
ε	A small number that represents the link connectedness
P_w	The index set of all candidate paths of an OD-pair, *w,* where $w \in W$

δ_{pl}	An indicator function, which is 1 if link *l* is on path *p,* and 0 otherwise
b b_i	Budget allocated to node *i,* where $i \in V$
$\hat{a}_i$	Threshold of an attack cost leading to a successful attack, which is a function of b_i
Decision Variables	
Notation	Description
y_i	1 if node *i* is compromised, and 0 otherwise
t_{wl}	1 if link *l* is used by OD pair, *w,* and 0 otherwise
x_p	1 if path *p* is chosen, and 0 otherwise
c_l	Cost of link *l*, which is ε if link *l* functions normally, and $M+\varepsilon$ if link *l* is broken

2.1.3 Problem Formulation

Objective function:

$$\min_{y_i} \sum_{i \in V} y_i \hat{a}_i , \qquad \text{(IP1)}$$

subject to

$$c_l = y_i M + \varepsilon \qquad \forall i \in V,\ l \in OUT^i \qquad \text{(IP 1.1)}$$

$$\sum_{l \in L} t_{wl} c_l \le \sum_{l \in L} \delta_{pl} c_l \qquad \forall p \in P_w,\ w \in W \qquad \text{(IP 1.2)}$$

$$\sum_{p \in P_w} x_p \delta_{pl} = t_{wl} \qquad \forall w \in W,\ l \in L \qquad \text{(IP 1.3)}$$

$$M \le \sum_{l \in L} t_{wl} c_l \qquad \forall w \in W \qquad \text{(IP 1.4)}$$

$$\sum_{p \in P_w} x_p = 1 \qquad \forall w \in W \qquad \text{(IP 1.5)}$$

$$x_p = 0 \text{ or } 1 \qquad \forall p \in P_w,\ w \in W \qquad \text{(IP 1.6)}$$

$$y_i = 0 \text{ or } 1 \qquad \forall i \in V \qquad \text{(IP 1.7)}$$

$$t_{wl} = 0 \text{ or } 1 \qquad \forall w \in W,\ l \in L. \qquad \text{(IP 1.8)}$$

Explanation of the mathematical formulation:

Objective function: To minimize the total attack cost; the attacker minimizes the objective value by deciding which nodes to compromise (i.e., y_i for each node *i*).

Constraint (IP 1.1) describes the definition of the link cost, which is ε if the link functions normally, and $M+\varepsilon$ if the link is broken.

Constraint (IP 1.2) requires that the selected path for each OD-pair, *w,* should be a shortest cost path.

Constraint (IP 1.3) is the relations among t_{wl}, x_p and δ_{pl}. We use the auxiliary set of decision variables, t_{wl}, to replace the sum of all $x_p\delta_{pl}$. The substitution is to further simplify the problem solving procedures.

Constraint (IP 1.4) requires that the given critical OD-pairs are all disconnected. We depict the phenomenon by showing that the cost of the shortest path for each OD-pair to communicate is greater than *M*.

Constraint (IP 1.5) and (IP 1.6) jointly require that exactly one path is selected between each given OD-pair.

Constraint (IP 1.7) determines whether each node *i* is compromised, or not.

Constraint (IP 1.8) determines whether each link *l* is used to form a shortest cost path by OD-pair, *w,* or not.

2.1.4 Problem Reformulation

In order to mathematically solve the optimization problem, we reformulate the problem with one assumption and some adjustments without affecting the problem structure and the optimality conditions.

Assumption: In order to simplify the problem, we assume that $\hat{a}_i = b_i, \forall i \in V$, which means that the minimal attack cost of compromising a node equals the allocated budget for it.

We adjust some constraints, add two sets of redundant constraints, and explain them later.

Objective function:

$$\min_{y_i} \sum_{i \in V} y_i b_i , \qquad \text{(IP2)}$$

subject to

$$c_l \le y_i M + \varepsilon \qquad \forall i \in V,\ l \in OUT^i \qquad \text{(IP 2.1)}$$

$$\sum_{l \in L} t_{wl} c_l \le \sum_{l \in L} \delta_{pl} c_l \qquad \forall p \in P_w,\ w \in W \qquad \text{(IP 2.2)}$$

$$\sum_{p \in P_w} x_p \delta_{pl} \le t_{wl} \qquad \forall w \in W,\ l \in L \qquad \text{(IP 2.3)}$$

$$M \le \sum_{l \in L} t_{wl} c_l \qquad \forall w \in W \qquad \text{(IP 2.4)}$$

$$\sum_{p \in P_w} x_p = 1 \qquad \forall w \in W \qquad \text{(IP 2.5)}$$

$$x_p = 0 \text{ or } 1 \qquad \forall p \in P_w,\ w \in W \qquad \text{(IP 2.6)}$$

$$y_i = 0 \text{ or } 1 \qquad \forall i \in V \qquad \text{(IP 2.7)}$$

$$t_{wl} = 0 \text{ or } 1 \qquad \forall w \in W,\ l \in L \qquad \text{(IP 2.8)}$$

$$c_l = \varepsilon \text{ or } M + \varepsilon \qquad \forall l \in L \qquad \text{(IP 2.9)}$$

$$\sum_{i \in V} y_i \ge V_{lb.} \qquad \text{(IP 2.10)}$$

Explanation of the reformulation:

1. The objective function is modified to simplify the original problem.
2. Constraint (IP 2.1) is a relaxed version of (IP 1.1). Note that the relaxation of the equation into an inequality version does not violate its optimality conditions.
3. Constraint (IP 2.3) is a relaxed version of (IP 1.3). Note that the relaxation of the equation into an inequality version does not violate its optimality conditions.
4. Constraint (IP 2.9) is a set of redundant constraints, since the value of each c_l should be either ε or $M+\varepsilon$. We will need it in the Lagrangean relaxation problem.
5. Constraint (IP 2.10) is also a redundant constraint. We find a legitimate lower bound, V_{lb}, on the number of nodes an attacker should attack in order to compromise the connectivity of given critical OD-pairs. The legitimate lower bound can be obtained from either of the following methods.

Table 2-3 Methods for Getting a Legitimate Lower Bound of Nodes to Attack

Method 1: We deliberately assign one unit budget to each node. Then we solve this revised optimization problem and find an LR lower bound, denoted by LB, on the optimal objective function value. Then LB indicates a minimal (but may not be feasible) attack cost an attacker has to spend in order to reach his goal. Since each node is assigned with one unit budget, LB also serves as a lower bound of number of nodes an attacker needs to take away.
Method 2: We first find an LR lower bound on the primal objective function value of the primal problem. Denote this value by LB. We then find the min set of $\{b_i\}$, in terms of cardinality, in such a way that the sum of the elements in this set is no less than LB. Then the cardinality of this set serves as a legitimate lower bound on the number of

nodes an attacker needs to take away.

In our thesis, we adopt Method 1 to get a legitimate lower bound of V_{lb}.

We can further derive an upper bound on number of nodes an attacker may attack. We first apply any heuristic to calculate a primal feasible solution, of which the corresponding objective function value is denoted by UB. We then find the max set of $\{b_i\}$, in terms of cardinality, in such a way that the sum of the elements in this set is no greater than UB. If such a sum is less than UB, then increment the cardinality by 1. The cardinality of this set serves as a legitimate upper bound on the number of nodes an attacker needs to take away.

2.2 Model 2

2.2.1 Problem Description and Assumptions

In Model 1, we assume the defender's budget allocation is a given parameter. In Model 2, we introduce another factor by allowing the defender to decide the budget allocation strategy. In other words, the defender would like to distribute a given amount of budget efficiently so that the attacker has to pay a higher price to reach his goal, i.e., disconnection of given critical OD-pairs. Meanwhile, the attacker also wants to choose critical nodes to attack in order to minimize the total attack cost. Therefore, the problem becomes a max-min structure. We will present a well-formulated problem structure in the following section, and present a lemma in the next chapter.

We first introduce an argument to clarify the relationship between each b_i (the budget allocated to a node, i) and the total budget, B.

