Network Recovery Strategies for Maximization of Network Survivability

Frank Yeong-Sung Lin
Department of Information Management
National Taiwan University
Taipei, Taiwan, R.O.C.
yslin@im.ntu.edu.tw

Yu-Shun Wang
Department of Information Management
National Taiwan University
Taipei, Taiwan, R.O.C.
d98002@im.ntu.edu.tw

Pei-Yu Chen
Department of Information Management
National Taiwan University
Information & Communication Security Technology Center
Institute Information Industry
Taipei, Taiwan, R.O.C.
d96006@im.ntu.edu.tw

Yao-Yuan Chang
Department of Information Management
National Taiwan University
Taipei, Taiwan, R.O.C.
r97025@im.ntu.edu.tw

Abstract—**Although enterprises make profits by satisfying customers' needs, which is most often facilitated by information systems and network infrastructures, it is difficult to keep the systems and the network components regularly operating without any downtime. As a result, it is an important and critical issue for the system administrator or defender to efficiently evaluate network survivability. In this paper, a network optimization problem of attacker and defender behavior is considered. Both actors utilize their resources: the attackers launching attacks try to maximize the damage of the network, while the defenders deploy resources on the nodes and recover the compromised nodes. This problem is considering with survivability with a metric, Degree of Disconnectivity (DOD), which is used to evaluate the damage level of the network. The Lagrangean Relaxation Method is then applied to obtain optimal solutions for the proposed problem.**

Keywords- Survivability, Degree of Disconnectivity, Network Recovery, Lagrangean Relaxation, Network Attack, Optimization Problem, Resource Allocation.

I. Introduction

Enterprises seek profits by fulfilling the needs or wants of their customers with products and services. Computer systems and network infrastructure components play a critical role in supporting an enterprise's ability to meet customers' needs. In fact, their role has grown to a point where the slightest disruption can adversely affect the enterprise's ability to manage information and deliver products and services to its customers. System administrators often need to keep those systems to smoothly operating. However, the number and nature of the systems and components may be rendered dysfunctional by malicious and intentional attacks. Those attacks attempt to forcefully abuse or take advantage of targets, whether through computer viruses, social engineering, or phishing [1], and are often done with the intent of stealing a system's information or of reducing the functionality of a target component. This is a challenge to enterprises, which need to continuously provide services despite the presence of intrusions.

The term survivability refers to the capacity of any system to deliver essential services and maintain essential properties, including confidentiality, integrity, and availability, even under malicious and intentional attacks [2]. Unlike the traditional security measures that require central control or administration, survivability is intended to address unbounded network environments. The ability of survivability is the measure of whether a network can continue providing service in the presence of failure. High survivability represents the quick response processes of reconfiguration and reestablishment of connections upon failures. Among several survivability metrics, degree of disconnectivity (DOD) which is proposed in [3] is most sensible. This metric reflects the aim of an attacker to separate the target network into pieces, which enables the indication of the damage of the residual networks.

Hence, system administrators, i.e. defenders, require distributing their resources on vital components in advance or recovering those components that are compromised. The defenders choose their best strategy which would result in a higher survivability [4]. Based on common network models, current research typically focuses on determining optimal resource allocation of security investments. In [5], for example, defenders assign defense budgets according to their strategies, to protect systems from outside attacks. Meanwhile, the attackers distribute their effort evenly among all attacked elements under a homogeneous system which is separated into independent identical parallel elements. The resources to both defenders and attackers are limited. However, the recovery

978-1-4577-9538-2/11/$26.00 ©2011 IEEE

strategies of defenders, which is more generalized in network scenarios, is not included. Therefore, in this paper, an attack-defense scenario is modeled as a mathematical formulation, in which the attackers utilize their strategies, while the defenders can distribute resources on critical components and recover compromised ones.

