Maximization of Network Survivability Considering Degree of Disconnectivity

Frank Yeong-Sung Lin[1], Hong-Hsu Yen[2], and Pei-Yu Chen[1,3,4,*]

[1] Department of Information Management, National Taiwan University
yslin@im.ntu.edu.tw
[2] Department of Information Management, Shih Hsin University
hhyen@cc.shu.edu.tw
[3] Information and Communication Security Technology Center
Taipei, Taiwan, R.O.C.
d96006@im.ntu.edu.tw
[4] Institute Information Industry Taipei, Taiwan, R.O.C.

Abstract. The issues of survivability of networks, especially to some open year round services have increased rapidly over the last few years. To address this topic, the effective survivability metric is mandatory for managerial responsibility. In this paper, we provide a survivability mechanism called Degree of Disconnectivity (DOD) for the network operator to detect risks. To evaluate and analyze the robustness of a network for network operators, this problem is modeled as a mathematical programming problem. An attacker applies his limited attack power intelligently to the targeted network. The objective of the attacker is to compromise nodes, which means to disable the connections of O-D pairs, to achieve the goal of reaching a given level of the proposed Degree of Disconnectivity metric. A Lagrangean Relaxation-based algorithm is adopted to solve the proposed problem.

Keywords: Information System Survivability, Degree of Disconnectivity, Lagrangean Relaxation, Mathematical Programming, Network Attack, Optimization Problem, Resource Allocation.

1 Introduction

With customers' expectations of open year round service, the complete shutdown of an attacked system is not an acceptable option anymore. Nonetheless, over the past decade, malicious and intentional attacks have undergone enormous growth. With the number of attacks on systems increasing, it is highly probable that sooner or later an intrusion into those systems will be successful. As several forms of attacks are aimed at achieving pinpointed destruction to systems, like DDoS, the relatively new paradigms of survivability are becoming crucial. Compared with other metrics, like reliability and average availability, that measure a network, survivability is a network's ability to perform its designated set of functions under all potentially damaging events, such as failure in a network infrastructure component [1].

* Correspondence should be sent to d96006@im.ntu.edu.tw.

B. Murgante et al. (Eds.): ICCSA 2011, Part I, LNCS 6782, pp. 667–676, 2011.

Survivability focuses on preserving essential services in unbounded environments, even when systems in such environments are penetrated and compromised.

A number of papers have studied various theoretical aspects of survivability against antagonistic attacks. In [2], due to the diversified definitions of network survivability, the author categorized the methods to evaluate network survivability into three subcategories: connectivity, performance, and function of other quality or cost measures. The least twenty recognized quality models indicate that the survivability is that users could receive the services that they need without interruption and in a timely manner.

When evaluating survivability, the connectivity of a network to achieve a service level agreement is another vital issue. The definition of network connectivity is the minimum number of links or nodes that must be removed to disconnect an O-D (Original and Destination) pair [3]. In general, the more numbers of links or nodes that must be removed to disconnect an O-D pair, the higher the survivability of the network will be. Thus, there are many researches adopting the network connectivity with the quantitative analysis of network survivability. In [4], the author proposed using the network connectivity to measure the network survivability under intentional attacks and random disasters. In addition, in [5], the author also adopted the network connectivity to do the quantitative analysis of network survivability and the survivability metric is called the Degree of Disconnectivity (DOD).

Many network scenarios have traditionally assumed that the defender, i.e. network operator, only confront a fixed and immutable threat. However, the September 11 attacks in 2001 demonstrated that major threats today involve strategic attackers that can launch a serial action of malicious and intentional attacks, and choose the strategy that maximizes their objective function. The attacker utilizes his knowledge about the target network to formulate his attacking strategy order to inflict maximum damage on a system, a network, or a service under malicious and intentional attacks. Consequently, it is critical for the defender to take into consideration the attacker's strategy when it decides how to allocate its resource among several defensive measures [6].

However, the conflict interaction between the attacker and the defender suggests a need to assume that both of them are fully strategic optimizing agents with their different objectives. A number of papers have studied various theoretical aspects of protecting potential targets against attacks. Some of these papers discuss the scenarios and solved the problem with game theory. Here, in this paper, a conflict network attack-defense scenario is described as a mathematical model to optimize the resource allocation strategies for network operators and is expressed for both attackers and defenders considering the DOD [5].

