

國立臺灣大學管理學院資訊管理學系

碩士論文

Graduate Institute of Information Management

College of Management

National Taiwan University

master thesis

考慮攻擊者學習效應下之網路存活度衡量

An Evaluation of Network Survivability under
the Effect of Discounted Defense Levels
by Accumulated Experiences of Attackers



陳怡孜

Sherry, Yi-Tzu Chen

指導教授：林永松 博士

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

中華民國 96 年 7 月

July, 2007



考慮攻擊者學習效應下之網路存活度衡量

An Evaluation of Network Survivability under
the Effect of Discounted Defense Levels
by Accumulated Experiences of Attackers



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

陳怡孜

Sherry, Yi-Tzu Chen

指導教授：林永松 博士

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

中華民國 96 年 7 月

July, 2007



國立臺灣大學碩士學位論文
口試委員會審定書

考慮攻擊者學習效應下之網路存活度衡量

An Evaluation of Network Survivability under
the Effect of Discounted Defense Levels
by Accumulated Experiences of Attackers

本論文係 陳怡孜 君（學號 R94725054）在國立臺灣大學資訊管理學系、所完成之碩士學位論文，於民國九十六年七月十九日承下列考試委員審查通過及口試及格，特此證明

口試委員：

孫雅潔

吳俊宏

龔宏旭

林水松

祝國忠

所 長：

孫雅潔



謝誌

隨著論文的完稿畫上句號，薄薄一疊紙，是時間熬成的心血。「There is an end and there is a beginning」，結束同時，沒有離愁，因為我知道，學無止境。回首一年半的研究生涯，苦樂參半，從四處奔走找資料、挑燈夜戰的案牘勞形，到腸思枯竭、一片混沌鬱悶的煩心。感謝這一切的發生，因為我開始體悟出作研究的樂趣。

首先，感謝我敬愛的父母陳品睿先生和顏瓊爵女士，您們博大的胸懷與無聲的愛包容了我的一切，在我的人生路上建造了溫暖而平靜的空間，讓我不孤單；感謝我的家人，哥哥陳怡璋和姊姊陳柔妤，在春去秋來的風雨裡，有你們幫我頂著頭頂上的一片天，我才能無後顧之憂的致力於研究。

滿滿的感激要獻給恩師林永松教授，不論是在研究方向給予的指引及鼓勵，甚或不厭其煩解惑，尤其當自己思緒打結時，老師的一番話語總是讓我豁然開朗；更重要的是，從老師的身上，我漸漸領會做學問應具備的嚴謹思考以及待人處世謙卑的態度。此外也感謝本系孫雅麗教授、輔仁大學呂俊賢教授、世新大學顏宏旭教授、景文科技大學祝國忠教授，在口試時對本篇論文的指正及寶貴的建議，讓我發現了當初研究時的盲點，使得本論文更臻至完善。

感謝資安小組大家長柏皓學長，雖然是在糊里糊塗的情況下就變成了傳說中資安小組的閉門小弟子，才有機會擁有學長一路過來的打氣，和不斷的討論及建議，現在的我才能如此幸運。另外感謝資安小組的學長姐：雅芳、俊維、承賓、坤道及網路組的翊恆和豈毅學長，陪著我一同哀嚎度過苦難的歲月，我的研究生涯因此而多采多姿；中蓮學姐和義倫學長，感謝你們在這段時間不斷地關心我論文進度，更在我手足無措時，替我加油。

最後感謝奕廷、孜謙、政祐、至浩和志元，以及貝瑜、宇頌及景翔，因為你們的陪伴，讓緊繃的精神總是能鬆一口氣，尤其是在我困頓時，還會瘋狂地灌迷湯，沒想到最後真的能闖關成功！謝謝你們！

我捧著滿滿的感謝回到自己的生命裡，將雙臂展開，輕輕的轉一個圈子，溫暖的氣息灑遍角落，頓時間，我的生命因此而閃閃發光，謝謝願意在我生命中出現的你們！

陳怡孜 謹識
于台大資訊管理研究所
民國九十六年七月



論文摘要

論文題目：考慮攻擊者學習效應下之網路存活度衡量

作者：陳怡孜 九十六年七月

指導教授：林永松 博士

在九零年代開始，網際網路逐漸演變成全球共通的溝通媒介，許多恐怖份子開始利用其攻擊政府及國家，此一行為嚴重危害國家安全。是故，資訊安全逐漸演變成重要的議題。因此對網路營運者而言，如何有效評估網路攻擊者的威脅，達到提升網路存活度的問題已愈趨重要。

因此，本研究利用數學規劃及圖形理論為工具，建構網路攻防情境的資源分配問題，分別提出AEA(Accumulated Experiences of Attacker)與AAEA(Advanced Accumulated Experiences of Attacker)。於AEA模型中，先轉化存在旅行推銷員問題中，於不同城鎮間購買折扣券以降低旅行成本的概念，茲代表網路在攻擊者利用自身經驗及攻克節點成功時所獲得的經驗，以影響未來攻擊成本之情境，即：所有節點一經攻克後，所獲得之經驗將有效地降低後續發生的攻擊成本，並考慮攻擊者以一節點為入口進入目標網路之後，在經驗值影響下尋求一條最短路徑，俾便攻克網路中的一個目標節點，使目標網路無法存活，且利用圖形理論將問題轉化，運用一般化最短路徑演算法求解之；在AAEA模型中，考慮相同的攻擊者問題下，更考量攻擊者可在節點上花費不同等級之額外成本，以獲取對攻擊其餘網路節點不同等級的資訊(如：使用者權限或是網路拓撲圖...等)，達到有效地降低後續攻擊成本，由於此問題藉由圖形理論的轉化，也將AAEA模型利用一般化最短路徑演算法求解之。

關鍵詞：資訊安全、網路攻防、存活度、資源分配、旅行推銷員問題、經驗折扣、圖形理論、節點分裂法、一般化最短路徑、最佳化

THESIS ABSTRACT

GRADUATE INSTITUTE OF INFORMATION MANAGEMENT NATIONAL

TAIWAN UNIVERSITY

NAME : SHERRY, YI-TZU CHEN MONTH/YEAR : JULY/2007

ADVISER : FRANK, YEONG-SUNG LIN

AN EVALUATION OF NETWORK SURVIVABILITY

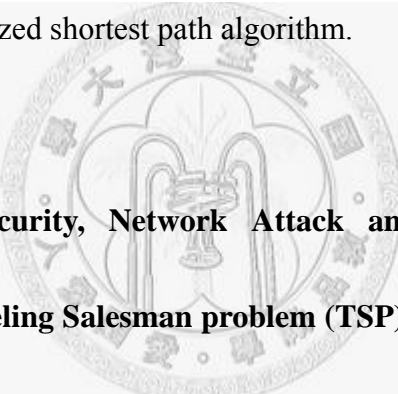
UNDER THE EFFECT OF DISCOUNTED DEFENSE LEVELS

BY ACCUMULATED EXPERIENCES OF ATTACKERS

Internet has become worldwide, publicly accessible network of interconnected computer networks since 1980s. Specifically, it becomes the tools that terrorists can use to attack the nations and their economy. Thus, any network operator could improve the network's survivability by effectively evaluating the attacker behavior.

As a result, this thesis focuses on the resource allocation of network attack and defense with mathematical programming and graph modeling to optimize the problems, and adopts a concept, discount coupon which is applied in TSP, to represent the attacker behavior of taking advantage of accumulated experiences from his previous attack actions of minimizing the total attack cost. In AEA, the attacker somehow gains some free experiences from a compromised node which could further reduce the cost of an attack. The attacker's objective is to minimize the total attack cost, while the core node is compromised and the network could not survive. Here, by transforming AEA with

node splitting into a generalized shortest path problem and applying the algorithm to optimally solve it. In AAEA, the attacker not only gains some free experiences from a compromised node but could spend different levels of extra expenses, probing fee, gaining different levels of valuable experiences, such as diverse user's rights or a network topology. Therefore, AAEA is proposed to describe such behavior which is also analyzed as a mixed nonlinear integer programming optimization problem. With node splitting technique, AAEA is transformed into a shortest path problem and is optimally solved by generalized shortest path algorithm.



Key words: Internet Security, Network Attack and Defense, Survivability, Resource Allocation, Traveling Salesman problem (TSP), Discount Coupon, Graph Modeling, Node Splitting, Generalized Shortest Path Problem, Optimization.



Table of Contents

論文口試委員審定書	I
謝誌	II
論文摘要	III
THESIS ABSTRACT	IV
Table of Contents	VI
List of Figures	VIII
Chapter 1 Introduction	1
1.1 Background	1
1.2 Motivation	3
1.3 Literature Review	6
1.3.1 Survivability of Quantitative Analysis with Attacker Behavior	6
1.3.2 Traveling Salesman Problem	9
1.4 Proposed Approach	11
1.5 Thesis Organization	12
Chapter 2 Graph Modeling of AEA and AAEA Models	13
2.1 Problem Description and Graph Modeling of AEA	13
2.1.2 Graph Modeling of AEA	14
2.2 Problem Description and Graph Modeling of AAEA	18
2.2.1 Problem Description of AAEA	18
2.2.2 Graph Modeling of AAEA	18
Chapter 3 Problem Formulation	21
3.1 Problem Formulation of AEA	21
3.1.1 Problem Assumptions	21
3.1.2 Notation and Formulation	23
3.2 Problem Formulation of AAEA	26
3.2.1 Problem Assumptions	26
3.2.2 Notation	27
Chapter 4 Solution Approach	30
4.1 Generalized Shortest Path Problem	31
4.2 Solution Approach to AEA	32
4.3 Solution Approach to AAEA	33
Chapter 5 Conclusion and Future Work	34
5.1 Conclusion	34
5.2 Future Work	35
Reference	42
簡歷	46

List of Tables

Table 1- 1 Default Security Settings for Groups	5
Table 3- 1 Problem Assumptions of the AEA.....	22
Table 3- 2 Problem Descriptions of the AEA	22
Table 3- 3 Given Parameters of the Proposed Model.....	23
Table 3- 4 Decision Variables of the Proposed Model	24
Table 3- 5 Problem Assumptions of the AAEA.....	26
Table 3- 6 Problem Descriptions of the AAEA	27
Table 3- 7 Given Parameters of the Proposed AAEA	27
Table 3- 8 Decision Variables of the Proposed AAEA.....	28
Table 5- 1 Given Parameters of the Proposed Model.....	38



List of Figures

Figure 1- 1 Typical Attacking Process [13]	7
Figure 1- 2 Attack Potential Increasing Over Time [15].....	8
Figure 1- 3 An Example of TSP [18].....	10
Figure 1- 4 An Example of GTSP [18].....	10
Figure 2- 1 An Attack Scenario	16
Figure 2- 2 An Attack Scenario with Node Splitting.....	17
Figure 2- 3 An Attack Scenario with Node Splitting in Different Levels	20
Figure 5- 1 An Attack Scenario	37
Figure 5- 2 Interaction between Attackers and Defenders	41





Chapter 1 Introduction

1.1 Background

After the unprecedented attacks on New York and Washington, September 11, 2001, the clash of identities played out in the transformed Internet Security environment of the post-9/11 world. This incident arises increasing number of researches to emphasize the effective and efficient protection of infrastructures, which encompass a wide array of physical assets, such as electric power grid, telecommunications, oil and gas pipelines, transportation networks and computer data networks [1]. Specifically, Internet has become worldwide, publicly accessible network of interconnected computer networks that consists of millions of smaller domestic, academic, business, and government networks, which together carry various information and services, such as E-mail, online chat, file transfer, E-commerce and the interlinked Web pages and other documents of the World Wide Web since 1980s. However, this new technology has become the tools that terrorists can use to attack the nations and their economy.