II. Problem Formulation and Notations

In the real world, network attack and defense are ongoing processes. For modeling purposes, the problem is defined as an attack-defense problem. An optimization model is developed that simulates the roles of attackers and defenders, in which attackers want to compromise nodes that cause maximal impact to the network, while defenders try to minimize the damage by deploying defense resources to nodes and repairing broken nodes. Damage of the network is measured in terms of the Degree of Disconnectivity (DOD) value, defined as S [3]. This metric is shown in equation (1). DOD 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. Here, 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.

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

When a node is compromised by the attacker, it is inoperable and thus cannot be used for transmitting information. Moreover, both sides have budget limitations: the attacker only has attack budget, whereas the defender has two types of budget, one for defense and the other for repair. When more defense budget is allocated to a node, it has a higher defense capability and is harder for an attacker to compromise, thus causing him to spend more resources to destroy that node. In this context, the terms “resource” and “budget” are used interchangeably to describe the effort spent on nodes by attacker or defender, and the defense capability of a node is related to the defense budget allotted to it.

The interaction of both actors is under complete information. The attackers and the defenders have a targeted network topology and the budget allocation is assumed. The defenders try to deploy defense resources to nodes in the network, in order to increase the attack cost of nodes. The attackers start to launch attacks that compromise nodes, trying to maximize the damage, i.e. DOD, of the network. Since attackers only have limited budget, they must make good use of their budget and decide which nodes to attack in order to cause the greatest impact to network operation. Meanwhile, the network defenders repair nodes compromised by attackers. The repair budget determined by the defenders is fully utilized to recover service and minimize the loss of the network. Note that in this problem, the defense resources are defined as hardware or software installed to protect nodes in the network. As a result, when compromised nodes with defense resources are repaired by the defenders, the nodes’ defense capability is restored to the level before the attack. The given parameters and decision variables of the problem are shown in Table I.

TABLE I. Given Parameters and Decision Variables

Notation	Description
Given parameter	
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 processing cost that indicates a node has been compromised
δ_{pi}	Indicator function, 1 if node i is on path p, 0 otherwise, where $i \in V$ and $p \in P_w$
b_i	Defense budget allocated to node i
d_i	Existing defense resources on node i, used for condition which has more than 1 round
$a_i(b_i+d_i)$	Attack cost of node i, which is a function of b_i+d_i
q_i	State of node i before this round. 1 if node i is inoperable, 0 otherwise, used for condition which has more than 1 round
A	Attacker’s total budget in this round
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 minimization problem:

Objective function:

$$\min_{z_i} \frac{\sum_{w\in W}\sum_{i\in V} t_{wi}c_i}{|W| \times M} , \qquad \text{(IP 1)}$$

Subject to:

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

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

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

$$\sum_{i\in V} e_i z_i \le B' \qquad \text{(IP 1.4)}$$

$$z_i \le y_i \qquad \forall i \in V \qquad \text{(IP 1.5)}$$

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

$$x_p = 0 \text{ or } 1 \qquad \forall p \in P_w,\ w \in W \quad \text{(IP 1.7)}$$

$$z_i = 0 \text{ or } 1 \qquad \forall i \in V \quad \text{(IP 1.8)}$$

$$t_{wi} = 0 \text{ or } 1 \qquad \forall\ i \in V,\ w \in W. \quad \text{(IP 1.9)}$$

The objective function (IP 1) is to minimize the damage of the network, where the defenders try to minimize the DOD value by deciding which nodes to repair (denoted by z_i). Constraint (IP 1.1) describes the definition of processing cost c_i, which is ε if i is functional, M if i is compromised. Constraint (IP 1.2) requires the selected path for an OD pair w should have the minimal cost. Constraint (IP 1.3) represents the relationship between $x_p\delta_{pi}$ and t_{wi}. Constraint (IP 1.4) restricts the total attack cost spent on the nodes and should not exceed attacker's budget A. Constraint (IP 1.5) enforces the attacker cannot attack a node that is already dysfunctional. Constraints (IP 1.6) and (IP 1.7) jointly limit the possibility that only one of the candidate paths of an OD pair w can be selected. Lastly, constraints (IP 1.7) to (IP 1.9) impose binary restrictions on decision variables.