2 Problem Formulation and Notations

The network scenario discussed in this paper can be seen as a game with attackers and defender entities: attackers represent intelligent or rational entities of the network that may choose a computer and corrupt its database and systems, such as hackers. The defender represents the distributed database administrator, whose goal is to maintain the integrity of the data. Once the database is compromised, the DOD is affected, which is defined as (1). Based on [5], the proposed survivability metric called degree

of disconnectivity (DOD) is defined as S, which assesses the average damage level of a network; it can also be called the degree of segmentation, degree of segregation, or degree of separation.

The DOD metric in this paper is defined as S, which is evaluated on the disconnected numbers of O-D pairs among all O-D pairs. DOD can be generated as the residual index of the networks. In this case, t_{wi} is 1, while node i on an O-D pair w is dysfunctional. The Original node here is source node, and the destination node is the database. The transmission cost of dysfunctional node is M, otherwise it is ε. The greater the value of S, the more the network is damaged.

$$S = \frac{\sum_{w \in W} \sum_{i \in V} t_{wi} c_i}{C_2^N \times M} . \tag{1}$$

Because the attacker's resources, i.e. time, money, and man power, are limited, only part of a network can be compromised. Therefore, the resources must be fully utilized so that the attacker can cause the maximum harm to the target network. In order to discuss the worst case scenario, the concept of [6], which assumes complete information and perfect perception on behalf of both attackers and defenders, is adopted. Hence, both the attacker and the defender have complete information about the targeted network topology and the budget allocation is assumed. The serial of attack actions considering the survivability of a network is then modeled as an optimization problem, in which the objective is to minimize the total attack cost from an attacker's perspective, such that the given critical O-D pair is disconnected and the survivability is over the given threshold resulting in the inability of the network to survive. Note that the network discussed here is at the AS level.

The above problem is formulated as a mathematical model as follows. For simplicity, since the targeted network is at the AS level, the attacker cannot simply attack any node directly. The notations used in this paper and problem formulation is defined in Table 1.

Table 1. Given Parameters and Decision Variables

Given parameter Notation	Description
V	Index set of nodes
W	Index set of OD pairs
P_w	Set of all candidate paths of an OD pair w, where $w \in W$
M	Large amount of processing cost that indicates a node has been compromised
ε	Small amount of cost processing cost that indicates a node is functional
δ_{pi}	Indicator function, 1 if node i is on path p, 0 otherwise, where $i \in V$ and $p \in P_w$
$\hat{a}_i$	The threshold of attack cost leading to a successful node attack
S	The threshold of a network crash, which is the average damage level of all O-D pairs
R_w	The weight of O-D pair w, where $w \in W$
$\hat{a}_i$	The threshold of attack cost leading to a successful node attack

Table 1. *(continued)*

Decision variable Notation	Description
x_p	1 if path p is chosen, 0 otherwise, where $p \in P_w$
y_i	1 if node i is compromised by attacker, 0 otherwise (where $i \in V$)
t_{wi}	1 if node i is used by OD pair w, 0 otherwise, where $i \in V$ and $w \in W$
c_i	Processing cost of node i, which is ε if i is functional, M if i is compromised by attacker, where $i \in V$

The problem is then formulated as the following minimization problem:

$$\min_{y_i} \sum_{i \in V} y_i \hat{a}_i \ , \qquad \text{(IP 1)}$$

Subject to:

$$c_i = y_i M + (1 - y_i)\varepsilon \qquad \forall i \in V \qquad \text{(IP 1.1)}$$

$$\sum_{i \in V} t_{wi} c_i \le \sum_{i \in V} \delta_{pi} c_i \qquad \forall\, p \in P_w,\ w \in W \qquad \text{(IP 1.2)}$$

$$\sum_{p \in P_w} x_p \delta_{pi} = t_{wi} \qquad \forall i \in V,\ w \in W \qquad \text{(IP 1.3)}$$

$$S \le \frac{\sum_{w \in W} R_w \sum_{i \in V} t_{wi} c_i}{|W| \times M} \qquad \text{(IP 1.4)}$$