Most network security issues depend on certain underlying assumptions about the

nature and structure of systems [2]. These assumptions generally include that systems are closed, that they are under central administrative control, and that administrators have the ability to observe any given activity within the system. Today, these kinds of assumptions may have no longer been appropriate while systems are not with highly controlled interfaces. As a result, systems are unbounded nowadays without any full administrative control [3].

Network Security issues were traditionally focused on hardness, resistance, and confidentiality of information. The state of such issues was used to define as safe or compromised [4]. Nowadays, security is related to the availability of information and continuity of services. Therefore, the binary concept is no longer sufficient to depict a system's state under malicious attacks or random error conditions. Concerning of the continuity to the critical services among the infrastructure providers, their customers, enterprise, and government agencies have gradually generalized as new field of security issue, survivability [5] [6] [7] [8] [9]. The most common definition of it is proposed by Ellison et al. [4], which is “the capability of a system to fulfill its mission, in a timely manner, in the presence of attack, failures, or accidents.”

1.2 Motivation

In an attack-defense scenario, the attacker sometimes has valuable information before his attack actions. For example, the attacker might know a newly discovered hole in a program or operating system before the software developer has made a fix available, which are known as **Zero day Attack** [10]. According to [10], sixty eight percent of the vulnerabilities found by Symantec are not confirmed by the affected vendor. For this reason, many attackers could make use of the vulnerability or hole in some piece of software to attack the target network. Moreover, in some situations, attacker could be the former or laid-off employee of the enterprise, who still has the ID and password valid of the networks. That is, these kinds of attacker behavior represent that the attacker might have some important information to discount his future attack cost before his attack actions starting.

Furthermore, after compromising a node, the attacker should gain some useful experiences from this node. For instance, the attacker could know the trust relationship [11], i.e. an administration and communication link between two domains, of the target networks. Under this circumstance, account information is shared to validate the rights and permissions of user accounts and global groups residing in the trusted domain without being authenticated. Owing to that, the trust relationship can simplify user

administration by combining two or more domains into an single administrative unit, the attack compromise a node then know the trust relationship of the network, this kind of experiences could effectively reduce the further attack cost.

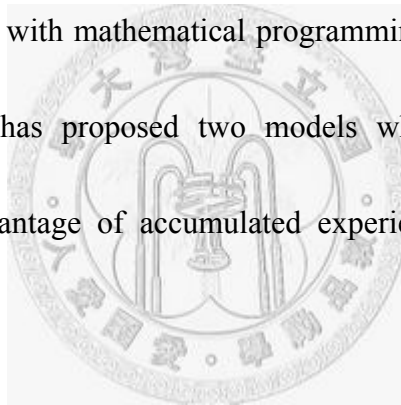
Since the attacker could gain the free experiences after compromising a node, he might pay different degrees of extra fee, which could be money or time to probe a compromised node and gain different levels of valuable experiences. The higher level of experience accompanies with the higher probing fee. If the attacker probes to the higher levels, it represents that this experience results in better benefit then the former ones. For example, Table 3- 1 [12] provides descriptions of the default groups located in the groups folder and lists the assigned user rights for each group. These rights are assigned within the local security policy. If attacker probes to a certain level to gain the Power User's rights, he does not need to spend another fee gaining the Guest rights, since the Power User's right includes Guest's. Although the most useful information could be worthwhile probing, the probing fee could be too expensive to result in unbenefited. To probe, or not to probe: that is a tradeoff. The attackers have the limited resource to attack the target network. It is a problem to strike the balance between gaining the discount to reduce the further attack cost and increasing the total attack cost with spending probing fee.

Table 1- 1 Default Security Settings for Groups [12]

Group	Administrators	
Description	Members of this group have full control of the server and can assign user rights and access control permissions to users as necessary. The Administrator account is also a default member. When this server is joined to a domain, the Domain Admins group is automatically added to this group. Because this group has full control of the server, add users with caution.	
Default rights	<ol style="list-style-type: none"> 1. Access this computer from the network; 2. Adjust memory quotas for a process; 3. Allow log on locally; 4. Allow log on through Terminal Services; 5. Back up files and directories; 6. Bypass traverse checking; 7. Change the system time; 8. Create a pagefile; 9. Debug programs; 10. Force shutdown from a remote system; 11. Increase scheduling priority; 12. Load and unload device drivers; 	<ol style="list-style-type: none"> 13. Manage auditing and security log; 14. Modify firmware environment variables; 15. Perform volume maintenance tasks; 16. Profile single process; 17. Profile system performance; 18. Remove computer from docking station; 19. Restore files and directories; 20. Shut down the system; 21. Take ownership of files or other objects.
Group	Power Users	
Description	Members of this group can create user accounts and then modify and delete the accounts they have created. They can create local groups and then add or remove users from the local groups they have created. They can also add or remove users from the Power Users, Users, and Guests groups. Members can create shared resources and administer the shared resources they have created. They cannot take ownership of files, back up or restore directories, load or unload device drivers, or manage security and auditing logs.	
Default rights	<ol style="list-style-type: none"> 1. Access this computer from the network; 2. Allow log on locally; 3. Bypass traverse checking; 4. Change the system time; 	<ol style="list-style-type: none"> 5. Profile single process; 6. Remove computer from docking station; 7. Shut down the system;
Group	Users	
Description	Members of this group can perform common tasks, such as running applications, using local and network printers, and locking the server. Users cannot share directories or create local printers. By default, the Domain Users, Authenticated Users, and Interactive groups are members of this group. Therefore, any user account created in the domain becomes a member of this group.	
Default rights	<ol style="list-style-type: none"> 1. Access this computer from the network; 2. Allow log on locally; 3. Bypass traverse checking; 	
Group	Guests	
Description	Members of this group will have a temporary profile created at log on, and when the member logs off, the profile will be deleted. The Guest account (which is disabled by default) is also a default member of this group.	
Default rights	No default user rights.	

Because of the limited resources, the attacker would keep the total attack cost in budget. Once the attacker compromised a node, he could gain some useful experiences which could somehow reduce the cost to compromise the rest of the nodes. Thus, the attacker makes use of the experiences to compromise the network with minimal cost by adjusting the policy.

Nevertheless, to the best of our knowledge, there are seldom researches about network attack and defense with mathematical programming to optimize the problems. Consequently, this thesis has proposed two models which described the attacker behavior about taking advantage of accumulated experiences to minimize the total attack cost.



1.3 Literature Review

In this section, the followings are some related works about survivability, attacker behavior, and discount coupon of the TSP (traveling salesman problem).

1.3.1 Survivability of Quantitative Analysis with Attacker Behavior

Some researchers [13] tried to use empirical data which were collected under

controlled conditions. But these kinds of intrusion process were thoroughly supervised and a great deal of data needs to be recorded. In [13], this paper also mentioned that the different phases of the attacker. As shown in Figure 1- 1, the attack behavior split into 3 phases: a learning phase, a standard attack phase, and an innovative attack phase. The main idea in this evolution is the attacker could gain experiences or other useful information by time.

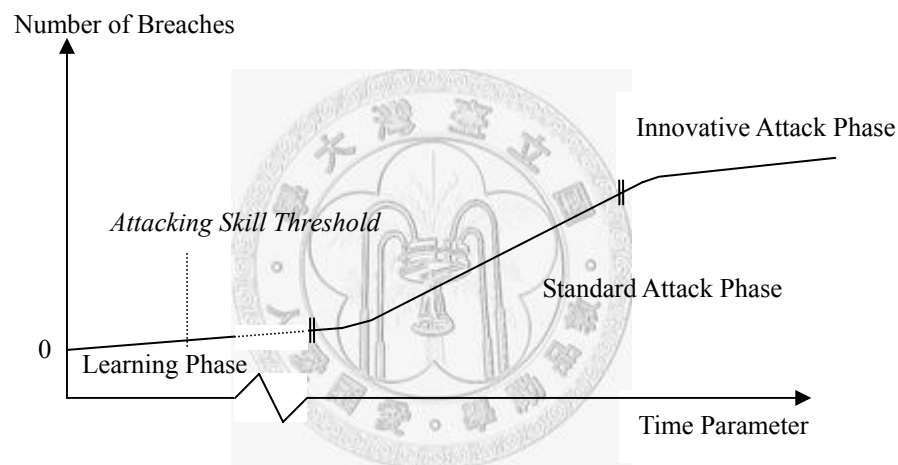


Figure 1- 1 Typical Attacking Process [13]

Ortalo et al. [14] presented the results of an experiment in security quantitative evaluation of the security of operational systems. The quantitative evaluation was based on a theoretical model, privilege graph, which described the system vulnerabilities that offered opportunities to potential attackers to defeat some security objectives. This research discussed the validity of these assumptions which were based on an experimental study performed on a real system and identified the scenarios of attacks

that might be attempted by a potential attacker to reach the target. In this model the attacker is sensible and he would not attempt an elementary attack that would give him privileges that he already possesses, i.e. the attacker would make use of the information that he has already known.