Argument: We claim that the optimality for the defender holds if and only if the total budget, B, is fully used. Note that this argument holds only when the set of decision variables, b_i, is continuous.

Table 2-4 Problem Assumptions of Model 2

Problem assumptions:

1. The survivability metric is measured as the connectivity of the given critical OD-pairs.
2. The attacker and the defender have complete information about the targeted network topology.
3. The objective of the attacker is to minimize the total attack cost of destroying all paths between given critical OD-pairs.
4. The objective of the defender is to distribute the total amount of budget effectively so that the minimal total attack cost can be maximized.
5. We consider node attacks only. (No link attacks are considered). If a node is attacked, its outgoing links are not functional.
6. We consider malicious attacks only. (No random errors are considered.)

Table 2-5 Problem Descriptions of Model 2

Given:

1. The network topology and the network size
2. A set of critical OD-pairs
3. The total budget of the defender

Objective:

To maximize the attacker’s minimal total attack cost

Subject to:

1. The total budget constraint of the defender
2. No path is available for each given critical OD-pair to communicate.

To determine:

1. The budget allocated to each node
2. Which nodes the attacker has decided to target

2.2.2 Notation

Given Parameters	
Notation	Description
B	Total budget of the defender
V	The index set of all nodes
L	The index set of all links
W	The index set of all given critical origin-destination pairs
OUT^i	The index set of outgoing links of node *i,* where $i \in V$
M	A big number that represents the link disconnection
ε	A small number that represents the link connectedness
P_w	The index set of all candidate paths of OD-pair, *w,* where $w \in W$
δ_{pl}	An indicator function, which is 1 if link *l* is on path *p,* and 0 otherwise
Decision Variables	
Notation	Description
b_i	The budget allocated to node *i*
y_i	1 if node *i* is compromised, and 0 otherwise
t_{wl}	1 if link *l* is used by OD pair, *w,* and 0 otherwise
x_p	1 if path *p* is chosen, and 0 otherwise
c_l	Cost of link *l*, which is ε if link *l* functions normally, and $M+\varepsilon$ if link *l* is broken

2.2.3 Problem Formulation

$$\max_{b_i} \min_{y_i} \sum_{i\in V} y_i b_i \quad , \qquad \text{(IP3)}$$

subject to

$$c_l \le y_i M + \varepsilon \qquad \forall i \in V,\ l \in OUT^i \qquad \text{(IP 3.1)}$$

$$\sum_{l\in L} t_{wl} c_l \le \sum_{l\in L} \delta_{pl} c_l \qquad \forall p \in P_w,\ w \in W \qquad \text{(IP 3.2)}$$

$$\sum_{p \in P_w} x_p \delta_{pl} \le t_{wl} \qquad \forall w \in W,\ l \in L \qquad \text{(IP 3.3)}$$

$$M \le \sum_{l \in L} t_{wl} c_l \qquad \forall w \in W \qquad \text{(IP 3.4)}$$

$$\sum_{p \in P_w} x_p = 1 \qquad \forall w \in W \qquad \text{(IP 3.5)}$$

$$x_p = 0 \text{ or } 1 \qquad \forall p \in P_w,\ w \in W \qquad \text{(IP 3.6)}$$

$$y_i = 0 \text{ or } 1 \qquad \forall i \in V \qquad \text{(IP 3.7)}$$

$$t_{wl} = 0 \text{ or } 1 \qquad \forall w \in W,\ l \in L \qquad \text{(IP 3.8)}$$

$$c_l = \varepsilon \text{ or } M + \varepsilon \qquad \forall l \in L \qquad \text{(IP 3.9)}$$

$$\sum_{i \in V} b_i = B \qquad \text{(IP 3.10)}$$

$$0 \le b_i \le B \qquad \forall i \in V. \qquad \text{(IP 3.11)}$$

Objective function:

To maximize the attacker's minimal total attack cost. The attacker minimizes $\sum_{i \in V} y_i b_i$ by deciding which nodes to compromise (i.e., y_i for each node i), while the defender maximizes $\sum_{i \in V} y_i b_i$ by properly deciding each b_i.

Explanation of the formulation:

1. Constraints (IP 3.1) ~ (IP 3.9) are the same as the reformulation of Model 1.
2. Constraint (IP 3.10) reflects our argument that the optimality condition for the defender holds if and only if the total budget, B, is fully used.
3. Constraint (IP 3.11) indicates that the set of decision variables, b_i, is continuous, and bounded by 0 and B.

Chapter 3 Solution Approach

In this chapter, we first introduce the proposed solution approach, Lagrangean relaxation, for Model 1, and show how we solve the problem in Model 1 with this method. We also show an elegant lemma for solving the problem in Model 2.

3.1 Solution to Model 1

3.1.1 Introduction to the Lagrangean Relaxation Method

Lagrangean relaxation method was originally used for scheduling and solving general integer programming problems in the 1970s [20], due to its effectiveness and efficiency in providing proper solutions to these problems. In recent years, however, it has gradually become one of the most popular tools for solving optimization problems, such as integer programming, linear programming combinatorial optimization, and non-linear programming problems.

There are several advantages to using the Lagrangean relaxation method. For example, we can use it to decompose mathematical models into several subproblems, which can then be separately, optimally, and easily solved by well-known algorithms. By doing so, the complexity of an original problem can be significantly reduced [20] [21].

In addition, Lagrangean relaxation can help us obtain the bounds of an objective function, and we can use the bounds to evaluate how good the implemented primal feasible solutions are. This is due to the definition of Lagrangean relaxation, in which we “pull apart” models by removing constraints and placing them in the objective function with associated Lagrangean multipliers. The new problem with fewer constraints is called the Lagrangean relaxation problem, where the optimal value is by nature a lower bound (for minimization problems) of the objective function value in the original problem. In order to get the best solution to the original problem, we try to enhance the Lagrangean lower bounds by tuning Lagrangean multipliers, which is also known as maximization of Lagrangean relaxation problems.

On the other hand, we iteratively lower the primal objective function value (for minimization problems) from the hints of solving the Lagrangean relaxation problem. Note that the optimal solution to the primal problem is guaranteed to be within the Lagrangean lower bounds and the primal feasible solution values.

We can solve the Lagrangean relaxation problem in a variety of ways; however, the most popular way is the subgradient optimization technique [20] [21]. **Figure 3-1** illustrates the main concepts of the Lagrangean relaxation method. A detailed flow chart of the Lagrangean relaxation method is presented in **Figure 3-2**.

