# Network Defense Strategies for Maximization of Network Survivability

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

[1] Department of Information Management, National Taiwan University
[2] Department of Information Management, Shih Hsin University
[3] Information and Communication Security Technology Center
[4] Institute Information Industry
Taipei, Taiwan, R.O.C.
yslin@im,ntu.edu.tw,hhyen@cc.shu.edu.tw,
d96006@im.ntu.edu.tw,r94048@im.ntu.edu.tw

**Abstract.** The Internet has brought about several threats of information security to individuals and cooperates. It is difficult to keep a network completely safe because cyber attackers can launch attacks through networks without limitations of time and space. As a result, it is an important and critical issue be able to efficiently evaluate network survivability. In this paper, an innovative metric called the Degree of Disconnectivity (DOD) is proposed, which is used to evaluate the damage level of the network. A network attack-defense scenario is also considered in this problem, in which the attack and defense actions are composed by many rounds with each round containing two stages. In the first stage, defenders deploy limited resources on the nodes resulting in attackers needing to increase attack costs to compromise the nodes. In the second stage, the attacker uses his limited budget to launch attacks, trying to maximize the damage of the network. The Lagrangean Relaxation Method is applied to obtain optimal solutions for the problem.

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

## 1 Introduction

With growth of internet use, the number of experienced computer security breaches has increased exponentially in recent years, especially impacting on businesses that are increasingly dependent on being connected to the Internet. The computer networks of these businesses are more vulnerable to access from outside hackers or cyber attackers, who could launch attacks without the constraints of time and space. In addition to the rapid growth in rate of cyber attack threats, another factor that influences overall network security is the network protection of the network defender [1]. Although it is impossible to keep a network completely safe, the problem of the network security thus gradually shifts to the issue of survivability [2]. As knowing

* Corresponding author.

K.G. Mehrotra et al. (Eds.): IEA/AIE 2011, Part I, LNAI 6703, pp. 125–134, 2011.

how to evaluate the survivability of the Internet is a critical issue, more and more researchers are focusing on the definitions of the survivability and evaluation of network survivability.

However, to enhance or reduce the network survivability, both network defender and cyber attacker usually need to invest a fixed number of resources in the network. The interaction between cyber attackers and network defenders is like information warfare, and how to efficiently allocate scarce resources to the network for both cyber attacker and network defender is a significant issue. Hence, the attack-defense situation can be formulated as a min-max or max-min problem. As a result, researchers can solve this kind of attack-defense problem of network security by mathematical programming approaches, such as game theory [3], Simulated Annealing [4], Lagrangean Relaxation Method [5]. In [5], the authors propose a novel metric called Degree of Disconnectivity (DOD) that is used to measure the damage level, or survivability, of a network. The DOD value is calculated by (1), in which a larger DOD value represents a greater damage level, which also implies lower network survivability. An attacker's objective is to minimize the total attack cost, whereas a defender's objective is to maximize the minimized total attack cost. The DOD is used as a threshold to determine whether a network has been compromised.

Considering the defense and attacker scenarios in the real world, it is more reasonable that the attacker fully utilizes his budget to cause maximal impact to the network rather than simply minimize his total attack cost. In this paper, the attack and defense actions are composed by rounds, where each round contains two stages. In the first stage, a defender deploys defense resources to the nodes in the network, whereas in the second stage, an attacker launches attacks to compromise nodes in the network in order to cause maximal impact to the network. Survivability and damage of the network is measured in terms of the DOD value.

$$\frac{\sum(number\ of\ broken\ nodes\ on\ shortest\ path\ of\ each\ OD\ pair)}{number\ of\ all\ OD\ pairs\ of\ a\ network} \tag{1}$$

## 2 Problem Formulation and Notations

In this paper, the two roles of attackers and defenders are described in this optimization model. An attacker wants to compromise nodes that cause maximal impact to the network, while a defender tries to minimize the damage by deploying defense resources to nodes. Both the attacker and the defender have perfect information about the network topology. Damage and impact of the network is measured in terms of the Degree of Disconnectivity (DOD) value here. If a node is compromised by the attacker, it is dysfunctional and thus cannot be used for transmitting information. Meanwhile, both sides have a budget limitation, and the total attack costs and defense resources are under their entire expenditure. The cost of compromising a node is related to the defense budget allocated to it. The result is that attackers have to allocate more costs on a node once more defense budget is allocated to the corresponding node. Note that in this context, the terms "resource" and "budget" are used interchangeably to describe the effort spent on nodes by attackers or defenders.