In recent years, a work in quantitative modeling of security with high-consequence systems was done by McDermott et al. [15] in 2005. They pointed out that the quantitative modeling of survivability for validation or measurement should be based on detailed intruder models. Since intruders are humans or are controlled by humans, they not only learn but accumulate experiences. Thus the unlikely intruder of today becomes the most probable intruder of tomorrow. In a word, the distribution of the intruder's attack potential behaviors which is shown in Figure 1- 2, moves to the right over time. The intruder's attack potential behaviors could have major impact on the survivability.

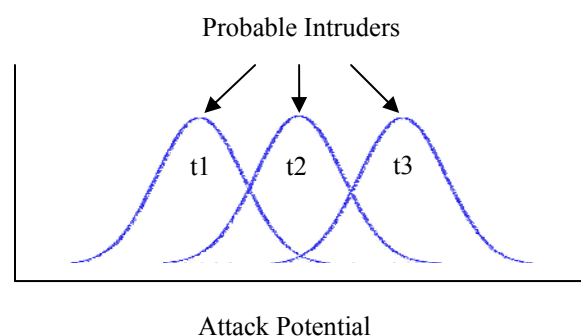


Figure 1- 2 Attack Potential Increasing Over Time [15]

In [16], this paper proposed two mathematical models to evaluate the survivability of a given network under two different metrics; they assessed the minimal attack cost incurred by an attacker. The two survivability metrics were assumed to be the connectivity of at least one given critical Origin-Destination pair (O-D pair) and that of all given critical O-D pairs. And they analyzed the problem with two optimization-based models, in which the problem structure is, by nature, a mixed nonlinear integer programming problem, as well. Though this research provided a well-formulated model of the attacker behavior, it neglected the experiences of the attackers over time.

1.3.2 Traveling Salesman Problem

The traveling salesman problem (TSP) [17] [18] [19] is a problem in discrete or combinatorial optimization. It is a prominent illustration of a class of problems in computational complexity theory which are hard to solve. Given a number of cities and the costs of traveling from any city to any other city, the solution to TSP is the cheapest round-trip route that visits each city exactly once and then returns to the starting city. In Figure 2- 1 [17], it shows that a tour, (1, 2, 3, 4, 5), which is obviously conjectured to be optimal in a regular pentagon. As a result, several scheduling and resource allocation problems of interests to the researchers have been formulated as TSPs or close variants.

For instance, a related problem is the bottleneck traveling salesman problem (bottleneck TSP) [20]: find a Hamiltonian cycle in a weighted graph with the minimal length of the longest edge. And GTSP (Generalized Traveling Salesman Problem) [21], a m set with several nodes in each sets can be also transformed into a m nodes TSP. Figure 2- 2 shows GTSP in a digraph, where the feasible tour is in bold.

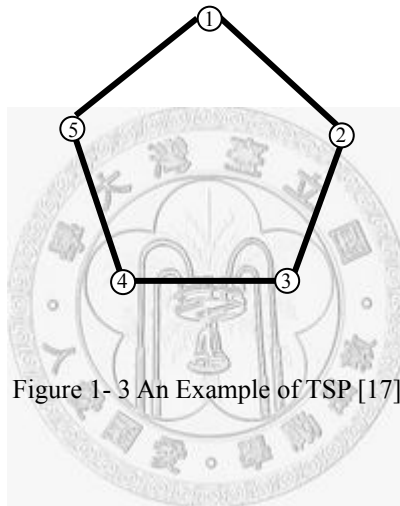


Figure 1- 3 An Example of TSP [17]

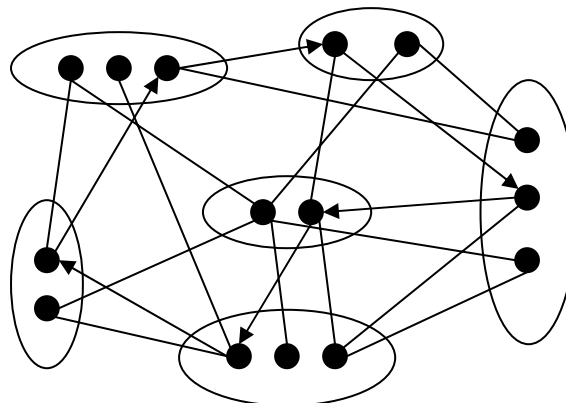


Figure 1- 4 An Example of GTSP [21]

An interesting application in the area of planning and scheduling problems has been discussed in [22]; the algorithm presented in this paper set each node with a coupon, whose price is chosen randomly. A salesman can only buy one coupon in each tour, with different coupon comes different discount factor falls in $[0, 0.8]$. Thus, the solution decides which node to buy the coupon could come up with the most benefit.

1.4 Proposed Approach

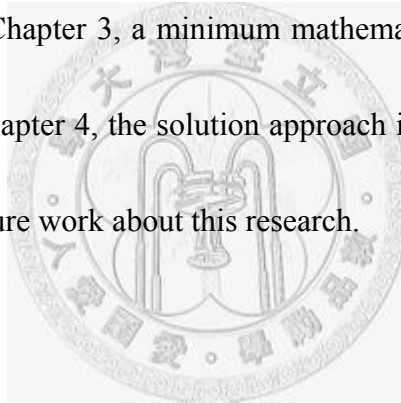
Above all discussions are about the related works of attacker behavior and discount coupon in TSP. Hence the coupon to the salesman in TSP is quite similar with the accumulated experiences of attacker behavior in real world, the accumulated experiences of the attacker is presented by applying discount coupon concept into network resource allocation.

To the best of our knowledge, very little research is done to model network attack and defense problem in quantitative terms. As a result, in this research, the attacker behavior via mathematical programming is modeled. Given that the discount factor represents two kinds of experiences from the compromised node. The attacker's objective is to minimal the total attack cost and compromising the core node, so that the network is not survival. The experience comes with compromised nodes without extra

fee models as Accumulated Experiences of Attacker (AEA); the extra experiences which should spend extra fee could model as Advanced Accumulated Experiences of Attacker (AAEA) and adopt the Generalized-Reverse-Dijkstra algorithm [23] to solve these problems.

1.5 Thesis Organization

The remainder of this thesis is organized as follow. In Chapter 2, a graph modeling technique is presented. In Chapter 3, a minimum mathematical formulation of attacker behavior is proposed. In Chapter 4, the solution approach is presented. Finally, Chapter 5 is the conclusions and future work about this research.



Chapter 2 Graph Modeling of AEA and AAEA Models

In chapter 2, a modeling technique on an attack-defense scenario is demonstrated.

The more details are shown in the followings.

2.1 Problem Description and Graph Modeling of AEA

2.1.1 Problem Description of AEA

This research considers network survivability in terms of protection of the “core node” in which organizations store their most valuable knowledge. Because of the node’s importance, attackers do their best to compromise it. As attack resources are limited, the attacker needs guidelines about how to make use of the experiences and his budget to compromise a node is addressed through this problem.

In AEA, the attacker somehow gains some free experiences from a compromised node which could further reduce the cost of an attack. The objective is to minimize the total attack cost from an attacker’s perspective, while the core node is compromised and

the network could not survive. Thus, the minimum attack cost could be also viewed as the evaluation of the robustness of a network under intentional or malicious attack from defenders' perspective.

2.1.2 Graph Modeling of AEA

In AEA, given that, the attacker has complete information about the targeted network topology and defense strategy. Though it is nearly impossible for an attacker to know everything about a network, the problem is assumed that is a worst case scenario for the network defender, so that the attack power is overestimated in this research.

In Figure 2- 1, initially, the network could have the core node in which enterprise stores their most valuable knowledge. The objective of the attacker is to enter this network via choosing a starting node and to compromise the core node by a serial of compromised nodes. And during the attack actions, the total attack cost is affected by the free experiences from a compromised node, i.e. discount factor. The minimum of the total attack cost is the optimal solution to the problem. By ignoring the discount factor, the problem is quite similar with a shortest path problem. But the solution to shortest path problem, like Dijkstra algorithms, is obtained an optimal solution by node labeling. Therefore, a node splitting transformation to this attack scenario into a shortest path

problem is presented as following.

The node splitting transformation splits each node i into dummy node i' and dummy node i'' , which corresponds to the node input and output, respectively, is illustrated as Figure 2- 2. Then an artificial link is introduced between node i' and node i'' , which represents as L_2 , and it replaces original node and its attributes, which are attack cost and discount factor. Meanwhile, L_2 are connected with a connected cost ε , otherwise with a disconnected cost $M + \varepsilon$. The original links, L_1 , only represent the connectivity of nodes. Besides, a dummy original node O and a dummy destination D node are introduced as well, which are connected to the dummy nodes i' and dummy nodes i'' with artificial link, L_3 . The dummy original node O and a dummy destination node D could take as the attacker's entrance and exit of a serial attack action. Remarkable for this, the artificial links, L_1 , L_3 , are with a discount factor 1. With this technique, AEA is completely transformed into a shortest path problem.