III. Solution Approach

A. Lagrangean Relaxation

In order to solve the (IP 1), the constraint (IP 2.3) is first reformulated as below, and a redundant constraint (IP 2.10) is added, as shown below. Note that the optimal condition is not violated if an equation is relaxed into an inequality version.

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

$$c_i = \varepsilon \text{ or } M \qquad \forall i \in V. \quad \text{(IP 1.10)}$$

After reformulation, by applying the Lagrangean Relaxation Method [6], (IP 1) is then transformed into the following Lagrangean relaxation problem (LR 1), where constraints (IP 1.1'), (IP 1.2), (IP 1.3') and (IP 1.4) are relaxed. With a vector of Lagrangean multipliers, the Lagrangean relaxation problem of (IP 1) is transformed. The Lagrangean multipliers v^1, v^2, v^3 are the vectors of $\{ v_i^1 \}$, $\{ v_{wp}^2 \}$ and $\{ v_{wi}^3 \}$, respectively, where v^1 is unrestricted, v^2 and v^3 are non-negative. Lagrangean multiplier v^4 is also non-negative. In order to solve (LR 2), it is further divided into three independent and easily solvable subproblems, as shown below.

Subproblem 1.1 (related to decision variable x_p):

$$Z_{\text{Sub 1.1}}(v^3) = \min \sum_{w \in W} \sum_{i \in V} \sum_{p \in P_w} v_{wi}^3 \delta_{pi} x_p\ , \quad \text{(Sub 1.1)}$$

Subject to: (IP 1.6), (IP 1.7).

Dijkstra's shortest path algorithm can be applied to (Sub 1.1) since the node weight v_{wi}^3 is non-negative. The time complexity of this problem is $O(|W| \times |V|^2)$, where $|W|$ is the number of OD pairs.

Subproblem 1.2 (related to decision variable y_i):

$$Z_{\text{Sub 1.2}}(v^1, v^4) = \min \sum_{i \in V} \left[v_i^1 (M - \varepsilon) + v^4 e_i \right] z_i\ , \quad \text{(Sub 1.2)}$$

Subject to: (IP 1.5), (IP 1.8).

(Sub 1.2) can be simply and optimally solved by examining the coefficient of y$_i$, for each node i, if the coefficient $\left[v_i^1 (M - \varepsilon) + v^4 e_i \right]$ is positive or the value of q_i is one, the value of y$_i$ is set to zero; conversely, if $\left[v_i^1 (M - \varepsilon) + v^4 e_i \right]$ is non-positive and the value of the value of q_i is equal to zero, and y$_i$ is set to one. The time complexity of (Sub 1.2) is $O(|V|)$.

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

$$\begin{aligned} Z_{\text{Sub 1.3}}(v^1, v^2, v^3) = {} & \\ \min \sum_{i \in V} c_i v_i^1 + {} & \sum_{i \in V} \sum_{w \in W} \sum_{p \in P_w} v_{wp}^2 \delta_{pi} c + \\ & + \sum_{i \in V} \sum_{w \in W} \frac{c_i t_{wi}}{|W| \times M} + \sum_{i \in V} \sum_{w \in W} \sum_{p \in P_w} c_i v_{wp}^2 t_{wi}\ , \quad \text{(Sub 1.3)} \\ & - \sum_{w \in W} v_{wi}^3 t_{wi} \end{aligned}$$

Subject to:

$$t_{wi} = 0 \ or\ 1 \qquad \forall i \in V,\ w \in W \quad \text{(IP 1.9)}$$

$$c_i = \varepsilon \text{ or } M \qquad \forall i \in V. \quad \text{(Sub 1.3.2)}$$

In (Sub 1.3), both decision variables t_{wi} and c_i have two options. As a result, the value of t_{wi} and c_i can be determined by applying an exhaustive search to obtain the minimal value. The time complexity here is $O(|W| \times |V|)$.