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

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

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

$$t_{wi} = 0 \text{ or } 1 \qquad \forall\ i \in V,\ w \in W. \qquad \text{(IP 1.8)}$$

The objective of the formulation is to minimize the total attack cost by of the attacker by deciding which node to compromise. Constraint (IP 1.1) describes the definition of the transmission cost of node i, which is ε if node i is functional, and M if node i is compromised. Constraint (IP 1.2) requires that the selected path for an O-D pair w should be the minimal cost path. Constraint (IP 1.3) denotes the relationship between t_{wi} and $x_p\delta_{pi}$. To simplify the problem-solving procedure, the auxiliary set of decision variables t_{wi} is replaced by the sum of all $x_p\delta_{pi}$. (IP 1.1) to (IP 1.3) jointly require that, when a node is chosen for attack, there must be exactly one path from the attacker's initial position, s, to that node, and each node on the path must have been compromised. These constraints are jointly described as the continuity constraints. And constraint (IP 1.4) determines that if a target network has been compromised, the DOD metrics must be larger than the given threshold. Constraints (IP 1.5) and (IP 1.6) jointly entail that only one of the candidate paths of an OD pair w can be selected. Lastly, constraints (IP 1.6) to (IP 1.8) impose binary restrictions on decision variables.

3 Solution Approach

3.1 Solution Approach for Solving the Problem of (IP 1)

3.1.1 Lagrangean Relaxation

Lagrangean Relaxation (LR) [7, 8] has been very useful in conjunction with branch and bound, which serves as the basis for the development of heuristics (dual ascent) and variable fixing. This approach is composed by sets of constraints that are relaxed and dualized by adding them to the objective function with penalty coefficients, the Lagrangian multipliers. The objective, in the relaxation, is to dualize, possibly after a certain amount of remodeling, which is then transformed into disconnected and easier to solve subproblems. In such a way, these subproblems obtain bounds on the actual integer optimal value, and separate solutions to the individual subproblems which, while not necessarily consistent because they may violate some of the linking constraints, might however suggest ways of constructing good globally feasible solutions.

By applying this method with a vector of Lagrangean multipliers u^1, u^2, u^3, and u^3, the model can be transformed into the following Lagrangean relaxation problem (LR 1). In this case, constraints (1-1) to (1-4) are relaxed, and dualized by adding them to the objective function with penalty coefficients, the Lagrangian multipliers, which are defined as u^1, u^2, u^3, and u^4 with the vectors of $\{u_i^1\}$, $\{u_{wp}^2\}$,$\{u_{wi}^3\}$,$\{u^4\}$ respectively. The objective, in this case, in the relaxation, is to dualize, possibly after a certain amount of remodeling, the constraints linking the component together in such a way that the original problem is transformed into disconnected and easier to solve subproblems. Here, (LR 1) is decomposed into three independent and easily solvable optimization subproblems with respect to decision variables x_p, y_i, and t_{wi}, c_i; the respective subproblems can thus be optimally solved.

Subproblem 1.1 (related to decision variable x_p):

$$Z_{Sub1}(u^3) = \min \sum_{w\in W}\sum_{i\in V}\sum_{p\in P_w} u_{wi}^3 \delta_{pi} x_p, , \qquad \text{(Sub 1.1)}$$

Subject to:

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

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

To reduce the complexity, subproblem 1.1 is decomposed into $|W|$ problems, which are all independent shortest path problems. The value of x_p for each O-D pair w is individually determined. Hence, u_{wi}^3 can be viewed as the cost of node i on O-D pair w. Dijkstra's algorithm is adopted to obtain x_p for each O-D pair w. The time complexity of Dijkstra's algorithm is $O(|V|^2)$, where $|V|$ is the number of nodes; therefore, the time complexity of subproblem 1 is $O(|W|\times|V|)$.