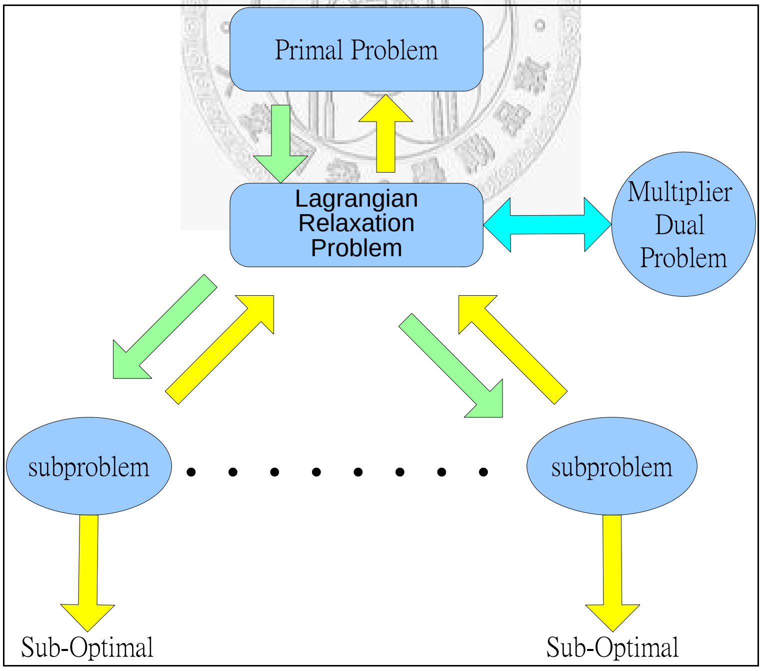

Figure 3-1 Illustration of Lagrangean Relaxation Method

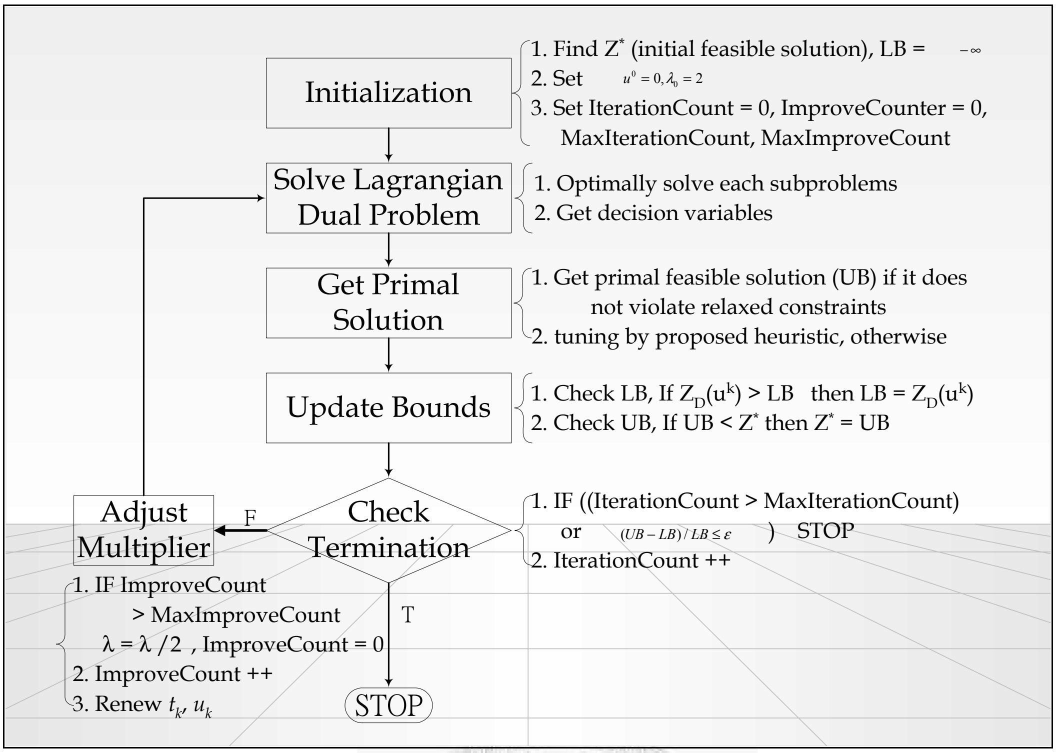
Initialization
1. Find Z* (initial feasible solution), LB = −∞
2. Set u⁰ = 0, λ₀ = 2
3. Set IterationCount = 0, ImproveCounter = 0,
MaxIterationCount, MaxImproveCount
Solve Lagrangian Dual Problem
1. Optimally solve each subproblems
2. Get decision variables
Get Primal Solution
1. Get primal feasible 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 ≤ ε) STOP
2. IterationCount ++
F
Adjust Multiplier
1. IF ImproveCount > MaxImproveCount
λ = λ /2 , ImproveCount = 0
2. ImproveCount ++
3. Renew t_k, u_k
T
STOP

Figure 3-2 Lagrangean Relaxation Procedures

3.1.2 Lagrangean Relaxation

By applying the Lagrangean relaxation method, we can transform the primal problem (IP2) into the following Lagrangean relaxation problem (LR), where constraints (IP 2.1), (IP 2.2), (IP 2.3), and (IP 2.4) are relaxed. With a vector of Lagrangean multipliers, the Lagrangean relaxation problem of IP2 is transformed as follows.

Optimization problem:

$$Z_D(u_1,u_2,u_3,u_4)=\min_{y_i}\sum_{i\in V} y_i b_i+\sum_{i\in V}\sum_{l\in OUT^i} u^1{}_{il}[c_l-(y_i M+\varepsilon)]+$$

$$+\sum_{w\in W}\sum_{p\in P_w} u^2{}_{wp}\sum_{l\in L}[t_{wl}c_l-\delta_{pl}c_l]+\sum_{w\in W}\sum_{l\in L} u^3{}_{wl}[(\sum_{p\in P_w} x_p\delta_{pl})-t_{wl}]+\sum_{w\in W} u^4{}_w\left[M-\sum_{l\in L} t_{wl}c_l\right]$$

(LR)

subject to

$$\sum_{p\in P_w} x_p = 1 \qquad \forall w\in W \qquad \text{(LR1)}$$

$$x_p = 0 \text{ or } 1 \qquad \forall p\in P_w,\ w\in W \qquad \text{(LR2)}$$

$$y_i = 0 \text{ or } 1 \qquad \forall i\in V \qquad \text{(LR3)}$$

$$t_{wl} = 0 \text{ or } 1 \qquad \forall w\in W,\ l\in L \qquad \text{(LR4)}$$

$$c_l = \varepsilon \text{ or } M+\varepsilon \qquad \forall l\in L \qquad \text{(LR5)}$$

$$\sum_{i\in V} y_i \geq V_{lb.} \qquad \text{(LR6)}$$

By definition, u_1,u_2,u_3,u_4 are the vectors of $\{u^1{}_{il}\}$, $\{u^2{}_{wp}\}$, $\{u^3{}_{wl}\}$, $\{u^4{}_w\}$,

respectively. Note that u_1,u_2,u_3,u_4 are Lagrangean multipliers and $u_1,u_2,u_3,u_4 \geq 0$. To optimally solve (LR), we decompose it into the following three independent and easily solvable optimization Subproblems.

3.1.2.1 Subproblem 1

SUB_1 (related to decision variable x_p)

$$Z_{sub1}(u_3)=\min\sum_{w\in W}\sum_{l\in L}\sum_{p\in P_w} u^3{}_{wl}\delta_{pl}x_p\ , \qquad \text{(Sub 1)}$$

subject to

$$\sum_{p\in P_w} x_p = 1 \qquad \forall w\in W \qquad \text{(Sub1.1)}$$

$$x_p = 0 \text{ or } 1 \qquad \forall p\in P_w,\ w\in W. \qquad \text{(Sub1.2)}$$

This problem can further be decomposed into $|W|$ independent shortest cost path Subproblems. In other words, we can determine the value of x_p individually for each OD-pair. Specifically, $u^3{}_{wl}$ can be treated as the cost of link *l* in OD-pair *w* in the shortest cost path Subproblems. Due to the phenomenon of the non-negativity constraint of each $u^3{}_{wl}$, we can therefore apply Dijkstra's shortest path algorithm to optimally solve these shortest cost path Subproblems. Since the time complexity of Dijkstra's shortest path algorithm is $O(|V|^2)$*)*, where $|V|$ is the number of nodes, the time complexity of SUB_1 is $O(|W|\times|V|^2)$.

3.1.2.2 Subproblem 2

SUB_2 (related to decision variable y_i)

$$Z_{sub2}(u_1) = \min \sum_{i\in V} y_i b_i + \sum_{i\in V}\sum_{l\in OUT^i} u^1{}_{il}(-M)y_i, \qquad \text{(Sub 2)}$$

subject to

$$y_i = 0 \text{ or } 1 \qquad \forall i\in V \qquad \text{(Sub 2.1)}$$

$$\sum_{i\in V} y_i \geq V_{lb.} \qquad \text{(Sub 2.2)}$$

To optimally solve SUB_2, we first apply a quick sort on the sum of the parameters of each y_i, i.e., $b_i - M\sum_{l\in OUT^i} u^1{}_{il}$, to get an array in ascending order. To satisfy the constraint (Sub 2.2), we then choose V_{lb} nodes from the left of the array, and set their values of y_i to one. The values of y_i of the remaining nodes are decided by their associated parameters, $b_i - M\sum_{l\in OUT^i} u^1{}_{il}$. For each remaining node $i\in V$, if $b_i - M\sum_{l\in OUT^i} u^1{}_{il}$ is positive, the value of y_i is set to zero, in order to minimize this

Subproblem. On the other hand, if the sum of the parameters is non-positive, it is set to one.