The Lagrangean Relaxation problem (LR 1) can be solved optimally if all the above subproblems are solved optimally. By the weak duality theorem [6], for any set of multipliers, the solution to the dual problem is a lower bound on the primal problem (IP 1). To acquire the tightest lower bound, the value of Lagrangean multipliers needs to be adjusted to maximize the optimal value of the dual problem. Although the dual problem can be solved in many ways, the subgradient method is the most widely used one, where the subgradient direction is obtained after all subproblems are minimized, and the multipliers are updated along this subgradient direction. Here, the subgradient method is adopted to solve the dual problem.

B. Getting Primal Feasible Solutions

By applying the Lagrangean Relaxation Method, a theoretical lower bound on the primal objective function can be found. This approach provides some suggestions for obtaining feasible solutions for the primal problem. However, the result of the dual problem may be invalid when compared to the original problem since some important and complex constraints are relaxed. Therefore, a heuristic is needed here to make infeasible solutions feasible. In order to obtain primal feasible solutions and an upper bound on the problem of (IP 1), the outcome of (LR 1) and Lagrangean multipliers are used as hints for deriving solutions. The concept of the proposed heuristic is described below.

Recall that subproblem 1.1 is related to decision variable x_p, which determines the path to be used for an OD pair. By using this hint provided by subproblem 1.1, for each OD pair w, the chosen path is used to traverse from source to destination and to calculate the number of times a node is used by all OD pairs, called node popularity (NP). A node with a larger NP value is likely to be an attack target, since more paths use this node. Therefore, attacking this node may result in larger DOD. An additional important issue for the attacker is the attack cost (AC) of the nodes in the network, because the attacker has a budget limitation. Hence, both factors are considered in the heuristic for getting primal feasible solutions. Once the popularity of nodes is determined, all nodes according to the ratio of NP to AC are sorted in descending order. For each of the sorted vertices i, the total attack cost and attack budget A is checked. If node i can be compromised without exceeding attack budget A, node i is selected as the attack target; else go to next node until all nodes are examined.

C. *Solution Approach for Solving (IP 1)*

The result of the problem represents the attack strategy under a certain initial defense budget allocation policy. The objective (IP 1) is to minimize the maximized damage of the network under malicious and intentional attacks. From the current attack strategy, the defender can adjust the budget allocated to nodes in the network according to certain reallocation policies. After budget adjustment, the problem is solved again to derive an attack strategy under the new defense budget allocation policy. This procedure is repeated a number of times until an equilibrium is achieved.

The concept used to adjust the defense budget allocation policy is similar to the subgradient method [7], in which the budget allocated to each node is redistributed according to current step size. This subgradient-like method is described as follows. Initially, the status of each node after attack is checked. If the node is uncompromised, this suggests that the defense resources (budget) allotted to this node is inadequate (more than needed) or it is unworthy for an attacker to attack this node as the node has too great a defense budget. Therefore, we can extract a fraction of the defense resources from the nodes unaffected by attacks, and allocate it to compromised nodes. The amount extracted is related to the step size coefficient, and it is halved if the optimal solution of (IP 1) does not improve in a given iteration limit.

Another factor that is related to the deducted defense resources is the importance of a node. In general, the greater the number of times a node is used by all OD paths implies higher importance. When a node with a larger number of times used by all OD paths is compromised, it provides a higher contribution to the growth of the objective function value (i.e. DOD), compared with a node with a smaller number of times. As a result, only a small amount of defense resources should be extracted from nodes with higher usage. In the proposed subgradient-like method, the importance factor to measure the importance of a node is used, which is calculated by t_i / t_{total}, where t_i is the average number of times node i used by all OD paths, and t_{total} is the summation of t_i ($\forall i \in V$). An uncompromised node with greater importance factor will have a lower amount of defense resources extracted.

