Evaluation of Network Survivability Considering Degree of Disconnectivity

Frank Yeong-Sung Lin, Hong-Hsu Yen, Pei-Yu Chen*, and Ya-Fang Wen

Department of Information Management, National Taiwan University
Taipei, Taiwan, R.O.C.
{yslin,d96006,r94048}@im.ntu.edu.tw,
hhyeh@cc.shu.edu.tw

Abstract. It is impossible for a system or network to keep completely safe with the possibility of many new threats occurring at any moment. To analyze and solve these kinds of problems, this paper presents a mathematical programming problem, which adopts a novel metric called Degree of Disconnectivity (DOD) to evaluate the damage level and survivability of a network. To evaluate and analyze the robustness of a network for network operators, this problem is modeled as a mathematical programming problem. Here, an attacker applies his limited attack power intelligently to the targeted network. The objective of the attacker is to compromise nodes, resulting in disconnections of O-D pairs, to ensure that the proposed degree of disconnectivity metric reachs a given level. A Lagrangean relaxation-based algorithm is adopted to solve the proposed problem.

Keywords: Degree of Disconnectivity, Lagrangean Relaxation, Network Attack, Optimization Problem, Resource Allocation.

1 Introduction

Increased reliance on the Internet has made information systems, computers and servers connected to the network more vulnerable to attacks. There are a variety of security threats on the Internet, and the number of new threats is growing rapidly [1]. The result of these threats may include system attacks or failures which may significantly reduce the capability of the communication network to efficiently deliver service to users.[1]. Therefore, the ability for a system or network to maintain a certain level of performance under the presence of security incidents is more important than to prevent a system or network from threats. This concept is called survivability, which is widely used in many networks [2, 3].

Network survivability is one of the most important issues in the planning and operation of networks and security systems, mainly when the threats are related with DoS attacks [4]. There has been a substantial amount of research related to network

[*] Corresponding author.

E. Corchado, M. Kurzyński, M. Woźniak (Eds.): HAIS 2011, Part I, LNAI 6678, pp. 51–58, 2011.

survivability solved by using mathematical programming approaches, such as an optimization problem as presented in [5] to solve network connectivity and flow interdiction problems, and, the problem of designing a network that is able to survive under intentional attacks is examined in [6]. Nevertheless, how to assess the survivability of a network under or after attacks is a continuing problem for information security researchers and experts.

2 Problem Formulation and Notations

2.1 Problem Description

Because an 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. Although in [7], the author proposed two extreme survivability metrics by considering the numbers of the O-D pairs that are connected or disconnected to measure the network survivability, it is too strict to comply with the real case. Based on [7], we have developed a more flexible metric for network survivability. The proposed survivability metric called the *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*, shown in Equation 1. *S* is evaluated on the disconnected numbers of O-D pairs among all O-D pairs, which can be generated as the residual index of the networks. t_{wi} is 1, while node *i* on an O-D pair *w* is dysfunctional. The transmission cost of dysfunctional node is *M*, otherwise it is ε. The greater the value of *S*, the more the network is damaged.

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

2.2 Problem Formulation

In this section, the serial of attack actions considering the survivability of a network is 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. Here, both the attacker and the defender have complete information about the targeted network topology and the budget allocation is assumed.

The above problem is formulated as a maximization 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 pair
P_w	Set of all candidate paths of an OD pair w, where $w \in W$
M	Large enough number of processing cost that indicates a node has been compromised
ε	Small enough number of 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

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 O-D 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 problem:

Objective function:

$$\min_{y_i} \sum_{i \in V} y_i \hat{a}_i \ , \tag{IP 1}$$

Subject to:

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

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

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

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

$$\sum_{p \in P_w} x_p = 1 , \ \forall w \in W \tag{IP 1.5}$$

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

$$y_i = 0 \text{ or } 1 , \ \forall i \in V \tag{IP 1.7}$$

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

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 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. Last, 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) [8] is an optimization method that can be applied to linear and integer programming, combinatorial optimization, and non-linear programming [9]. In this paper, a Lagrangean relaxation-based algorithm is thus proposed, in conjunction with the subgradient method, to solve (IP 1).