The time complexity of SUB_2 is $O(|V|\log|V|)$.

3.1.2.3 Subproblem 3

SUB_3 (related to decision variables t_{wl}, c_l)

$$Z_{sub3}(u_1,u_2,u_3,u_4) = \min \sum_{i\in V}\sum_{l\in OUT^i} u^1{}_{il}c_l + \sum_{w\in W}\sum_{p\in P_w} u^2{}_{wp}\sum_{l\in L}(t_{wl}c_l - \delta_{pl}c_l) + \sum_{w\in W}\sum_{l\in L} u^3{}_{wl}(-t_{wl}) + \sum_{w\in W} u^4{}_w(-\sum_{l\in L} t_{wl}c_l) \qquad \text{(Sub 3)}$$

subject to

$t_{wl} = 0$ or 1 $\qquad \forall w\in W,\ l\in L$ $\qquad$ (Sub 3.1)

$c_l = \varepsilon$ or $M+\varepsilon$ $\qquad \forall l\in L.$ $\qquad$ (Sub 3.2)

As constraints (Sub 3.1) and (Sub 3.2) show, either t_{wl} or c_l has two choices. We can therefore apply an exhaustive search to determine the values of t_{wl} and c_l, depending on which combination results in the smallest objective function value. To optimally solve SUB_3, we further decompose it into |*L*| independent Subproblems, which are shown below.

$$Z_{sub3'}(u_1,u_2,u_3,u_4) = \min\left\{ \left[u^1{}_{il} - \sum_{w\in W}\sum_{p\in P_w} u^2{}_{wp}\delta_{pl}\right] + \sum_{w\in W}\left[(\sum_{p\in P_w} u^2{}_{wp}) - u^4{}_w\right] t_{wl} \right\} c_l - \sum_{w\in W} u^3{}_{wl}t_{wl}\ , \qquad \text{(Sub 3')}$$

subject to

$t_{wl} = 0$ or 1 $\qquad \forall w\in W$ $\qquad$ (Sub 3.1’)

$c_l = \varepsilon$ or $M+\varepsilon.$ $\qquad$ (Sub 3.2’)

The time complexity of SUB_3 is $O(|W|\times|L|)$.

3.1.3 The Dual Problem and the Subgradient Method

According to the weak Lagrangean duality theorem [21], for any set of the multipliers $(u_1, u_2, u_3, u_4) \geq 0$, $Z_D(u_1, u_2, u_3, u_4)$ is a lower bound on Z_{IP2}. The following dual problem is then constructed to calculate the tightest lower bound.

Dual Problem (D)

Z_D =**max** Z_D(u_1, u_2, u_3, u_4)

s.t. (u_1, u_2, u_3, u_4) ≥ 0

There are several methods for solving the dual problem (D), of which the subgradient method [22] is the most popular one. We therefore adopt it as our solution approach to the dual problem. Let a vector *k* be a subgradient of Z_D(u_1, u_2, u_3, u_4). Then, in iteration *p* of the subgradient procedure, the multiplier vector λ= (u_1, u_2, u_3, u_4) is updated by

$$\lambda^{p+1} = \lambda^p + t^p k^p,$$

where the step size, t^p, is determined by

$$t^p = \delta \frac{Z_{IP2}^{h} - Z_D(\lambda_p)}{\| k^p \|^2}.$$

Z_{IP2}^{h} is the best upper bound on the primal objective function value after the pth iteration. δ is a value between 0 and 2. It is initiated with a value of 2 and halved whenever the best objective function value does not improve within a given iteration count.

3.1.4 Getting Primal Feasible Solutions

To obtain the primal feasible solutions to the original problem (IP2), we consider the solutions from the LR problem. By using the Lagrangean relaxation and the subgradient method to solve the LR problem, we not only get a theoretical lower bound on the primal objective function value, but also obtain good hints for getting primal feasible solutions. However, as some critical and difficult constraints are relaxed to obtain the easily-solvable LR problem, the solutions obtained from Z_D may not be valid to the primal problem. We therefore need to develop good heuristics to tune the values of these decision variables, so that primal feasible solutions can be obtained.

Our basic concept is as follows. From the solutions to Subproblem 2 of LR, we can determine whether or not each y_i should be set to one by examining its associated parameters. The more negativity associated with the parameter, the more likely it is that the y_i of that node should be set to one. We therefore apply a quick sort method to sort the parameters of y_i in ascending order.

In addition, the solutions to Subproblem 3 of LR provide us with other useful information. For each node, if any of its outgoing link costs in the dual solution is set to $M + \varepsilon$, the more likely it is that the node will be attacked. Recall the definition of the link cost in the problem formulation.

If all nodes with the above characteristics have been considered, but there still exists some path for at least one OD-pair to communicate, we have to consider extra nodes by first choosing the smaller positive parameters of y_i. We stop when there does not exist any available path for each OD-pair to communicate.

By combining the above ideas, we are able to derive a heuristic for getting primal feasible solutions. However, we find that the solution quality is not as good as we expect. After examining the results carefully, we conclude that some of the nodes are “mis-attacked”, meaning that the attacker does not necessarily need to attack the nodes in order to reach his goal. To improve the solution quality, we apply a greedy algorithm to lower the primal objective function value as much as possible. The algorithm is given below.

Table 3-1 Getting Primal Feasible Algorithm

```
1   Sort the nodes in ascending order w.r.t. the parameters of $y_i$ we mentioned
2   in Subproblem2.
3   While (there is an available path for at least one OD-pair to communicate,
4   and some nodes remain unexamined){
5       One at a time, attack the leftmost unexamined node with a negative
6   parameter of $y_i$ or a large M of its outgoing link cost.
7   }
8   While (there is an available path for at least one OD-pair to
9   communicate){
10      One at a time, attack the left-most node which was not determined to
11  be attacked yet.
12  }
13  While (some nodes remain unexamined){
14      Apply a greedy algorithm; we sequentially recover the attacked node
15  with the largest budget, $b_i$, and test if this recovery will lead to any
16  available path for any OD-pair. If yes, we do not recover this node.
17  }
18  While (some nodes remain unexamined){
19      Apply a greedy algorithm; we sequentially examine if a recovery of
20  any two combinations of the attacked nodes will lead to any available
21  path for any OD-pair. If yes, we do not recover the nodes.
22  }
```

Step 1: In Line 1 and 2, we sort the nodes in an ascending order according to their associated parameters in Subproblem2.

Step 2: In Line 3 to 7, we sequentially set the y_i of the leftmost unexamined node in the sorted array to one, if the sum of its associated parameters in SUB_2 is negative or any of the node's outgoing link cost in SUB_3 is greater than *M*. We exit the *while* loop if and only if a primal feasible solution is obtained or all nodes are examined.

Step 3: In Line 8 to 12, if a primal feasible solution is not obtained yet, we sequentially set the leftmost unexamined node of which $y_i = 0$ to one. That is, we ensure a primal feasible solution after Step 3.

Step 4: In Line 13 to 17, we apply a greedy heuristic to "recover" the attacked nodes. That is, we one at a time recover the attacked node with the largest budget, b_i, and test if this recovery will lead to any available path for any OD-pair. If we find a recovery can lead some available path for some OD-pair, this recovery is not allowed because it violates the constraints of the primal problem; if a recovery is allowable, we save a cost of b_i.

Step 5: In Line 18 to 22, to further enhance the saving, we try the combinations of "picking 2 out of *N*." That is, for each un-attacked node, we try all "picking 2 out of *N*" combinations of other attacked nodes and test if the two nodes can be taken over by the one node with a saving.

The time complexity of the getting primal heuristic is $O(|W| \times |V|^5)$.

3.2 Solution to Model 2

3.2.1 Basic Concept

Despite the complicated max-min mathematical form, we find that an optimal solution can always be easily obtained. The basic concept is as follows.