IV. Computational Experiments

A. *Experiment Environment*

For the proposed Lagrangean Relaxation algorithm, a simple algorithm is implemented using C++ language, and the program was executed on a PC with AMD 3.6 GHz quad-core CPU. Here three types of network topology acted as attack targets: the grid network, random network and scale-free network. To determine which budget allocation policy is more effective under different cases, two initial budget allocation policies were designed uniform and degree based. The former distributed the defense budget evenly to all nodes in the network, while the latter allocated budget to each node according to the percentage of a node's degree.

B. *Computational Experiment of (IP 1)*

To prove the effectiveness of the Lagrangean Relaxation algorithm and the proposed heuristic, one simple algorithm were developed, introduced in Table II for comparison purposes. We designed two repair cost distributions. The first is uniform distribution, defined as RC1, where each node in the network has same repair cost; the second is degree-based distribution, defined as RC2, in which nodes with a larger degree have a higher repair cost.

TABLE II. Experiment parameter settings

```
//initialization

total_repair_cost = 0;
sort all nodes by their node degree in descending
order;

for each node i { //already sorted
        if  (  total_repair_cost+  repair_cost_i<=
TOTAL_REPAIR_BUDGET
        AND node i is compromised ){
                repair node i;
                total_repair_cost+=repair_cost_i;
        }
}

calculate DOD;
return DOD;
```

C. *Experiment Result of (IP 1)*

Figure 1 shows the experiment results before and after recovery, and compares the performance between the proposed LR repair algorithm and simple algorithm (SA). Furthermore, the gap between LR and LB is displayed. Each point on the chart represents the DOD of different node numbers and topologies under uniform repair cost distribution. Obviously, the performance of our proposed LR repair algorithm is better than that of the degree-based simple algorithm (approximately 35% improvement on average); the mean gap between LR and LB is 30%.

Figure 2 to Figure 3 illustrate the survivability, i.e. DOD, of the network before and after recovery under different topologies, node numbers and repair cost distributions. From the above figures, the proposed LR-based repair algorithm performs well in both repair cost distributions. In addition, it also provides an insight for defenders. Since the RC2 is greater than RC1 in all cases, which shows that networks with degree-based repair cost distribution of higher DOD. It represents that lesser effect after restoration, and the defender has to spend more resources repairing important nodes.

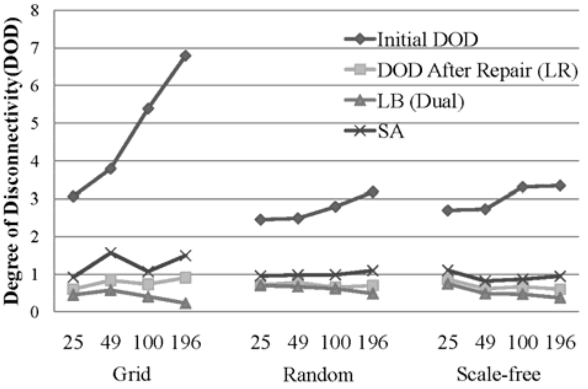

Figure 1. Survivability of Different Network Size and Topology after Repair

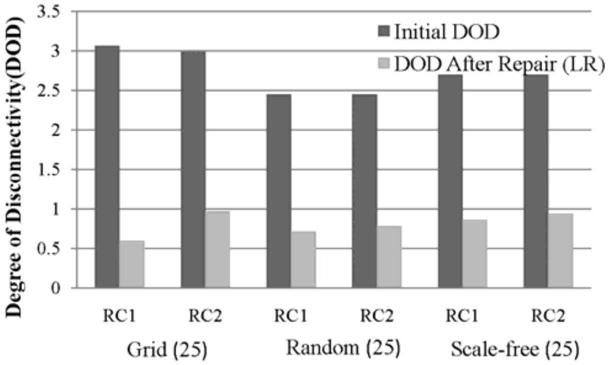

Figure 2. Survivability of Small Size Networks under Different Repair Cost Distributions