Subproblem 1.2 (related to decision variable y_i):

$$Z_{Sub2}(u^1) = \min \sum_{i\in V} y_i \hat{a}_i(b_i) + \sum_{i\in V} u_i^1 y_i \varepsilon + \sum_{i\in V} u_i^1 y_i(-M) + u_i^1 \varepsilon$$
$$= \min \sum_{i\in V} \left[\hat{a}_i(b_i) + u_i^1 \varepsilon + u_i^1(-M) \right] y_i + u_i^1 \varepsilon, \quad \text{(Sub 1.2)}$$

Subject to:

$y_i = 0$ or 1 $\quad \forall i \in V$ (IP 1.7)

To solve subproblem 1.2 optimally, this problem can also be decomposed into $|V|$ individual problems. The value of decision variable y_i is determined by its coefficient, whose value is $\hat{a}_i(b_i) + u_i^1 \varepsilon + u_i^1(-M)$. In order to minimize subproblem 2, if this coefficient is positive, y_i is set as zero; otherwise it is one. The time complexity of subproblem 2 is *O(|V|)*.

Subproblem 1.3 (related to decision variable t_{wi} and c_i):

$$Z_{Sub3}(u^1, u^2, u^3, u^4)$$
$$= \min \sum_{i\in V} u_i^1 c_i + \sum_{w\in W} \sum_{p\in P_w} u_{wp}^2 \sum_{i\in V} t_{wi} c_i + \sum_{w\in W} \sum_{p\in P_w} u_{wp}^2 \sum_{i\in V} (-\delta_{pi} c_i)$$
$$+ \sum_{w\in W} \sum_{i\in V} u_{wi}^3 (-t_{wi}) + u^4 (-\sum_{w\in W} R_w \sum_{i\in V} t_{wi} c_i) + u^4 S|W|M \quad \text{(Sub 1.3)}$$
$$= \min \sum_{i\in V} \left\{ \left[u_i^1 - \sum_{w\in W} \sum_{p\in P_w} u_{wp}^2 \delta_{pi} + \sum_{w\in W} \left((\sum_{p\in P_w} u_{wp}^2) - u^4 R_w \right) t_{wi} \right] c_i - \sum_{w\in W} u_{wi}^3 t_{wi} \right\}$$
$$+ u^4 S|W|M,$$

Subject to:

$t_{wi} = 0$ *or* 1 $\quad \forall i \in V,\ w \in W$ (IP 1.8)

$c_i = \varepsilon$ *or* M $\quad \forall i \in V.$ (Sub 1.3.2)

To optimally solve subproblem 1.3, it is further decomposed it into $|V|$ independent subproblems. However, since each decision variable t_{wi} and c_i in (LR 4) and (LR 5) have only two kinds of value, the exhaustive search is applied here to find the optimal objective function value among the four combinations of t_{wi} and c_i. The time complexity of subproblem 1.3 is O(|V|×|W|).

These relaxed problems are solved optimally to get a lower bound for the primal problem. After solving (LR 1), the resulting bounds are taken as the initial bounds in the next stage. Three stage heuristics are adopted to derive feasible solutions to the primal problem, and the subgradient method is used to update the Lagrangean multipliers to obtain a better bound.

3.1.2 Getting Primal Feasible Solutions

To obtain the primal feasible solutions of (IP 1), the solutions obtained from (LR) are considered. By using the Lagrangean relaxation method and the subgradient method, it is possible to get the tightest possible bound on the optimal value. The *Zn* auxiliary problem consisting in optimizing the bound over all possible values of the multipliers

is thus solved. This theoretical lower bound on the primal objective function value, as well as ample hints for getting primal feasible solutions, is obtained. However, as some critical and difficult constraints are relaxed to obtain the (LR) problem, the solutions may not be valid for the primal problem. Thus, there is the need to develop heuristics to tune the values of the decision variables so that primal feasible solutions can be obtained. As a result, a heuristic is adopted to improve this situation. In this heuristic, each solution to (LR) is adjusted to a feasible solution to (IP 1).

The concept of this heuristic arises from the attacker's strategy. Given that the node was traversed several times, the attacker would have a higher possibility of attacking it. Hence, the compromised nodes are separated in the *Attack-Bucket*, while the rest nodes are in the *Safety-Bucket.* The nodes in both buckets are separately sorted in descending order by their attacked frequencies. First, select nodes with most frequently from the Safety-Bucket to transfer to the Attacked-Bucket. Then adjust the nodes transferred to the Attacked-Bucket from the Safety-Bucket. In this manner, a heuristic for getting a primal feasible solution is developed. The time complexity for this heuristics is $O(|V|)$.