We remind the readers that the goal of an attacker is to disconnect all paths of given critical OD-pairs. Since a smart attacker may always find the best approach to attain his goal, if a defender unevenly distributes the total amount of budget, some budgetary resources are “wasted.” To fully utilize a total budget, we come up with an idea of protecting one critical path, and allocate all budgetary resources to it. In addition, a “balanced” budget allocation strategy should be considered so that an attacker cannot play tricks. Moreover, if there are fewer nodes on a critical path, the more budget a node on the path is allocated, since the total amount of budget is fixed.

From the above statements, we propose a budget allocation policy: given a total budget, a topology, and a set of critical OD-pairs, we find the minimal hop path among the set of OD-pairs, in terms of number of nodes on the path, and evenly distribute the total budget to each of the node on the minimal hop path. If there are ties on the minimal hop path, arbitrarily choose one.

3.2.2 Lemma

We further write the above statements as a lemma.

Lemma:

Given a total budget, *B*, a topology, *G*= (*V*, *E*), and a set of critical OD-pairs, *W*. The best budget allocation strategy to maximize the minimal attack cost is to evenly distribute *B* to the nodes on a minimal hop path in *G* among all *W*. The corresponding minimal attack cost is $\frac{B}{H_m}$, where H_m is the number of nodes on the minimal hop path.

Assume that there is another budget allocation strategy such that the minimal cost of an attack is *A*, which is greater than $\frac{B}{H_m}$. In such a case, both the source and the destination node of the minimal hop path should be allocated a budget of at least *A*. If not, we simply attack either the source or the destination node and we are done with minimal attack cost less than $\frac{B}{H_m}$. Moreover, in order not to grant an attacker any trick, we have to allocate a budget of at least A to the remaining H_m-2 nodes along the minimal hop path. Therefore, in such a case, the total budget used will be H_m*A, which is more than B. It leads to a contradiction since the total budget constraint, $\sum_{i \in V} b_i = B$, is violated.

Chapter 4 Computational Experiments

In order to show that the solution quality of our primal heuristic is better than other approaches, we implement the following two simple algorithms for comparison purposes.

4.1 Simple Algorithm 1

Since the core of our problem objective is to find a minimal total attack cost such that all given critical OD-pairs cannot communicate, we want to find a set of critical nodes and attack them. The concept is similar to finding a set of cuts to disconnect the communications. Thus to minimize the total attack cost, we should find a "minimum cut". According to the maximum flow-minimum cut theorem, we obtain the minimum cut by executing the maximum flow algorithm. Hence, we adopt the maximum flow algorithm for each OD-pair to obtain the minimum cuts. By taking the union of the minimum cuts, we are guaranteed to obtain a feasible solution to the primal problem. In order to improve the solution quality, we apply the same concept to this simple algorithm, as we did in "getting primal feasible solutions." We now present the core algorithm.

Table 4-1 Simple Algorithm 1

```
For (each OD-pair){
   Run Maximum Flow algorithm to get the minimum cuts.
}
Take the union of all the minimum cuts, and let all the nodes, with at least one outgoing link labeled as M, be the candidates.
```

```
Sequentially recover one of the candidates, and run Dijkstra's Shortest Path algorithm to investigate if the recovery is allowable.
```

4.2 Simple Algorithm 2

In the literature, a survivability measure (SM) [11] is proposed to evaluate how a network sustain malicious attacks, under the assumption that the most important node is removed each time. We have shown that the importance of nodes can be evaluated by their level of connectivity. We now propose a simple algorithm that considers the removal of the most connected node sequentially. We stop the algorithm when there is not any available path for each OD-pair to communicate. The pseudo code is as follows.

Table 4-2 Simple Algorithm 2

```
Sort the nodes in descending order w.r.t. the degree of connectivity.
While (there is an available path for at least one OD-pair to communicate){
    Attack the most connected node among those not being attacked yet.
}
```

4.3 Parameters and Cases of the Experiment

We organize our experimental parameters and design of cases as the following table.

Table 4-3 Experimental Parameters

Number of Nodes	16 ~ 100
Number of Links	60 ~ 400
Number of critical OD-pairs	8 ~ 250
Testing Topology	Random networks, Grid networks, and Scale-free networks
Number of Iterations	2000

Non-improvement Counter	80
Initial Upper Bound	Solution of SA_1
Initial budget allocation policy	Uniform distribution, Degree-based distribution
Test Platform	CPU: Intel Pentium-4 2.0 GHz OS: MS Windows XP

4.4 Experimental Results

We present the experimental results by a list of tables. The SA_1 and SA_2 are the solutions from Simple Algorithm 1 and 2; the LR value means the primal feasible solution from the LR process; the LB represents the lower bound gained from the LR process. Moreover, the Gap is calculated by $\frac{\text{LR-LB}}{\text{LB}}*100\%$; the improvement ratio of SA_1 and SA_2 are calculated by $\frac{\text{SA}_1\text{-LR}}{\text{LR}}*100\%$ and $\frac{\text{SA}_2\text{-LR}}{\text{LR}}*100\%$, respectively.

Case 1: Small-scale networks with uniform budget distribution

(Number of nodes is 16.)

Network Topology	No. of Critical OD-pairs	SA_1	SA_2	LR	LB	Gap	Imp. Ratio of SA_1	Imp. Ratio of SA_2
Grid Networks	8	4	16	4	3.563926	12.24%	0.00%	300.00%
	16	7	16	7	6.370007	9.89%	0.00%	128.57%
	24	7	16	7	6.73727	3.90%	0.00%	128.57%
	32	10	16	10	8.539403	17.10%	0.00%	60.00%
	40	12	16	12	9.945028	20.66%	0.00%	33.33%
Random Networks	8	8	11	6	4.812023	24.69%	33.33%	83.33%
	16	8	13	8	6.232452	28.36%	0.00%	62.50%

	24	7	8	7	5.470252	27.96%	0.00%	14.29%
	32	9	15	9	7.660677	17.48%	0.00%	66.67%
	40	10	11	10	8.83108	13.24%	0.00%	10.00%
Scale-free Networks	8	3	8	3	2.948217	1.76%	0.00%	166.67%
	16	5	7	5	4.847389	3.15%	0.00%	40.00%
	24	6	9	6	4.862614	23.39%	0.00%	50.00%
	32	10	15	10	8.995957	11.16%	0.00%	50.00%
	40	9	11	9	8.610195	4.53%	0.00%	22.22%

Case 2: Medium-scale networks with uniform budget distribution

(Number of nodes is 50.)

Network Topology	No. of Critical OD-pairs	SA_1	SA_2	LR	LB	Gap	Imp. Ratio of SA_1	Imp. Ratio of SA_2
Grid Networks	25	12	36	10	7.441391	34.38%	20.00%	260.00%
	50	19	40	18	14.06399	27.99%	5.56%	122.22%
	75	20	45	19	14.5307	30.76%	5.26%	136.84%
	100	19	42	17	12.30638	38.14%	11.76%	147.06%
	125	20	46	20	15.29588	30.75%	0.00%	130.00%
Random Networks	25	15	23	13	9.824965	32.32%	15.38%	76.92%
	50	17	31	16	12.16454	31.53%	6.25%	93.75%
	75	19	40	18	13.22959	36.06%	5.56%	122.22%
	100	24	46	18	14.50284	24.11%	33.33%	155.56%
	125	21	46	19	15.21835	24.85%	10.53%	142.11%
Scale-free Networks	25	6	6	6	4.724655	26.99%	0.00%	0.00%
	50	9	15	9	7.636606	17.85%	0.00%	66.67%
	75	25	35	13	10.93413	18.89%	92.31%	169.23%
	100	14	44	14	11.63209	20.36%	0.00%	214.29%
	125	18	49	18	15.51449	16.02%	0.00%	172.22%

Case 3: Large-scale networks with uniform budget distribution

(Number of nodes is 100.)