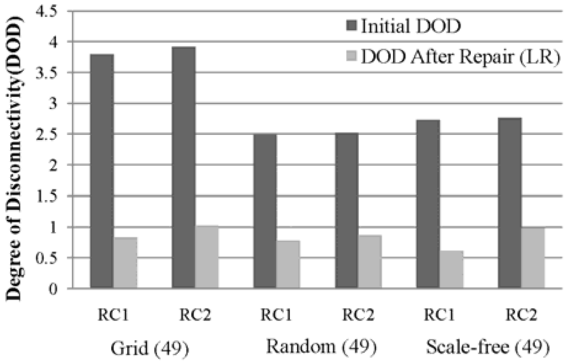

Figure 3. Survivability of Medium Size Networks under Different Repair Cost Distributions

V. Conclusion

In this paper, a mathematical programming model combining a survivability analysis with optimization is developed and which can be used for solving a network attack-defense problem by considering the two actors of the defender and the attacker. Attackers try to maximize network damage by compromising nodes in the network, whereas the defenders' goal is to minimize the impact by deploying defense resources to nodes, enhancing their defense capability and repairing dysfunctional nodes. In this context, the Degree of Disconnectivity (DOD) is used to measure the damage of the network. The scenario is solved by Lagrangean relaxation-based algorithm, in which the defender attempts to minimize the impairment by repairing dysfunctional nodes. The solution to repair the problem is also derived from Lagrangean relaxation-based algorithm.

The main contribution of this research is the proposed model narrates behaviors of attackers and defenders on network scenarios in an adaptive way, especially on the defenders' repair strategies. From the experiment results, the proposed Lagrangean relaxation-based algorithms are proven effective and can be applied to real-world networks, such as grid, random and scale-free networks. Also, the survivability of networks with different topologies, sizes and budget allocation policies have also been examined.

It is assumed that the repair costs of the nodes in the network are the same or related to their degree. Nevertheless, nodes with higher defense resources should be harder for the defender to repair and thus have larger repair cost. Therefore, in future research, the form of the function appropriate for describing this relationship is an issue that can be further studied and can be applied in this scenario.

Acknowledgment

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

References

[1] P.O. Okenyi and T.J. Owens, "On the Anatomy of Human Hacking, Information Systems Security, " vol. 16, issue 6, pp. 302–314, 2007.

[2] N.R Mead, R.J. Ellison, R.C. Linger, T. Longstaff, and J. McHugh, "Survivable Network Analysis Method," CMU/SEI-2000-TR-013, September 2000.

[3] F.Y.S. Lin, H.H. Yen, P.Y. Chen, "Maximization of Network Survivability Considering Degree of Disconnectivity, " 7th International Wireless Communications and Mobile Computing Conference, June 2011.

[4] S. Rani, A.K. Sharma, and P. Singh, "Resource Allocation Strategies for Survivability in WDM Optical Networks, " Optical Fiber Technology, vol. 13, issue 3, pp. 202–208, 2007.

[5] J.E. Ramirez-Marquez, C.M. Rocco, G. Levitin, "Optimal Network Protection against Diverse Interdictor Strategies, Reliability Engineering and System Safety, " vol. 96, issue 3, pp. 37–282, 2008, March 2011.

[6] M.L. Fisher, "The Lagrangian Relaxation Method for Solving Integer Programming Problems, " Management Science, vol. 27, no. 1, pp. 1–18, January 1981.

[7] M. Held, P. Wolfe, and H.P. Crowder, "Validation of Subgradient Optimization," Mathematical Programming, vol. 6, pp. 62–88, 1974.