4 Computational Experiments

4.1 Experiment Environment

The proposed algorithms for the DOD model are coded in Visual C++ and run on a PC with an INTEL^{TM} Core2 CPU 6400 2.13 GHz CPU. Two types of network topology, grid and scale-free networks, as attack targets are demonstrated here. The network size here is under 9, 16, 25, 16 nodes. The parameters used in the experiments are detailed as below.

Table 2. Experiment Parameter Settings

Parameters	Value
Network Topology	Grid (square), Scale-free
Number of Nodes $\|N\|$	9, 16, 25, 36
Total Defense Budget	Equal to Number of Nodes
No. of O-D pairs $\|W\|$	72, 240, 600, 1260
Degree of Disconnectivity (S)	80%, 60%, 40%, 20%
Defense Capability $\hat{a}_i(b_i)$	$\hat{a}_i(b_i) = 0.5b_i + \varepsilon, b_i$

4.2 Computational Experiment of (IP 1)

To demonstrate the effectiveness of the proposed heuristics, we implement one algorithm, Degree-based Attack Algorithm (DAA) for comparison purposes. The details are described in Table 3. The concept of the DAA is derived from the heuristic of stage_1 of the Three-Stage Heuristic for getting a primal feasible solution.

Table 3. Degree-based Attack Algorithm (DAA)

```
1. //Initialization
2. SumOfRTC= ∑_{w∈W} R_w ∑_{i∈V} t_wi c_i
3. Threshold= (S×|W|×M);
// Stage 1: MAX(Node_ Degree) in Safety-Bucket
4. WHILE (SumOfRTC < Threshold AND unfinished==TRUE ){
5.    //Find the node i among the Safety-Bucket
6.    FIND node i, whose degree is maximal;
7.      SET node i to attack; // switch node i to Attack-
Bucket;
8. IF (all the nodes' is in the Attack-Bucket){
9. unfinished==FALSE;
10. }
11. ELSE{
12. unfinished==TRUE;
13. }
14. RUN Dijkstra then to calculate the SumOfRTC;
15.}//end of while
```

4.3 Experiment Result of (IP 1)

To compare attack behavior under different scenarios, we use the attackers' attack cost to evaluate the degree to which the attacker's objective is achieved. The greater the attack cost, the more robust the network. The LR value means the attack cost is calculated by the optimal feasible solution derived from the Lagrangean Relaxation process. The experiment results under different topology types [10], numbers of nodes, and damage distribution patterns are shown in Table 4-4.