Network Topology	No. of Critical OD-pairs	SA_1	SA_2	LR	LB	Gap	Imp. Ratio of SA_1	Imp. Ratio of SA_2
Grid Networks	50	27	92	23	16.44631	39.85%	17.39%	300.00%
	100	34	94	26	17.54971	48.15%	30.77%	261.54%
	150	30	95	28	20.09422	39.34%	7.14%	239.29%
	200	38	98	31	22.50487	37.75%	22.58%	216.13%
	250	36	92	36	20.63084	74.50%	0.00%	155.56%
Random Networks	50	33	57	25	16.93092	47.66%	32.00%	128.00%
	100	37	99	30	21.54363	39.25%	23.33%	230.00%
	150	41	62	34	26.22784	29.63%	20.59%	82.35%
	200	38	80	34	24.61151	38.15%	11.76%	135.29%
	250	47	87	40	31.66511	26.32%	17.50%	117.50%
Scale-free Networks	50	18	29	18	14.31243	25.76%	0.00%	61.11%
	100	21	53	21	16.7806	25.14%	0.00%	152.38%
	150	26	40	23	18.22227	26.22%	13.04%	73.91%
	200	26	96	25	20.57828	21.49%	4.00%	284.00%
	250	27	53	25	20.96103	19.27%	8.00%	112.00%

Case 4: Small-scale networks with degree-based budget distribution

(Number of nodes is 16.)

Network Topology	No. of Critical OD-pairs	SA_1	SA_2	LR	LB	Gap	Imp. Ratio of SA_1	Imp. Ratio of SA_2
Grid Networks	8	4.33	16	4.33	4.13249	4.86%	0.00%	269.23%
	16	7.33	16	7.33	6.63511	10.52%	0.00%	118.18%
	24	7.33	16	7.33	6.853707	7.00%	0.00%	118.18%

	32	10.33	16	10.33	9.182209	12.54%	0.00%	54.84%
	40	12.33	16	12.33	10.24175	20.42%	0.00%	29.73%
Random Networks	8	8.5	13.25	6	4.905528	22.31%	41.67%	120.83%
	16	8.75	14.5	8.75	7.140306	22.54%	0.00%	65.71%
	24	10.5	15	10.5	8.701734	20.67%	0.00%	42.86%
	32	11.5	15.5	10.25	8.964373	14.34%	12.20%	51.22%
	40	11.31	15.45	10.75	9.872351	8.89%	5.21%	43.70%
Scale-free Networks	8	5.517241	11.58621	5.517241	4.984125	10.70%	0.00%	110.00%
	16	8.827586	10.75862	7.448276	6.341982	17.44%	18.52%	44.44%
	24	7.724138	12.13793	7.724138	6.552931	17.87%	0.00%	57.14%
	32	10.75862	15.44828	10.48276	8.082209	29.70%	2.63%	47.37%
	40	10.75862	13.24138	10.75862	8.964434	20.01%	0.00%	23.08%

Case 5: Medium-scale networks with degree-based budget distribution

(Number of nodes is 50.)

Network Topology	No. of Critical OD-pairs	SA_1	SA_2	LR	LB	Gap	Imp. Ratio of SA_1	Imp. Ratio of SA_2
Grid Networks	25	12.35294	38.82353	10.58824	7.891004	34.18%	16.67%	266.67%
	50	22.35294	42.35294	18.82353	14.93268	26.06%	18.75%	125.00%
	75	20.58824	46.76471	19.11765	14.68369	30.20%	7.69%	144.62%
	100	18.82353	44.11765	18.23529	13.46099	35.47%	3.23%	141.94%
	125	20.58824	47.64706	20	15.19656	31.61%	2.94%	138.24%
Random Networks	25	17.5	32.25	16	12.2877	30.21%	9.38%	101.56%
	50	21.25	40	18	13.92853	29.23%	18.06%	122.22%
	75	22.16495	47.93814	21.13402	15.37474	37.46%	4.88%	126.83%
	100	23.71134	47.93814	22.16495	16.74541	32.36%	6.98%	116.28%
	125	23.96907	47.93814	22.16495	16.98841	30.47%	8.14%	116.28%
Scale-free Networks	25	19.3299	20.61856	16.49485	12.30288	34.07%	17.19%	25.00%
	50	23.71134	29.63918	20.10309	16.47015	22.06%	17.95%	47.44%

	75	25	42.26804	21.90722	18.20349	20.35%	14.12%	92.94%
	100	28.09278	46.90722	25.7732	20.80022	23.91%	9.00%	82.00%
	125	29.38144	49.48454	26.03093	21.35496	21.90%	12.87%	90.10%

Case 6: Large-scale networks with degree-based budget distribution

(Number of nodes is 100.)

Network Topology	No. of Critical OD-pairs	SA$_1$	SA$_2$	LR	LB	Gap	Imp. Ratio of SA$_1$	Imp. Ratio of SA$_2$
Grid Networks	50	33.05556	94.44444	23.05556	16.48301	39.87%	43.37%	309.64%
	100	31.94444	96.11111	26.66667	18.34765	45.34%	19.79%	260.42%
	150	32.5	96.94444	29.16667	20.84595	39.92%	11.43%	232.38%
	200	37.22222	98.88889	32.77778	21.08786	55.43%	13.56%	201.69%
	250	40.83333	94.44444	36.94444	23.14333	59.63%	10.53%	155.64%
Random Networks	50	35.5	75	30.5	20.89109	46.00%	16.39%	145.90%
	100	43	80	38.5	25.62157	50.26%	11.69%	107.79%
	150	44	85	42.25	31.91765	32.37%	4.14%	101.18%
	200	47	92.25	41.75	29.68885	40.63%	12.57%	120.96%
	250	51.75	95.75	46.25	37.33963	23.86%	11.89%	107.03%
Scale-free Networks	50	37.05584	56.09137	29.94924	23.38481	28.07%	23.73%	87.29%
	100	45.68528	75.88833	37.05584	28.72076	29.02%	23.29%	104.79%
	150	46.70051	65.98985	40.10152	31.20025	28.53%	16.46%	64.56%
	200	42.8934	97.96954	42.13198	35.31172	19.31%	1.81%	132.53%
	250	51.52284	75.88833	44.67005	33.1085	34.92%	15.34%	69.89%