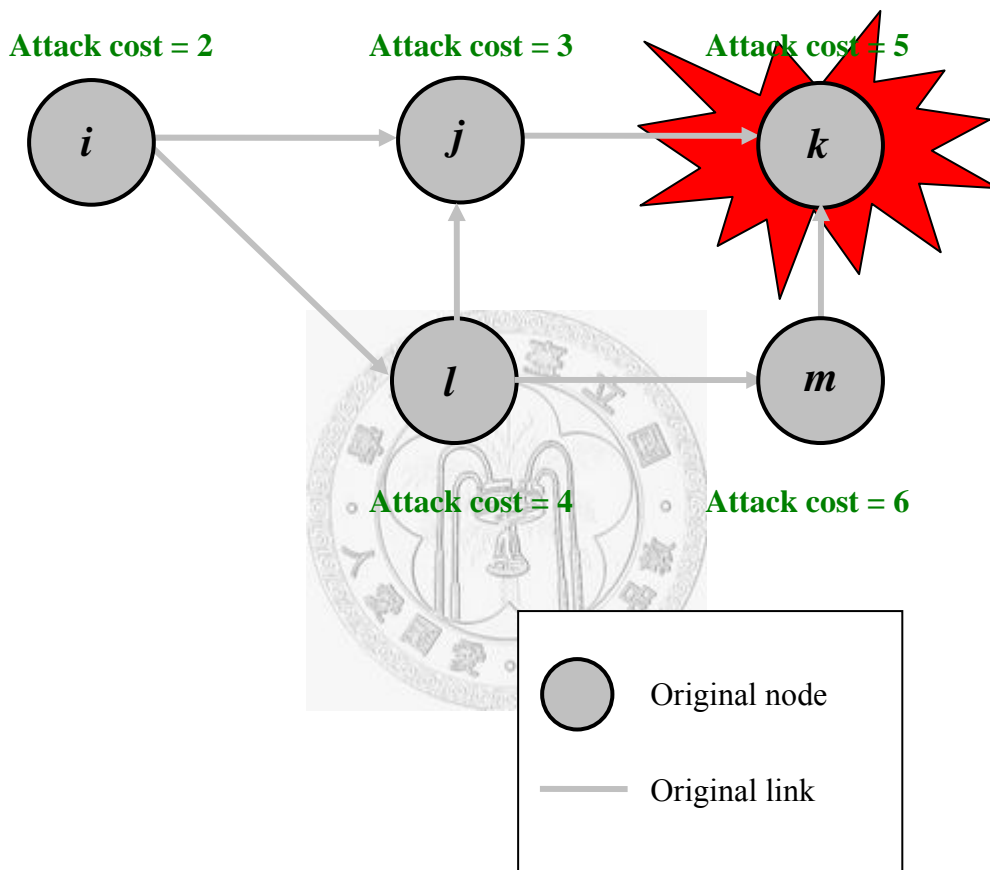


Figure 2- 1 An Attack Scenario

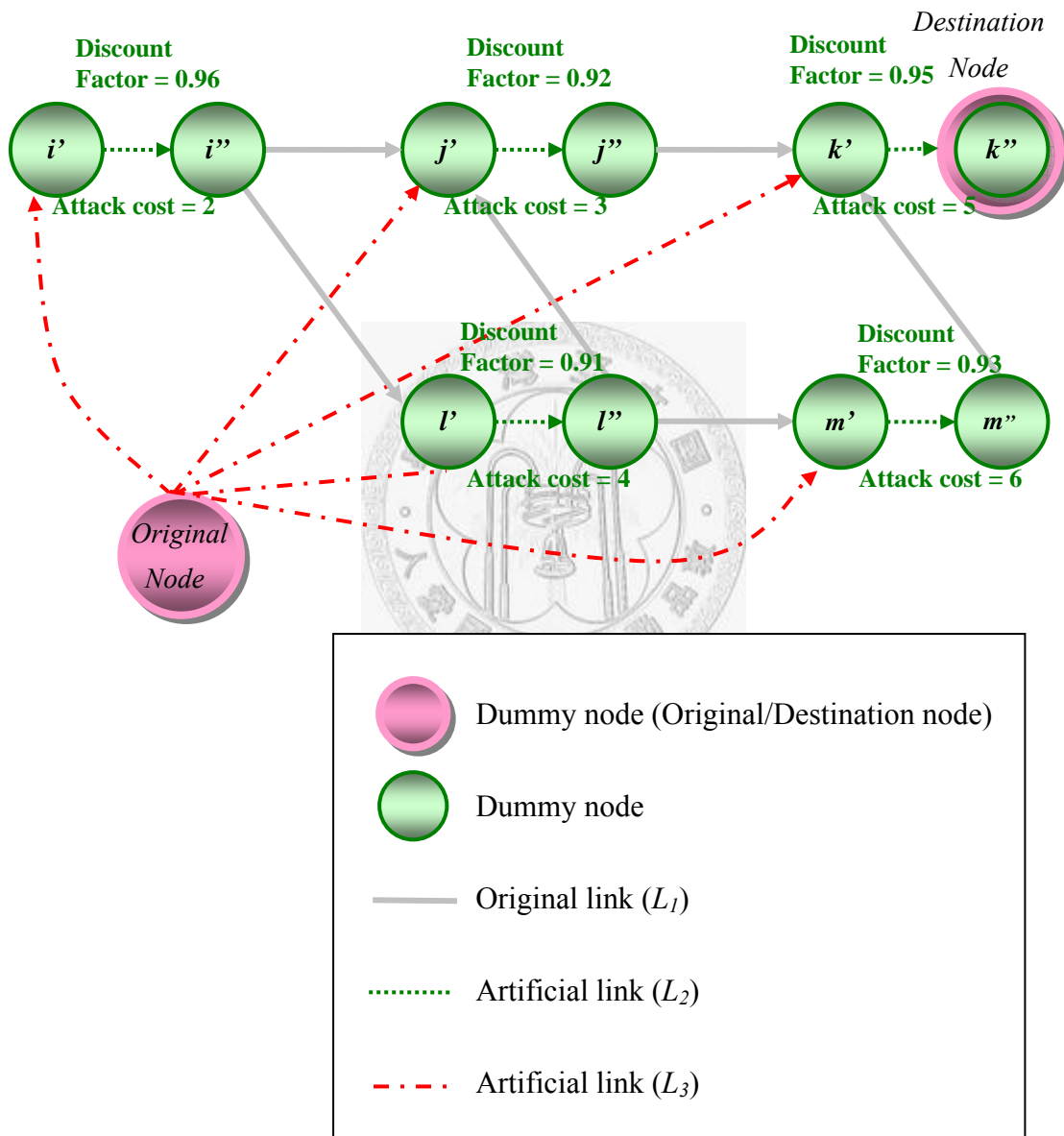
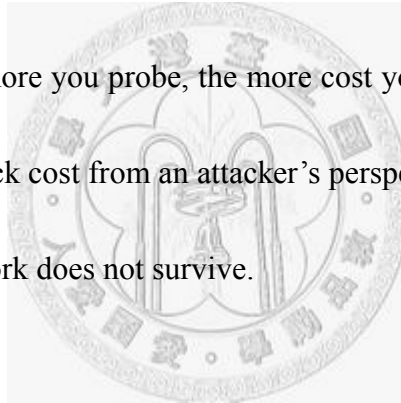


Figure 2- 2 An Attack Scenario with Node Splitting

2.2 Problem Description and Graph Modeling of AAEA

2.2.1 Problem Description of AAEA

In AAEA, a more reality model is further extended. From the practical point of view, the attacker could not only gain some free experiences from a compromised node also spend extra expenses, probing fee, gaining some valuable information or experiences. Nevertheless, the probing fee are various among different degrees of the probing. By intuition, the more you probe, the more cost you should pay. The objective is to minimize the total attack cost from an attacker's perspective, while the core node is compromised and the network does not survive.



2.2.2 Graph Modeling of AAEA

Compared with AEA, the attacker has to make decisions of which level to probe in order to gain the valuable discount factor with minimum total attack cost in AAEA. Due to this characteristic, node splitting is demonstrated again to transform the problem. As Figure 2- 4 shows, artificial nodes and conjunction nodes are introduced to represent different levels between dummy nodes i' and dummy nodes i'' . The artificial link, L_4 , connected from artificial node to the conjunction node c' is a link with attribute (d_{ij}, m_{ij}) on it. m_{ij} is the extra fee to gain the level j 's discount factor d_{ij} . The artificial link, L_2 ,

with attack cost and discount factor is 1 from dummy nodes i' to conjunction node c' .

The artificial links from artificial node to conjunction node c'' and from conjunction node c'' to dummy nodes i'' are all L_3 with a discount factor is 1 and cost is 0. By this transformation, AAEA could be also transformed into a generalized shortest path problem.



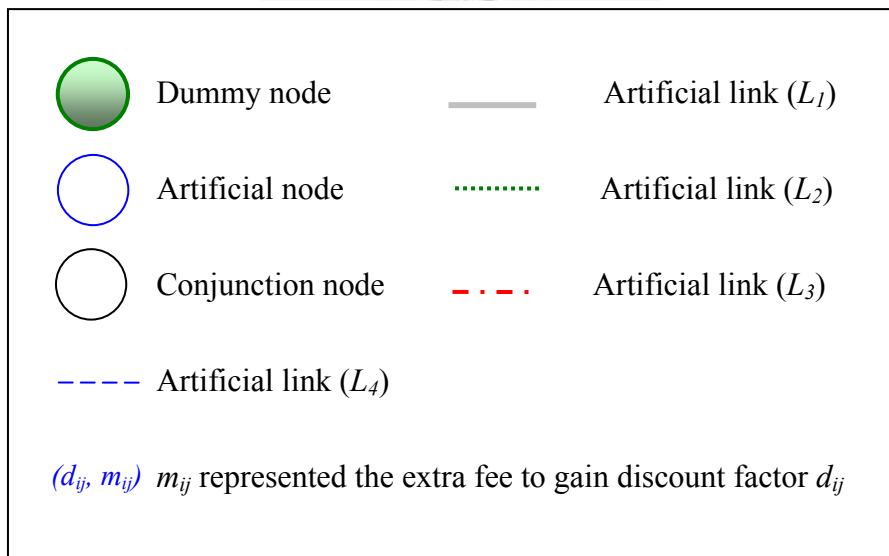
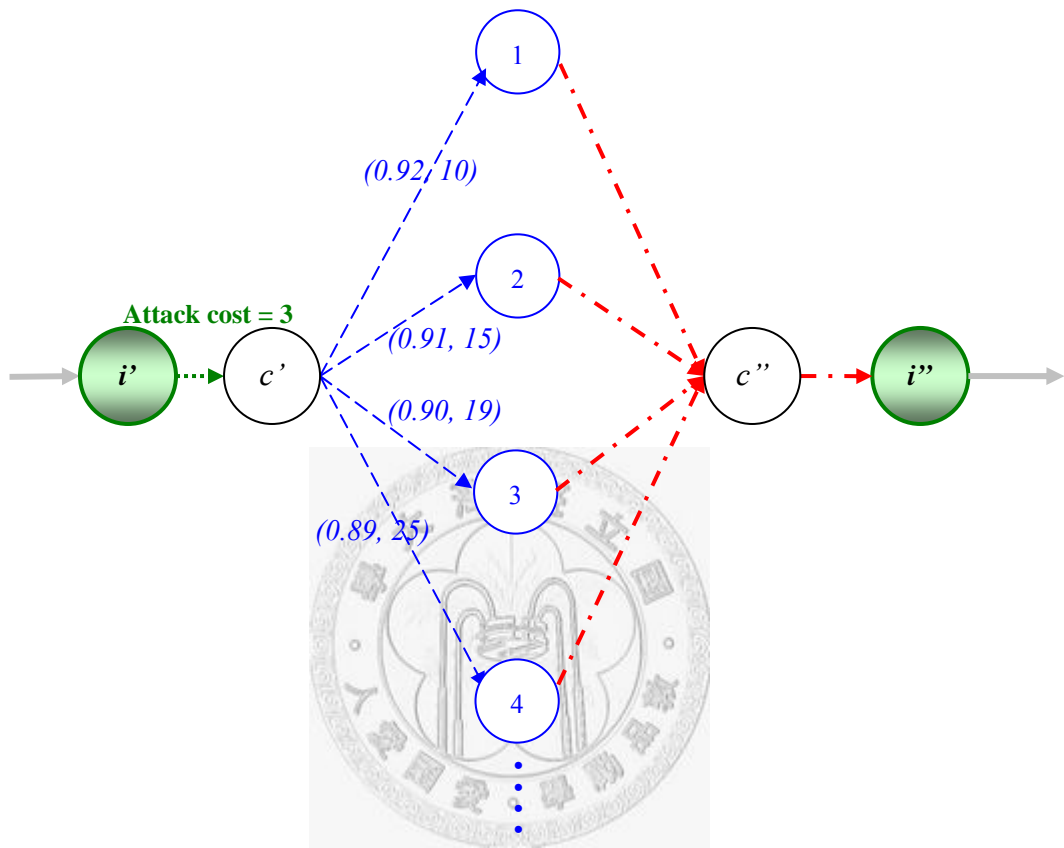
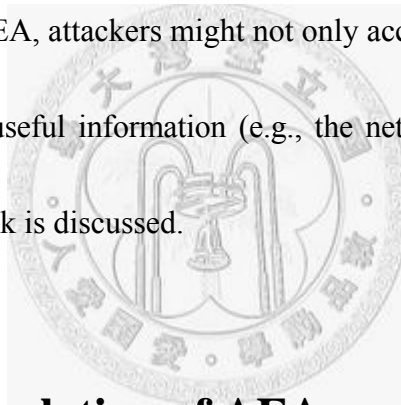