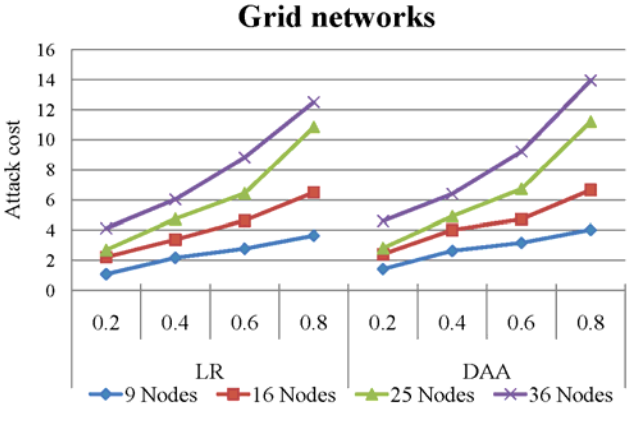

Fig. 1. The comparison of LR and DAA under grid networks

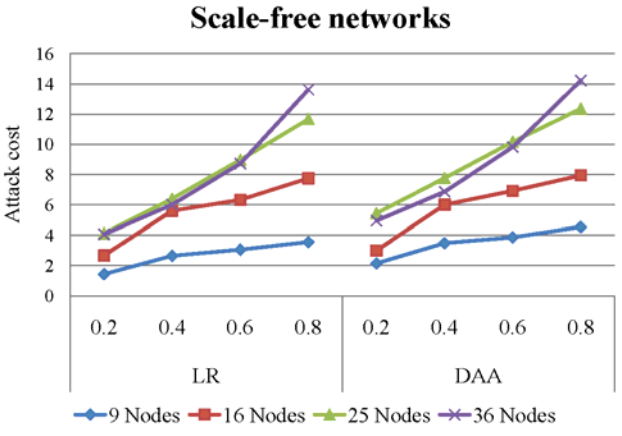

Fig. 2. The comparison of LR and DAA under scale-free networks

As Fig. 1 and Fig. 2 show, among these figures, the cross axle is the Attack cost. Each point on the chart represents the DOD value under degree-based initial budget allocation strategy. The vertical axle is the given threshold of DOD under the given network topologies and budget allocations. Compared to the solution quality of the proposed Lagrangean Relaxation-based algorithm (LR) with DAA, the LR obtained the lowest attack costs. The proposed heuristic outperforms in all cases, which always causes the lowest network survivability (the highest DOD value) in all network topologies and sizes. The attackers' resources are utilized and generalized by the solution derived from LR among various types of network topology. Meanwhile, the survivability of grid networks is lower than others using the DOD metric, since grid networks are more regular and more connected. As a result, some nodes are used more often by OD pairs. If these nodes are compromised by the attacker, the DOD value increases.

5 Conclusions

In this paper, the attack and defense scenarios consider the DOD metric to describe attacker and defender behavior of networks by simulating the role of the defender and the attacker. The attacker tries to maximize network damage by compromising nodes in the network, whereas the defender's goal is to minimize the impact by deploying defense resources to nodes and enhance their defense capability. In this context, the DOD is used to measure the damage of the network. The problem is solved by a Lagrangean Relaxation-based algorithm, and the solution to the problem is obtained from the subgradient-like heuristic and budget adjustment algorithm.

The main contribution of this research is the generic mathematical model for solving the network attack-defense problem, which is modeled as a generic mathematical model. The model is then optimally solved by the proposed heuristic. With this mathematical technique, the complex problems based on the optimized methodology is resolved.

The novel network DOD reflects the aim of an attacker to separate the target network into pieces. This metric enables the indication of the damage of the residual networks. Also, we have examined the survivability of networks with different topologies, sizes and budget allocation policies. Their survivability can be significantly improved by adjusting the defense budget allocation. From the outcomes of the experiments, we can conclude that the defense resources should be allocated according to the importance of nodes.

The current research considers a one-round scenario in which both actors deploy their best strategies under the given topology, but it would be more comprehensive if the scenario is demonstrated in multi-rounds. Both actors may not exhaustively distribute their resources in single round. Moreover, the defenders could deploy some false targets, i.e. honeypots, to attract attackers to waste their budgets. This more complex attacker behavior, therefore, should be considered in further research.

Acknowledgments. This research was supported by the National Science Council of Taiwan, Republic of China, under grant NSC-99-2221-E-002-132.

References

1. Snow, A.P., Varshney, U., Malloy, A.D.: Reliability and Survivability of Wireless and Mobile Networks. IEEE Computer 33(7), 449–454 (2000)
2. Ellison, R.J., Fisher, D.A., Linger, R.C., Lipson, H.F., Longstaff, T., Mead, N.R.: Survivable Network Systems: An Emerging Discipline, Technical Report CMU/SEI-97-TR-013 (November 1997)
3. Westmark, V.R.: A Definition for Information System Survivability. In: Proceedings of the 37th Hawaii International Conference on System Sciences (2004)
4. Al-Kofahi, O.M., Kamal, A.E.: Survivability Strategies in Multihop Wireless Networks. IEEE Wireless Communications (2010)
5. Bier, V.M., Oliveros, S., Samuelson, L.: Choosing What to Protect: Strategic Defense Allocation Against an Unknown Attacker. Journal of Public Economic Theory 9, 563–587 (2007)
6. Powell, R.: Defending Against Terrorist Attacks with Limited Resources. American Political Science Review 101(3), 527–541 (2007)
7. Fisher, M.L.: An Applications Oriented Guide to Lagrangian Relaxation. Interfaces 15(2), 10–21 (1985)
8. Ahuja, R.K., Magnanti, T.L., Orlin, J.B.: Network Flows: Theory, Algorithms, and Applications: Chapter 16 Lagrangian Relaxation and Network Optimization, pp. 598–639. Prentice-Hall, Englewood Cliffs (1993)