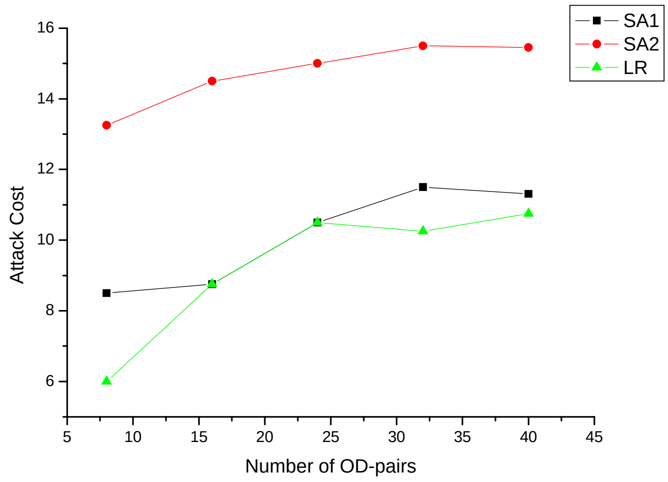

Figure 4-1 Small-Sized Random Networks in Case 4

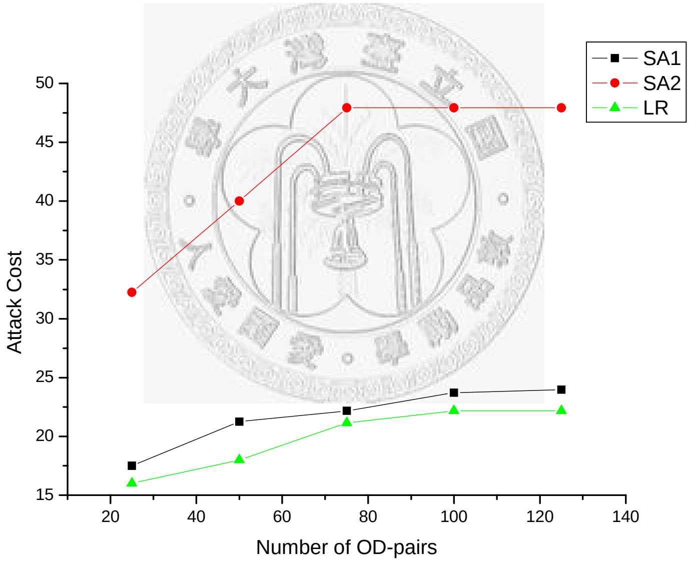

Figure 4-2 Medium-Sized Random Networks in Case 5

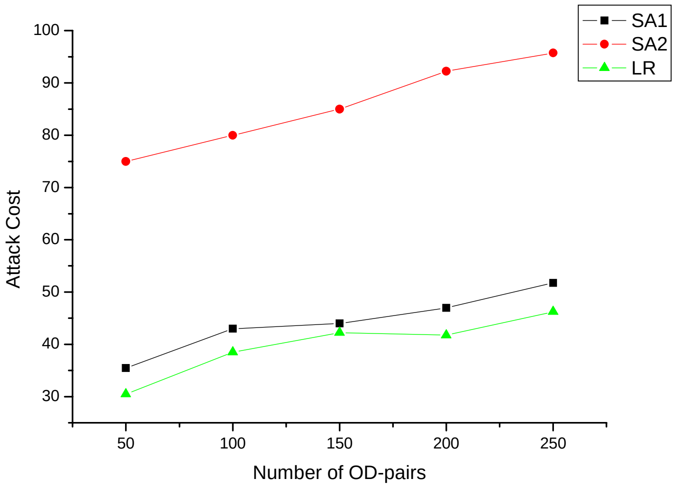

Figure 4-3 Large-Sized Random Networks in Case 6

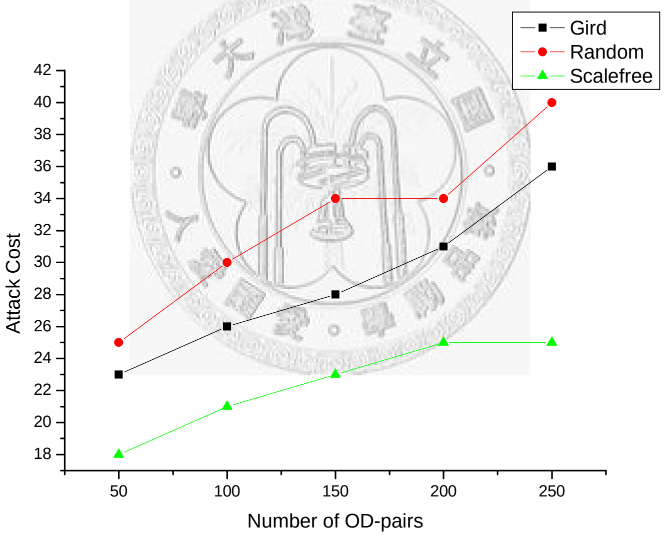

Figure 4-4 Effect of Different Topologies

(cases of a large size network and uniform budget allocation policy)

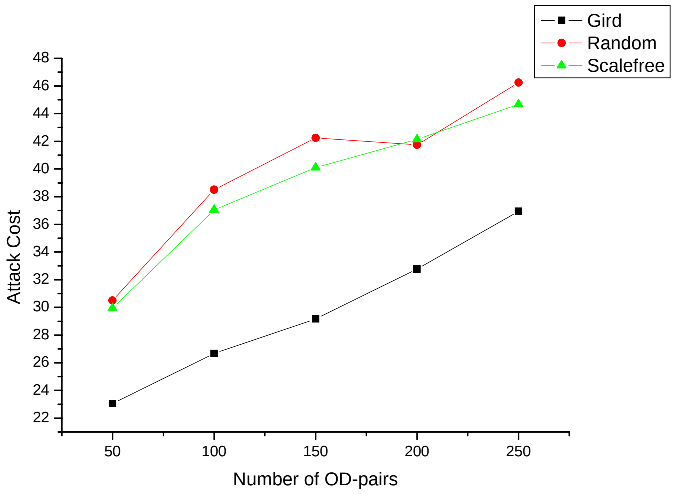

Figure 4-5 Effect of Different Topologies

(cases of a large size network and degree-based budget allocation policy)

4.5 Discussion of the Results

From Figure 4-1, Figure 4-2, and Figure 4-3, we can see that the curves of the LR-based algorithms are always below those of SA_1 and SA_2, which means that the solution quality of LR is evidently better than that of SA_1 and SA_2, for this is a minimization problem.

Looked at in more detail, the solution excellence of the LR-based algorithm is more obvious when a network grows in size and more OD-pairs are considered. The solution quality of SA_2 is not good enough due to its blindness in attacking the most-connected nodes without considering the cost of the attack. Although the solutions of SA_1 are effective in small-scale networks, its drawback of considering the union of minimum-cuts is significant when a network grows.

Since a legitimate lower bound of the primal objective function value (LB) is obtained through the process of Lagrangean Relaxation, we can also evaluate the solution quality of LR by comparing with LB. We find that in a small-scale network, the duality gap, which is calculated by $\frac{\text{LR-LB}}{\text{LB}}*100\%$, is less than 30%. Even in a medium-scale network or a large-scale network, the duality gap in most cases is less than 50%.

Moreover, we find that a network’s topological structure will greatly influence its robustness against attacks. As shown in Figure 4-4, the cost to attack a random network is evidently greater than a grid network or a scale-free network, given that a uniform budget allocation policy is applied, where other conditions, such as the network size, the number of critical OD-pairs, are the same. It indicates that the property of randomness may greatly help maintain the connectivity of a network. As the connectivity of a scale-free network is mainly maintained by a few super nodes, the effect of destroying super nodes is significant and therefore the robustness of a scale-free network is weaker than that of a random network. As to a grid network, the regularity of the topology may be the reason for an attacker to incur a relatively less attack cost to compromise the network.

In addition, if we compare Figure 4-4 with Figure 4-5, we can see that proper budget allocation enhances the robustness of a network. As we can see in Figure 4-4, a random network incurs the highest cost and a scale-free network incurs the lowest cost; in Figure 4-5, while adjusting the budget allocation policy according to the degree of connectivity, we achieve almost the same level of robustness of a random network and a scale-free network. We therefore conclude that if we allocate proper budgetary resources to the high-connectivity nodes, we will effectively increase the costs incurred by an attacker.

4.6 Computational Complexity

The time complexities of all the algorithms we used to solve the problems are presented below.

Table 4-4 Time Complexity

Problem	Time complexity to solve this problem
Subproblem 1	$O(\|W\|\|V\|^2)$
Subproblem 2	$O(\|V\|\log\|V\|)$
Subproblem 3	$O(\|W\|\|L\|)$
Getting Primal Feasible Heuristics	$O(\|W\|\|V\|^5)$
Simple Algorithm 1	$O(\|W\|\|V\|^3)$
Simple Algorithm 2	$O(\|W\|\|V\|^3)$

Chapter 5 Summary and Future Work

5.1 Summary

In this thesis, we have focused on two issues. First, we have shown how robust a network is by evaluating the minimal attack cost it may experience based on the survivability metric of connectivity of given critical OD-pairs. Second, we have presented a lemma showing that the best allocation policy is to evenly distribute the budgetary resources on the nodes along the minimal hop path among all critical OD-pairs.

One of the main contributions of our thesis is the mathematical models. We have researched the problem characteristics carefully, identified the problem objectives and the associated constraints, and proposed the well-formulated mathematical models. We also have solved the problem of minimal attack cost and derived a legitimate lower bound on the number of nodes an attacker should target.

Another contribution is the lemma that solves the max-min complicated form. We have fully described the max-min problem structure and its associated constraints and presented a lemma that solves the problem elegantly.

Moreover, we have evaluated different topologies and observed their survivability under malicious attacks. We have found that a random network is more survivable than a grid or a scale-free network. However, with a proper budget allocation policy, a scale-free network may achieve the same level of robustness as a random network.

5.2 Future Work

There are still a number of research issues to be addressed, which we summarize in the following paragraphs.