Figure 2- 3 An Attack Scenario with Node Splitting in Different Levels

Chapter 3 Problem Formulation

In this chapter, two mathematical models with specific assumptions and problem objectives are proposed. In AEA, that attacker may gain experiences from his previous attack actions (i.e., obtained discount coupons) to further reduce the cost of a future attack is considered. In AAEEA, attackers might not only accumulate experiences but pay an extra fee to gain more useful information (e.g., the network's topology) for further reducing the cost of an attack is discussed.



3.1 Problem Formulation of AEA

3.1.1 Problem Assumptions

Given that both the attacker and the defender have information about the targeted network topology. Meanwhile, the attacker has complete information about the defender's budget allocation. Though it is almost impossible for the attacker to know everything about the target network, the problem is described as a worst case scenario with specific assumptions and problem objectives in the following sections. In general, researchers focus on the node failure but link failure, which are more common to the

real world; therefore, only node attacks are considered in this research. The more detailed about problem assumptions are given in Table 3- 1 and descriptions are in Table 3- 2.

Table 3- 1 Problem Assumptions of the AEA

<p>Problem Assumptions:</p> <ol style="list-style-type: none"> 1. The attacker and the defender have complete information about the target network topology. 2. The attacker could have some experiences before compromised the first node. 3. The attacker gains and accumulates experiences from a compromised node to further reduce the cost of a future attack. 4. That the effect of accumulated experiences from compromised nodes which is represented by the discounted factor is a given parameter. 5. The attacker only chooses a single path without groping around or trace back. 6. The defender's budgets allocation strategy is a given parameter. 7. Only node attacks are considered. 8. Only malicious attacks are considered.
--

Table 3- 2 Problem Descriptions of the AEA

<p>Given:</p> <ol style="list-style-type: none"> 1. The network topology and network size 2. The defender's budget allocation policy 3. The discounted factor of accumulated experiences from compromised nodes 4. That the minimal attack cost to compromise a node is a given function of the budget allocation <p>Objective:</p> <ol style="list-style-type: none"> 1. To minimize the total attack cost <p>Subject to:</p> <ol style="list-style-type: none"> 1. The node to be attacker must be a single path and compromise the core node <p>To determine:</p> <ol style="list-style-type: none"> 1. which path will be attacked

3.1.2 Notation and Formulation

The attacker behavior with mathematical programming problem is modeled as following. The given parameters and decision variables are defined as Table 3- 3 and Table 3- 4.

Table 3- 3 Given Parameters of the Proposed Model

Given parameters	
Notation	Description
V	The index set of all original nodes
L_1	The index set of all original links
L_2	The index set of all original nodes , which are artificial links
L_3	The index set of all artificial links connect to artificial origin or destination
W	The index set of all given critical Origin-Destination pairs (s, n) , where s is the source node, and n is the core node
$p_{(k)}$	The index set of 1-st node to k -th node on path p , where $p_{(k)} \in V$
M	A large number that represents the link disconnection
ε	A small number that represents the link connectedness
d_i	The discounted factor between $[0, 1]$ that represents the effect of accumulated experiences at the compromised node i without paying an extra fee, where $i \in V$
P_w	The index set of all candidate paths of the O-D pair w , where $w \in W$
δ_{pl}	An indicator function, which is 1 if link l is on path p , and 0 otherwise, where $l \in L_1 \cup L_2 \cup L_3, \forall p \in P_w$
b_i	The budget of defense resources that allocated to node i , where $i \in V$
\hat{a}_i	Threshold of an attack cost leading to a successful attack, which is a monotone increasing function of b_i

Table 3- 4 Decision Variables of the Proposed Model

Decision Variables	
Notation	Description
y_l	1 if link l is compromised, and 0 otherwise, where $l \in L_1 \cup L_2 \cup L_3$
t_{wl}	1 if link l is used by the O-D pair w , and 0 otherwise, where $l \in L_1 \cup L_2 \cup L_3$, $w \in W$
c_l	Cost of link l , where $l \in L_1 \cup L_2 \cup L_3$
x_p	1 if path p is chosen, and 0 otherwise, where $\forall p \in P_w$

The proposed model is as follows.

Objective function:

$$\min_{y_l} \sum_{p \in P_w} \left(\sum_{i \in V'} \hat{a}_i \prod_{i \in p(k-1)} d_i \right) x_p \quad (\text{IP 1})$$

subject to

$$c_l = y_l M + \varepsilon \quad l \in L_2 \quad (\text{IP 1.1})$$

$$\sum_{l \in L_1 \cup L_2 \cup L_3} t_{wl} c_l \leq \sum_{l \in L_1 \cup L_2 \cup L_3} \delta_{pl} c_l \quad \forall p \in P_w, w \in W \quad (\text{IP 1.2})$$

$$\sum_{p \in P_w} x_p \delta_{pl} = t_{wl} \quad \forall w \in W, l \in L_1 \cup L_2 \cup L_3 \quad (\text{IP 1.3})$$

$$\sum_{p \in P_w} x_p \delta_{pl} \leq y_l \quad \forall w \in W, l \in L_1 \cup L_2 \cup L_3 \quad (\text{IP 1.4})$$

$$\sum_{p \in P_w} x_p = 1 \quad (\text{IP 1.5})$$

$$x_p = 0 \text{ or } 1 \quad \forall p \in P_w \quad (\text{IP 1.6})$$

$$y_l = 0 \text{ or } 1 \quad l \in L_1 \cup L_2 \cup L_3 \quad (\text{IP 1.7})$$

$$t_{wl} = 0 \text{ or } 1 \quad \forall w \in W, l \in L_1 \cup L_2 \cup L_3. \quad (\text{IP 1.8})$$

Explanation of the mathematical formulation:

- ✓ **Objective function:** To minimize the total attack cost; the attacker minimizes the objective value by deciding which path will be attacked.
- ✓ **Constraint (IP 1.1)** describes the definition of the link cost, which 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 O-D pair, w , should be the minimum cost path.
- ✓ **Constraint (IP 1.3)** is the relations among t_{wl} , x_p and δ_{pl} . The auxiliary set of decision variables, t_{wl} , was used 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 compromised link is equal to the total chosen path p .
- ✓ **Constraint (IP 1.5) and (IP 1.6)** jointly require that exactly one path is selected between each given O-D pair.
- ✓ **Constraint (IP 1.7)** determines whether each link l is compromised, or not.
- ✓ **Constraint (IP 1.8)** determines whether each link l is used to from a shortest cost path by O-D pair, w , or not.

3.2 Problem Formulation of AAEA

3.2.1 Problem Assumptions

In AAEA, the attacker not only gains some free experiences from a compromised node but could spend extra expenses, probing fee, learning some valuable information, such diverse user's right or a network topology graph. Meanwhile, the probing fee are various among different degrees of the probing. The more you probe, the more cost you should pay. The attacker behavior with mathematical programming problem is modeled. The given parameters and decision variables are defined as Table 3- 5 and Table 3- 6.

Table 3- 5 Problem Assumptions of the AAEA

Problem Assumptions:

1. The attacker and the defender have complete information about the target network topology.
2. The attacker could have some experiences before compromised the first node.
3. The attacker gains and accumulates experiences from a compromised node to further reduce the cost a future attack.
4. That the effect of the accumulated experiences from probing the compromised nodes which is represented by the level of discounted factor is a given parameter.
5. The cost represents the extra fee that the attacker probes from level 1 to level j from node i is a given parameter.
6. The attacker only chooses a single path without groping around or trace back.
7. The defender's budgets allocation strategy is a given parameter.
8. Only node attacks are considered.
9. Only malicious attacks are considered.

Table 3- 6 Problem Descriptions of the AAEA

<p>Given:</p> <ol style="list-style-type: none"> 1. The network topology and network size 2. The defender’s budget allocation policy 3. The level of discounted factor of accumulated experiences at compromised nodes 4. The extra fee of the attacker probes from compromised nodes 5. That the minimal attack cost to compromise a node is a given function of the budget allocation <p>Objective:</p> <ol style="list-style-type: none"> 1. To minimize the total attack cost <p>Subject to:</p> <ol style="list-style-type: none"> 1. The node to be attacker must be a single path and compromise the core node <p>To determine:</p> <ol style="list-style-type: none"> 1. which path will be attacked
--

3.2.2 Notation

The more detailed about problem assumptions are given in Table 3- 7 and descriptions are in Table 3- 8.