By applying this method [8] with a vector of Lagrangean multipliers u^1, u^2, u^3, and u^3, the model into the following Lagrangean Relaxation problem (LR 1) is transformed. In this case, Constraints (1-1) to (1-4) are relaxed. To achieve better results, a Lagrangean relaxation procedure is adopted. By definition, u^1, u^2, u^3, and u^4 are the vectors of $\{u_i^1\}$, $\{u_{wp}^2\}$,$\{u_{wi}^3\}$,$\{u^4\}$ respectively. (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, and the respective subproblems can thus be optimally solved.

Subproblem 1 (related to decision variable x_p)

$$Z_{Sub1}(u^3) = \min \sum_{w\in W}\sum_{i\in V}\sum_{p\in P_w} u_{wi}^3 \delta_{pi} x_p , \tag{Sub 1}$$

$$\sum_{p\in P_w} x_p = 1 , \forall w\in W \tag{LR 1}$$

$$x_p = 0 \text{ or } 1 , \forall p\in P_w , w\in W. \tag{LR 2}$$

To reduce the complexity, subproblem 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*|×|*V*|*)*.

Subproblem 2 (related to decision variable y_i)

$$\begin{aligned} Z_{Sub2}(u^1) &= \min \sum_{i\in V} y_i \hat{a}_i(b_i) + \sum_{i\in V} u_i^1 y_i \varepsilon + \sum_{i\in V} u_i^1 y_i(-M) + u_i^1 \varepsilon \\ &= \min \sum_{i\in V} \left[\hat{a}_i(b_i) + u_i^1 \varepsilon + u_i^1(-M) \right] y_i + u_i^1 \varepsilon, \end{aligned} \qquad \text{(Sub 2)}$$

$$y_i = 0 \text{ or } 1\,,\ \forall i \in V. \qquad \text{(LR 3)}$$

To solve subproblem 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 3 (related to decision variables t_{wl}, c_l)

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

$$t_{wi} = 0 \text{ or } 1 \qquad \text{(LR 4)}$$

$$c_i = M \ or\ \varepsilon\ ,\ \forall i \in V. \qquad \text{(LR 5)}$$

To optimally solve subproblem 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 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, a theoretical lower bound on the primal objective function value and ample hints for getting primal feasible solutions are 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 a have higher possibility of attacking it. Hence, the compromised nodes are separated in the *Attack-Bucket*, while the rest nodes are in the *Safety-Bucket.* First, select nodes from the Safety-Bucket to transfer to the Attacked-Bucket. Then adjust the nodes transferred to the Attacked-Bucket from the Safety-Bucket. Along 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. To determine which budget allocation policy is more effective under different cases, two initial budget allocation policies are designed–uniform and degree-based. The former distributes the defense budget evenly to all nodes in the network, while the latter allocates budget to each node according to the percentage of a node's degree.

4.2 Experiment Result of the Problem of (IP 1)

To compare attack behavior under different scenarios, we use the attacker's attack cost to evaluate the degree to which the attacker's objective is achieved. The greater the attack cost, the more robust of the network. As Fig. 1 shows, the robustness of grid networks of these two budget allocations, uniform and degree-based, is quite similar. Inasmuch as the property of grid networks is fair to each node within networks, the same tendency can be found with these two budget allocations.