Budget Allocation Strategy with an Initial Budget

Recall that, in Section 3.2.2 we presented a lemma for the optimality condition in our definition of survivability. If we consider an initial budget on each node, the trivial solution may no longer hold. One can easily examine this phenomenon via the following graph. In Figure 5-1, the number on each node is the initial budget. If we have an additional unit of budget, what should we do so that the overall $\underset{y_i}{Min}\sum_{i\in V} y_i b_i$ is maximized? If we distribute the additional unit of budget evenly along the minimum hop path, i.e., the budget of A, B, S, and D becomes 5.25, 5.25, 100.25, and 100.25, respectively, the minimal attack cost will be 3+5+5.25 = 13.25. If, on the other hand, we assign all the one unit budget to node C, i.e., the budget of C becomes 4, the minimal attack cost will become 4+5+5 = 14, which is evidently better than the former case. The best budget allocation

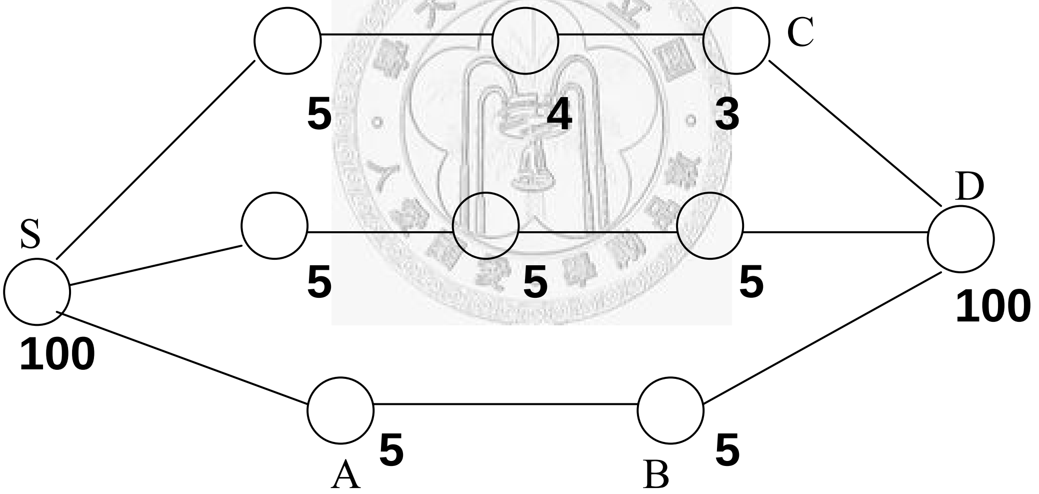

Figure 5-1 A Graph with the Initial Budget

strategy for an initial budget is definitely a very challenging and interesting issue.

Different Survivability Metrics

Another issue to be addressed in the future is the adoption of different survivability metrics in the domain of attack and defense. In this thesis, we assumed that a network is survivable if there is at least one available path between at least one critical OD-pair. To highlight the importance of critical OD-pairs, we can modify the definition of network survivability as follows: if there is at least one available path between **each** critical OD-pair, the network is survivable. To deal with the modification, we find that our original formulation, IP2, remains useful in characterizing the problem: we simply rewrite the constraint, IP2.4, as $M \le \sum_{w\in W}\sum_{l\in L} t_{wl}c_l$.

Moreover, we can further generalize the concept as follows. If there is at least one available path between **a given thresholds of** critical OD-pairs, the network is survivable. We could also analyze the impact on minimal attack cost with different thresholds.

In addition to considering the connectivity of given critical OD-pairs, we could further consider different kinds of connectivity, such as the connectivity of the largest fragment in a network, as survivability metrics. With different definitions of survivability, we believe that we could derive different mathematical models and obtain different but interesting results.

Moreover, we could take the Quality of Services (QoS) performance metrics as our survivability metrics. For example, when considering malicious attacks, if the flow capacities between given OD-pairs are greater than a given threshold, or the average delay is lower than a tolerable level, the system is survivable. Recoverability is another interesting metric. If a system can be recovered within a given time period, it is regarded as acceptable, and therefore, survivable.

Different Attack Behaviors

In our research, we have described the attack behavior on a node as a zero-one decision, i.e., either to attack it or not. Actually, we can further characterize attack behaviors as probabilistic models. A node is more likely to be successfully attacked if fewer budgetary resources are allocated for it. We can therefore claim with 95% confidence, for example, that the system is survivable under malicious attacks and random errors.

Another way to model the attack behavior is the attack path. Assume that an attacker has controlled one or more nodes of the given network; his objective is to reach a core node or multiple core nodes through the most likely path or the minimal attack cost path.

Applications on Different Transmission Media

In our problem description, we assumed a wired network; however, a growing number of applications on the wireless media, such as cellular phone networks, and wireless ad-hoc networks, have drawn much attention in recent years. In a wireless network, a network topology is determined by the transmission radius of each node in the network; therefore, a network topology may be changed dynamically and dramatically. It is definitely a challenging task to incorporate the wireless issues when discussing survivability.

References

[1] 雷定中, “資訊時代國家安全的基礎--通資網路存活率之研究,” *國防通信電子及資訊季刊* 第五期, 2004

[2] Sean P. Gorman, Laurie Schintler, Raj Kulkarni, and Roger Stough, “The Revenge of Distance: Vulnerability Analysis of Critical Information Infrastructure,” *Journal of Contingencies and Crisis Management* vol. 12, pp. 48-63, 2004

[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] A. Broida and K. C. Claffy, “Internet topology: Connectivity of IP graphs, in Scalability and Traffic Control in IP Networks,” S. Fahmy and K. Park, eds., *Proc. SPIE 4526, International Society for Optical Engineering*, Bellingham, WA, pp. 172–187, 2001

[5] Q. Chen, H. Chang, R. Govindan, S. Jamin, S. J. Shenker, and W. Willinger, “The origin of power laws in Internet topologies revisited,” in *Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE Computer Society*, Los Alamitos, CA, 2002

[6] Murali Kodialam and T. V. Lakshman, “Detecting Network Intrusions via Sampling: A Game Theoretic Approach,” *IEEE INFOCOM*, 2003

[7] 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*, Software Engineering Institute, Carnegie Mellon University, 1999

[8] Vickie R. Westmark, “A Definition for Information System Survivability,” *IEEE Proceedings of the 37th Hawaii International Conference on System Sciences*, 2004

[9] M, A. Schroeder, and K. T. Newport, “A Connectivity Using a Graph Theory Approach,” *MTR 9278*, The MITRE Corporation, Rome, NY, 1986

[10] M, A. Schroeder, “A Knowledge-Based Approach to the Computation of

Network Nodal Survivability," *Military Communications Conference, MILCOM 90*, 1990.

[11] Haizhuang Kang, Clive Bulter, and Qingping Yang, "A New Survivability Measure for Military Communication Networks," *Military Communications Conference*, *MILCOM 98*, 1998

[12] Tong Ze Jiang, "A New Definition on Survivability of Communication Networks," *MILCOM*, 1991

[13] Jianxu Shi and John P. Fonseka, "Traffic-Based Survivability Analysis of Telecommunication Networks," *IEEE*, 1995

[14] Ali Zolfaghari and Fred J. Kaudel, "Framework for Network Survivability Performance," *IEEE Journal on Selected Areas in Communications*, vol. 12, No.1, 1994

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

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

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

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

[19] Albert-Laszlo Barabasi and Reka Albert, "Emergence of Scaling in Random Networks," *Science* 286, pp. 509-512, 2001

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

[21] A. M. Geoffrion, "Lagrangean Relaxation and its use in Integer Programming," *Mathematical Programming Study*, vol. 2, pp. 82-114, 1974

[22] M. Held, *et al.*, "Validation of subgradient optimization," *Math. Programming*, vol. 6, pp. 62-88

簡 歷

姓 名：陳建宏

出生地：台灣省台北縣

出生日：中華民國七十年八月九日

學 歷：八十八年九月至九十二年六月
國立台灣大學資訊管理學系

九十二年九月至九十四年七月
國立台灣大學資訊管理學研究所