Table 3- 7 Given Parameters of the Proposed AAEA

Given parameters	
Notation	Description
V	The index set of all original nodes
S_i	The index set of all levels at each node i
L_1	The index set of all original links
L_2	The index set of all original nodes , which are artificial links
L_3	The index set of all artificial links connect to artificial origin or destination
L_4	The index set of all levels at each node i , which are artificial links
W	The index set of all given critical Origin-Destination pairs (s, n) , where s is the

	source node, and n is the core node
$p_{(k)}$	The index set of 1-st node to k -th node on path p , where $p_{(k)} \in V$
M	A large number that represents the link disconnection
ε	A small number that represents the link connectedness
d_{ij}	The level of discounted factor between $[0, 1]$ that represents the effect of accumulated experiences from level 1 to level j at the compromised node i , where $i \in V, j \in S_i$
m_{ij}	The cost represents the extra fee that the attacker probes from level 1 to level j at node i , where $i \in V, j \in S_i$
P_w	The index set of all candidate paths of the O-D pair w , where $w \in W$
δ_{pl}	An indicator function, which is 1 if link l is on path p , and 0 otherwise, where $l \in L_1 \cup L_2 \cup L_3 \cup L_4, p \in P_w$
b_i	The budget of defense resources that allocated to node i , where $i \in V$
\hat{a}_i	Threshold of an attack cost leading to a successful attack, which is a monotone increasing function of b_i

Table 3- 8 Decision Variables of the Proposed AAEA

Decision Variables	
Notation	Description
y_l	1 if link l is compromised, and 0 otherwise, where $l \in L_1 \cup L_2 \cup L_3 \cup L_4$
t_{wl}	1 if link l is used by the O-D pair w , and 0 otherwise, where $l \in L_1 \cup L_2 \cup L_3 \cup L_4, w \in W$
c_l	Cost of link l , where $l \in L_1 \cup L_2 \cup L_3 \cup L_4$
x_p	1 if path p is chosen, and 0 otherwise, where $\forall p \in P_w$
r_{ij}	1 if level 1 to level j from node i is probed and 0 otherwise, where $i \in V, j \in S_i$

AAEA is proposed as following.

Objective function:

$$\min_{y_l} \sum_{p \in P_w} \left(\sum_{i \in V, j \in S_i} (\hat{a}_i + m_{ij} r_{ij}) \prod_{i \in p_{(k-1)}} \sum_{j \in S_i} d_{ij} r_{ij} \right) x_p \quad (\text{IP 2})$$

subject to

$$c_l = y_l M + \varepsilon \quad l \in L_2 \quad (\text{IP 2.1})$$

$$\sum_{l \in L_1 \cup L_2 \cup L_3 \cup L_4} t_{wl} c_l \leq \sum_{l \in L_1 \cup L_2 \cup L_3 \cup L_4} \delta_{pl} c_l \quad \forall p \in P_w, w \in W \quad (\text{IP 2.2})$$

$$\sum_{p \in P_w} x_p \delta_{pl} = t_{wl} \quad \forall w \in W, l \in L_1 \cup L_2 \cup L_3 \cup L_4 \quad (\text{IP 2.3})$$

$$\sum_{p \in P_w} x_p \delta_{pl} \leq y_l \quad \forall w \in W, l \in L_1 \cup L_2 \cup L_3 \cup L_4 \quad (\text{IP 2.4})$$

$$\sum_{p \in P_w} x_p = 1 \quad (\text{IP 2.5})$$

$$\sum_{j \in S_i} r_{ij} \leq 1 \quad i \in V \quad (\text{IP 2.6})$$

$$x_p = 0 \text{ or } 1 \quad \forall p \in P_w \quad (\text{IP 2.7})$$

$$y_l = 0 \text{ or } 1 \quad l \in L_1 \cup L_2 \cup L_3 \cup L_4 \quad (\text{IP 2.8})$$

$$t_{wl} = 0 \text{ or } 1 \quad \forall w \in W, l \in L_1 \cup L_2 \cup L_3 \cup L_4 \quad (\text{IP 2.9})$$

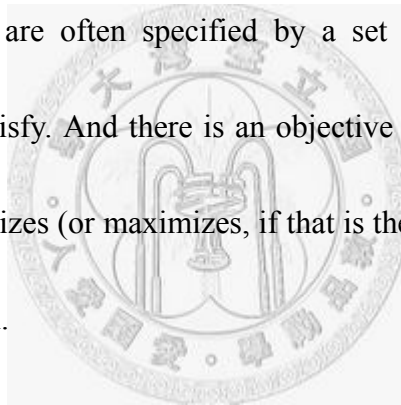
$$r_{ij} = 0 \text{ or } 1 \quad i \in V, j \in S_i \quad (\text{IP 2.10})$$

Explanation of the mathematical formulation:

- ✓ **Objective function:** To minimize the total attack cost; the attacker minimizes the objective value by deciding which path will be attacked.
- ✓ **Constraint (IP 2.6)** requires that if the level of the discounted factor is chosen or not.

Chapter 4 Solution Approach

In a networking or telecommunications mindset, many real-world and theoretical problems could be effectively solved by algorithms or more preferment algorithms in practice. Furthermore, these problems could be modeled in this general framework. Generally, these problems are often specified by a set of constraints, equalities or inequalities that have to satisfy. And there is an objective function, or cost function. A feasible solution that minimizes (or maximizes, if that is the goal) the objective function is called an optimal solution.



The efforts to develop solution algorithms for optimization problems can be classified broadly into two categories, rigorous and heuristic approaches [22]. The former are algorithms that proposed for solving optimal problems, for examples, Linear Programming, Integer Programming, Nonlinear Programming, Combinatorial Optimization, Dynamic Programming, Convex Programming, and Stochastic Programming. The latter one is concerned with an algorithm that gives up one or both of these goals; for example, it usually finds pretty good solutions, the near optimal one.

The remainder of this chapter is organized as follows. In 4.1, a more detail of generalized shortest path algorithm is presented. In 4.2 and 4.3, AEA and AAEA are solved by Generalized-Reverse-Dijkstra algorithm [24].

4.1 Generalized Shortest Path Problem

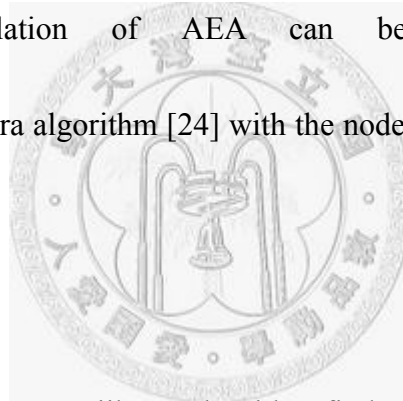
Among these, the shortest path problem is one of the most important issues among network problems. In the traditional setting the link weight is static and set to one. In generalized vision the discount of a link depends on its history on a path. Thus, a shortest path problem with cost and discount factor functions for the links of a graph, the problem is known as a generalized shortest path problem [23]. The discount factor might be additive or multiplicative on a path [24]. In this research, the weight is multiplicative to present the discount effect of the accumulated experiences.

The generalized shortest path problem is a special case of the shortest path problem. Hence the generalized shortest path problem can be solved in polynomial time using general LP algorithms with Generalized-Reverse-Dijkstra algorithm [24]. More precisely, in this problem each link has a weight which might discount the further cost of the path in a multiplicative fashion.

4.2 Solution Approach to AEA

In chapter 2, AEA is transformed into a shortest path problem by neglecting the progressive discount effects and node splitting techniques. Here, Lemma 1 is presented that AEA is optimally solved by Generalized-Reverse-Dijkstra algorithm [24] without ignoring the accumulated experiences of attacker is applied.

Lemma 1 Given a budget allocation strategy, a topology, $G = (V, L)$, and critical O-D pairs, W , the formulation of AEA can be optimally solved by Generalized-Reverse-Dijkstra algorithm [24] with the node splitting method [11] within time complexity $O(|V|^2)$.



Proof. The Generalized-Reverse-Dijkstra algorithm finds the shortest path that finds a shortest path with minimal cost. With the node splitting method, on the other hand, a node can be converted into a link by dividing it into two independent sub-nodes and introducing an artificial link to connect the sub-nodes. By assuming that the link capacity between two sub-nodes of a node is inherited the attributes of the original node (i.e., the attack cost and discount factor) of the node and other links' attributes are discount factor is 1 and attack cost is 0, then transform $G(V, L)$ into $G'(V', L')$. Using the Generalized-Reverse-Dijkstra algorithm can find a shortest path in G' .

4.3 Solution Approach to AAEA

In AAEA, different probing fee and the corresponding discount factor are taken as the attack cost and the corresponding discount factor in AEA. In chapter 2, by node splitting, AAEA is also transformed into AEA, which is a generalized shortest path problem. Here, Lemma 2 is presented AAEA is solved by Generalized-Reverse-Dijkstra algorithm.

Lemma 2 Given a budget allocation strategy, a topology, $G = (V, L)$, all level of each node i , S_i , and critical O-D pairs, W , the formulation of AAEA can be transformed into AEA and be optimally solved by Generalized-Reverse-Dijkstra algorithm [24] with the node splitting method [11] within time complexity $O(|V^2 \cup L_4|)$.

proof. A node j is converted into two sub-nodes j' and j'' . With the node splitting method again, all levels of a node can be converted into artificial nodes which are connected to node c' and node c'' . The link from node c' to the artificial nodes are inherited the attributes of the levels (i.e., discount factor and money) and link from node j' to node c' with discount factor is 1 and the original attack cost. The other links' attributes are discount factor is 1 and attack cost is 0. AAEA is transform into AEA.

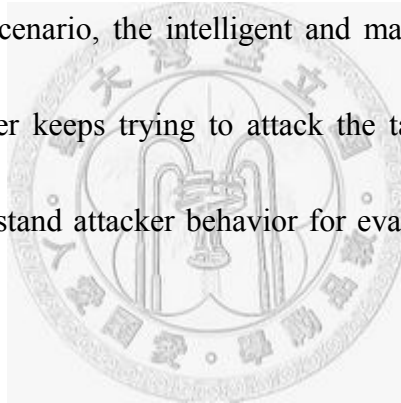
Thus AAEA can be optimally solved by Generalized-Reverse-Dijkstra algorithm.