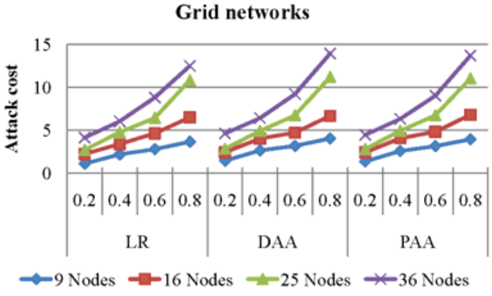

Fig. 1. Attack cost of grid networks under different budget allocations

For Fig. 2, under scale-free networks, comparing these two budget allocations, the uniform type is more vulnerable than degree-based. The regulation is an undesigned coincidence with Figure 4-4 and Figure 4-5. The uniform budget allocation, which treats each node equally, fails to reflect the discrepancy between the nodes, and results in an insecure network.

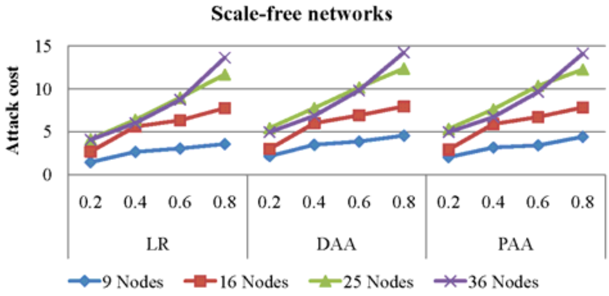

Fig. 2. Attack cost of scale-free Networks under different budget allocation

From Fig. 1 and Fig. 2, the increasing average damage level apparently gave rise to attack costs under diverse topologies and budget allocations. It is unmistakably clear that the proposed DOD metric is reflected in the residual survivable nodes of the networks. By disbursing more resources, the attackers achieve a higher average damage level to the target networks.

5 Conclusion

In this paper, we use attack and defense scenarios considering the DOD metric to describe attacker and defender behavior of networks. According to attacker's objective, the robustness of the networks is evaluated by the defender. The lesser the attack cost, the worse the survivability. The key contribution of this paper is that the attack and defense scenarios are successfully modeled as a well-formulated mathematical model, which is then optimally solved by the proposed heuristic. With this mathematical technique, we can resolve the complex problems based on the optimized methodology.

The novel network DOD metric is another contribution of this paper. The metric 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. Finally, we have also examined different network topologies and observed their robustness to malicious and intelligent attacks. The experiment results show that the degree-based defense budget allocation strategy is the most robust.

In this paper, we adopt a DOD metric in the computational experiments. The current research considers two attack strategies under given topology, but it would be more comprehensive if attacker behavior is more vivid. If the attacker's apparent objective is to compromise a network, he will try his best to damage the target network, for example, by spending different budgets according to the importance of a node. 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. Peters, S.: 2009 CSI Computer Crime and Security Survey, Computer Security Institute (December 2009)
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. Garg, M., Smith, J.C.: Models and Algorithms for the Design of Survivable Multicommodity Flow Networks with General Failure Scenarios. Omega 36(6), 1057–1071 (December 2008)
4. Pinzón, C., De Paz, J.F., Zato, C., Pérez, J.: Protecting Web Services against DoS Attacks: A Case-Based Reasoning Approach. In: Graña Romay, M., Corchado, E., Garcia Sebastian, M.T. (eds.) HAIS 2010. LNCS, vol. 6076, pp. 229–236. Springer, Heidelberg (2010)
5. Murray, A.T., Matisziw, T.C., Grubesic, T.H.: Critical Network Infrastructure Analysis: Interdiction and System Flow. Journal of Geographical Systems 9(2), 103–117 (June 2007)
6. Smith, J.C., Lim, C., Sudargho, F.: Survivable Network Design Under Optimal and Heuristic Interdiction Scenarios. Journal of Global Optimization 38(2), 181–199 (June 2007)
7. Lin, Y.S., Tsang, P.H., Chen, C.H., Tseng, C.L., Lin, Y.L.: Evaluation of Network Robustness for Given Defense Resource Allocation Strategies. In: 1st International Conference on Availability, Reliability and Security, pp. 182–189 (April 2006)
8. Fisher, M.L.: An Applications Oriented Guide to Lagrangian Relaxation. Interfaces 15(2), 10–21 (April 1985)