Chapter 5 Conclusion and Future Work

This chapter briefly outlines conclusion and future work of this research.

5.1 Conclusion

In an attack-defense scenario, the intelligent and malicious attacks emerge in an endless stream. The attacker keeps trying to attack the target network by all means. Thus, it is helpful to understand attacker behavior for evaluating the robustness of the network.



In this research, two issues have focused on. First, the robustness of a network and evaluated the minimal attack cost of an attacker based on two different mathematical models of the Accumulated Experiences of Attackers (AEA), and the Advanced Accumulated Experiences of Attackers (AAEA) are discussed. In these models, the intelligent attackers choose a node as the starting node of the target network, and find a minimal attack cost path. These problems could be modeled as a mixed integer programming problem.

Second, by graph modeling and node splitting technique, AEA and AAEA are successfully transformed into a revised shortest path problem, a generalized shortest path problem, which algorithm shows a pseudo-polynomial time in solving the proposed model

The contribution of this research is that a special insight into attack patterns about the attacker experiences has derived, which would be useful in modeling and evaluating the robustness of a network. Another more obvious contribution is the development of the mathematical models with AEA and AAEA. An elegant mathematical technique, graph modeling and node splitting has been performed to effectively turn the dynamic context of the attacker of the real networks into a well-formulated mathematical model, and been optimally solved by Generalized-Dijkstra algorithm.

5.2 Future Work

In recent years, there has been an increasing interest in the study of networks of attack-defense scenario. AEA and AAEA, however, is still can further research in many aspects, which are summarized in the following paragraphs.

- **One Critical O-D pair**

As Figure 5- 1 shows, initially, the network has one critical Original-Destination pair (O-D pair). For example, this critical O-D pair could be the Office of the President to the Ministry of National Defense, which could be the most important connection in the government network. The more details are shown in Table 5- 1 and (IP3).The objective of the attackers is to enter this network via choosing a starting node and disconnecting the O-D pair with minimal attack cost path composed by a serial of compromised nodes.



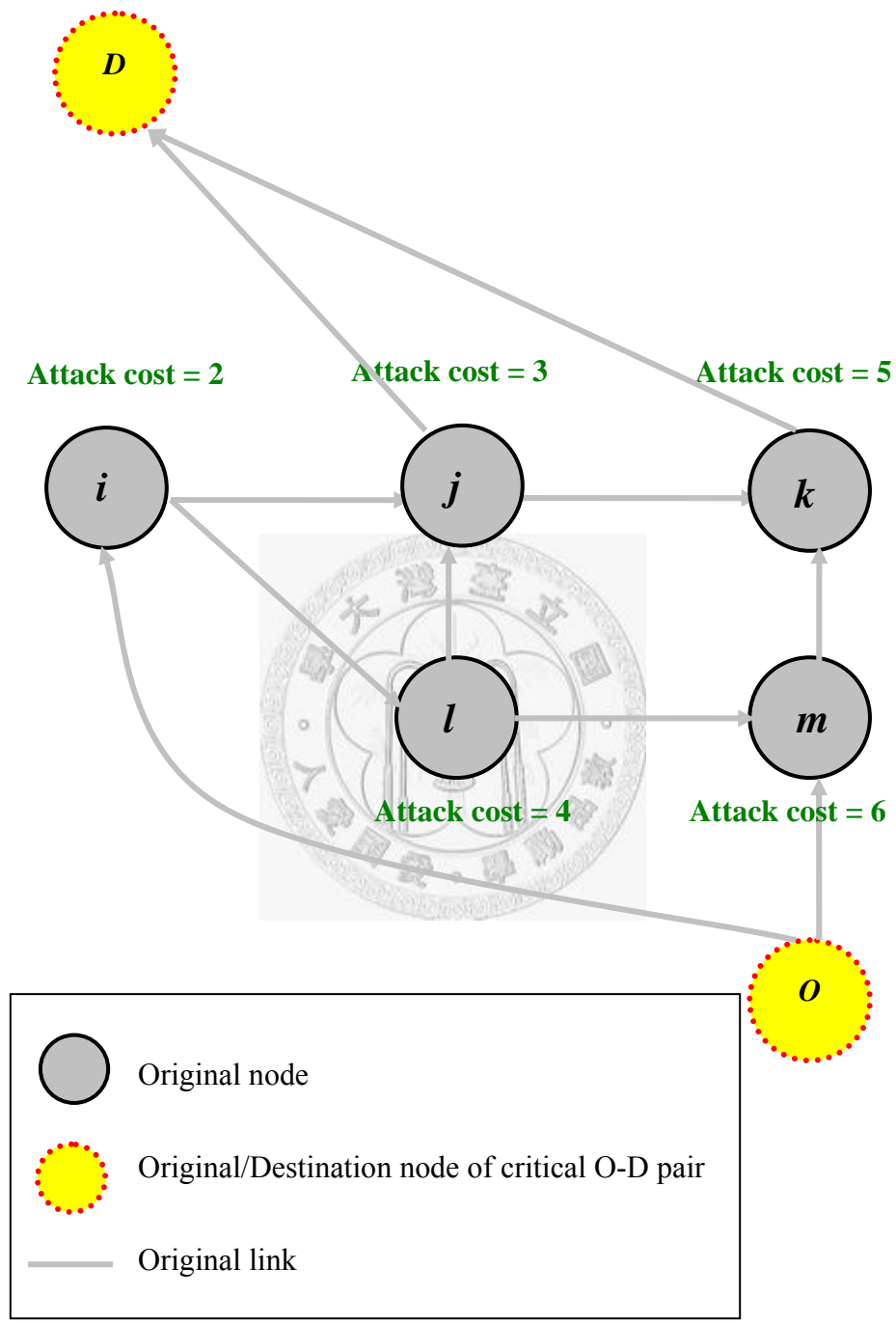


Figure 5- 1 An Attack Scenario

Table 5- 1 Given Parameters of the Proposed Model

Given parameters	
Notation	Description
W	The index set of all given critical Origin-Destination pairs, where only has one critical O-D pair, w , in it

The proposed model is as follows.

Objective function:

$$\min_{y_l} \sum_{p \in P_w} \left(\sum_{i \in V} \hat{a}_i \prod_{i \in P_{(k-1)}} d_i \right) x_p \quad (\text{IP 3})$$

subject to

$$c_l = y_l M + \varepsilon \quad l \in L_1 \cup L_2 \cup L_3 \quad (\text{IP 3.1})$$

$$\sum_{l \in L_1 \cup L_2 \cup L_3} t_{wl} c_l \leq \sum_{l \in L_1 \cup L_2 \cup L_3} \delta_{pl} c_l \quad \forall p \in P_w, w \in W \quad (\text{IP 3.2})$$

$$\sum_{p \in P_w} x_p \delta_{pl} = t_{wl} \quad \forall w \in W, l \in L_1 \cup L_2 \cup L_3 \quad (\text{IP 3.3})$$

$$M \leq \sum_{l \in L_1 \cup L_2 \cup L_3} \sum_{w \in W} t_{wl} c_l \quad (\text{IP 3.4})$$

$$\sum_{p \in P_w} x_p \delta_{pl} \leq y_l \quad \forall w \in W, l \in L_1 \cup L_2 \cup L_3 \quad (\text{IP 3.5})$$

$$\sum_{p \in P_w} x_p = 1 \quad (\text{IP 3.6})$$

$$x_p = 0 \text{ or } 1 \quad \forall p \in P_w \quad (\text{IP 3.7})$$

$$y_l = 0 \text{ or } 1 \quad l \in L_1 \cup L_2 \cup L_3 \quad (\text{IP 3.8})$$

$$t_{wl} = 0 \text{ or } 1 \quad \forall w \in W, l \in L_1 \cup L_2 \cup L_3. \quad (\text{IP 3.9})$$

Explanation of the mathematical formulation:

- ✓ **Objective function:** To minimize the total attack cost; the attacker minimizes the objective value by deciding which path will be attacked.
- ✓ **Constraint (IP 3.4)** requires that at least one critical O-D pair is disconnected. The

phenomenon by showing that the sum of the shortest path costs for each O-D pair to communicate is greater than M is depicted.

- **Interaction between Attackers and Defenders**

Another issue to be addressed in the future would be the behavior of the defender against the accumulated experiences of the attackers. While attackers do their best to compromise a node; thus, defenders must change their strategies to protect the node against compromise by the constantly evolving strategies of attackers. As can be noticed in Figure 5-1, the attacker spend fee gaining some experiences which might cause discount in the further attack; meanwhile, the defender reallocate the defense power for putting more resources on the attack path with counter discount factor. By these two factors, the behavior in the attack-defense scenario would be well-modeled.

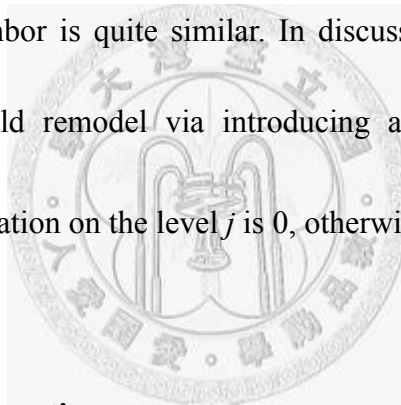
- **Multi Core Nodes**

In this thesis, the attacker only chooses one core node to attack. But in a more common attack-defense scenario, the attacker sometimes chooses several core nodes to attack. Because of the multi core nodes, the attack path extends to a tree but a single path.

- **Information issues**

- ◆ **Duplicated Information**

Recall that, this research assumed that the attacker is such well-skilled that would not pay any useless fee. For this assumption, we tried to avoid any possibility of buying duplicated information from the attackers' point of view. The more reality networking scenario, for example, the routing table of a node in the neighbor is quite similar. In discussing the result, by modeling technique, it could remodel via introducing a parameter, θ_{rj} , where the duplicated information on the level j is 0, otherwise 1.



- ◆ **Aggregated Information**

Compared with duplicated information, there still some significant information was separated into several nodes. A most skilled attacker could collect this aggregated information and piece up into completed information to further reduce the attack cost.

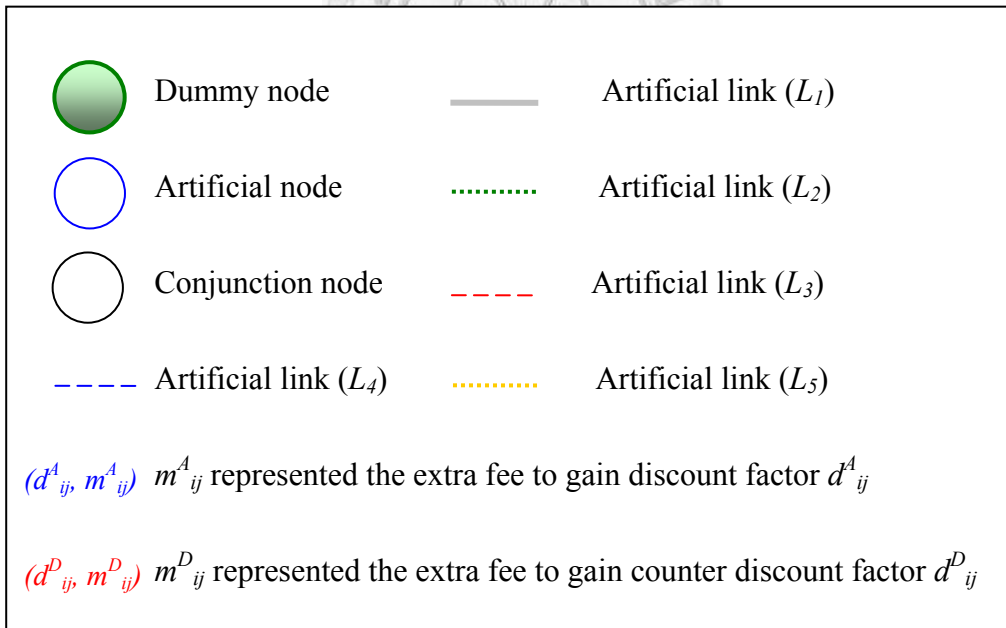
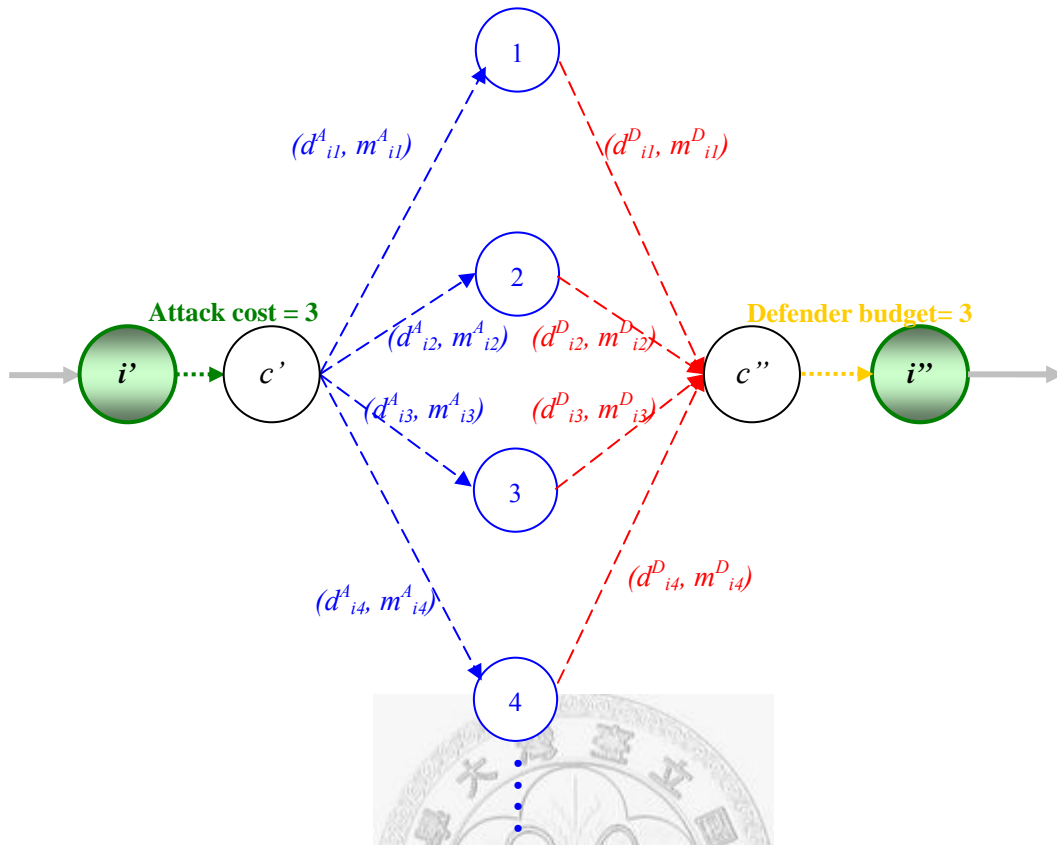


Figure 5- 2 Interactions between Attackers and Defenders

Reference

- [1] S. P. Gorman, L. Schintler, R. Kulkarni, and R. Stough, “The Revenge of Distance: Vulnerability Analysis of Critical Information Infrastructure”, *Journal of Contingencies and Crisis Management*, Volume 12, Number 2, pp. 48-63, June 2004.
- [2] B. Blakley, “The Emperor’s Old Armor”, *Proceedings of the 1996 New Security Paradigms Workshop*, Lake Arrowhead, California, September 17-20, 1996, Association for Computing Machinery, 1997.
- [3] H. F. Lipson and D. A. Fisher, “Survivability – A New Technical and Business Perspective on Security”, *Proceedings of the 1999 ACM Workshop on New Security Paradigms*, pp. 33-39, September 1999.
- [4] R. J. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, T. A. Longstaff, and N. R. Mead, “Survivable Network Systems: An Emerging Discipline”, *Technical Report CMU/SEI-97-TR-013*, Software Engineering Institute, Carnegie Mellon University, November 1997 (Revised: May 1999).
- [5] J. C. Knight, K. J. Sullivan, M. C. Elder, and C. Wang, “Survivability Architectures: Issues and Approaches”, *Proceedings of the DARPA Information Survivability Conference and Exposition*, Volume 2, pp.157-171, January 2000.

- [6] J. C. Knight and K. J. Sullivan, "On the Definition of Survivability", Technical Report CS-TR-33-00, Department of Computer Science, University of Virginia, December 2000.
- [7] J. C. Knight, E. A. Strunk, and K. J. Sullivan, "Towards a Rigorous Definition of Information System Survivability", Proceedings of the DARPA Information Survivability Conference and Exposition, Volume 1, pp.78-89, April 2003.
- [8] Y. Liu and K. S. Trivedi, "A General Framework for Network Survivability Quantification", Proceedings of the 12th GI/ITG Conference on Measuring, Modeling and Evaluation of Computer and Communication Systems, September 2004.
- [9] Y. Liu, V.B. Mendiratta, and K.S. Trivedi, "Survivability Analysis of Telephone Access Network", Proceedings of the 15th IEEE International Symposium for Software Reliability Engineering, pp.367-378, November 2004.
- [10] Report spells out global attack patterns: More zero-days and phishing, but less critical flaws Computer Fraud & Security, Volume 2007, Number 4, pp. 3-4, April 2007.
- [11] http://www.windowsnetworking.com/articles_tutorials/Trust-Relationships-Windows-Server-2003-Environment.html
- [12] <http://technet.microsoft.com/en-us/windowsserver/default.aspx>

- [13] E.Jonsson and T. Olovsson, “A Quantitative Model of the Security Intrusion Process Based on Attacker Behavior”, IEEE Transactions of Software Engineering, Volume 23, Number 4, pp. 235-245, April 1997.
- [14] R. Ortalo, Y. Deswarte, and M. Ka[^]aniche, “Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security”, IEEE Transactions on Software Engineering, Volume 25, Number 5, pp. 633-650, September 1999.
- [15] J. McDermott, “Attack-Potential-Based Survivability Modeling for High-Consequence Systems ” , Proceedings of the 3rd IEEE International Workshop on Information Assurance, pp. 119-130, March 2005.
- [16] C.H. Chen, Y.L. Lin, F.Y.S. Lin, P.H. Tsang, C.L. Tseng and H.H. Yen, “Evaluation of Network Robustness for Given Defense Resource Allocation Strategies, Proceedings of IEEE ARES’06, 2006
- [17] G. B. Dantzig, R. Fulkerson, and S. M. Johnson, “Solution of a Large-scale Traveling Salesman Problem”, Operations Research 2, pp.393-410, 1954.
- [18] E. L. Lawler and Jan Karel Lenstra and A. H. G. Rinnooy Khan and D. B. Shmoys, “The Traveling Salesman Problem: A Guided Tour of Combinatorial Optimization”, John Wiley & Sons, Inc. ISBN 0-471-90413-9, 1985.
- [19] G. Gutin and A. P. Punnen, “The Traveling Salesman Problem and Its Variations”, Springer, ISBN 0-387-44459-9, 2006.

- [20] M. R. Garey and D. S. Johnson, “Computers and Intractability: A Guide to the Theory of NP-Completeness”, W.H. Freeman, ISBN 0-7167-1045-5, 1979.
- [21] Charles E. Noon. and James C. Bean, “A Lagrangian Based Approach for the Asymmetric Generalized Traveling Salesman Problem”, Operations Research, Volume 39, Number 4, pp. 623-632, 1991.
- [22] J. Choi, M. J. Realff_ and J. H. Lee, “An Algorithmic Framework for Improving Heuristic Solutions Part I: A Deterministic Discount Coupon Traveling Salesman Problem”, Computers & Chemical Engineering, Volume 28, Number 8, pp. 1285-1296, 2004.
- [23] R.K. Ahuja, T.L. Magnagi and J.B. Orlin, “Network Flows”, Prentice Hall, Englewood Cliffs, ISBN 978-0136175490, 1993.
- [24] V. Batagelj, F.J. Brandenburg, P.O.D. Mendez, and A. Sen, “The Generalized Shortest Path Problem”, The Pennsylvania State University CiteSeer Archives, July 2000.

簡歷

姓名：陳怡孜

出生地：台灣 高雄市

生日：中華民國七十三年二月十一日

學歷：九十一年九月至九十五年一月

國立暨南國際大學資訊管理學系學士

九十五年二月至九十六年七月

台灣大學資訊管理研究所碩士