In the real world, network attack and defense are continuous processes. For modeling purposes, the problem is defined as an attack-defense problem, with each round contains the two stages of defense and attack. First, the defender tries to minimize network damage, i.e., DOD value, by deploying defense resources to the nodes in the network. The allocation is restricted by the defender's defense budget. Next, attackers start to launch attacks that compromise nodes, trying to maximize the damage, i.e. DOD value, of the network. Since attackers only have a limited budget and thus have to make good use of their budget, they need to decide which nodes to attack in order to cause the greatest impact to network operation. The given parameters and decision variables of the problem are shown 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 |
| $\varepsilon$ | Small enough number of processing cost that indicates a node is functional |
| $\delta_{pi}$ | Indicator function, 1 if node $i$ is on path $p$, 0 otherwise, where $i \in V$ and $p \in P_w$ |
| $d_i$ | Existing defense resources on node $i$, used for condition which has more than 1 round, where $i \in V$ |
| $a_i(b_i+d_i)$ | Attack cost of node $i$, which is a function of $b_i+d_i$, where $i \in V$ |
| $q_i$ | State of node $i$ before this round. 1 if node $i$ is inoperable, 0 otherwise, used for a condition which has more than 1 round, where $i \in V$ |
| $A$ | Attacker's total budget in this round |
| $B$ | Defender's defense 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 OD pair $w$, 0 otherwise, where $i \in V$ and $w \in W$ |
| $c_i$ | Processing cost of node $i$, which is $\varepsilon$ if $i$ is functional, $M$ if $i$ is compromised by attacker, where $i \in V$ |
| $b_i$ | Defense budget allocated to node $i$, where $i \in V$ |

The problem is then formulated as the following min-max problem:
Objective function:

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

Subject to:

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

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

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

$$\sum_{i\in V} y_i a_i \left(b_i + d_i\right) \le A \qquad \text{(IP 1.4)}$$

$$\sum_{i\in V} b_i \le B \qquad \text{(IP 1.5)}$$

$$0 \le b_i \le B \qquad \forall i\in V \qquad \text{(IP 1.6)}$$

$$y_i + q_i \le 1 \qquad \forall i\in V \qquad \text{(IP 1.7)}$$

$$\sum_{p\in P_w} x_p = 1 \qquad \forall w\in W \qquad \text{(IP 1.8)}$$

$$x_p = 0 \text{ or } 1 \qquad \forall p\in P_w,\ w\in W \qquad \text{(IP 1.9)}$$

$$y_i = 0 \text{ or } 1 \qquad \forall i\in V \qquad \text{(IP 1.10)}$$

$$t_{wi} = 0 \text{ or } 1 \qquad \forall\ i\in V,\ w\in W. \qquad \text{(IP 1.11)}$$

Objective function (IP 1) is to minimize the maximized damage of the network. That is, the attacker tries to maximize the DOD value by deciding which nodes to attack (denoted by $y_i$), while the defender tries to minimize the DOD value by deciding to which nodes defense resources should be allocated (denoted by $b_i$). Constraint (IP 1.1) describes the definition of processing cost $c_i$, which is $\varepsilon$ 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 and should not exceed attacker's budget $A$. Constraint (IP 1.5) specifies that the total defense budget allocated to nodes should not exceed defense budget $B$. Constraint (IP 1.6) indicates that variable $b_i$ is continuous and bounded by 0 and defense budget $B$. Constraint (IP 1.7) specifies the attacker cannot attack a node that is already dysfunctional. Constraints (IP 1.8) and (IP 1.9) jointly limit the possibility that only one of the candidate paths of an OD pair $w$ can be selected. Lastly, constraints (IP 1.9) to (IP 1.11) impose binary restrictions on decision variables.

## 3 Solution Approach

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

#### 3.1.1 Lagrangean Relaxation

In order to solve the (IP 1), the problem is decomposed into an inner problem and outer problem. The inner problem with constraints (IP 1.1), (IP 1.3) is reformulated and added as a redundant constraint (IP 1.12), as shown below. Note that the optimal solution is not affected if an equation is relaxed into an inequality version.

$$c_i \le \left(y_i + q_i\right)M + \left[1 - \left(y_i + q_i\right)\right]\varepsilon \qquad \forall i\in V \qquad \text{(IP 1.1')}$$

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

$$c_i = \varepsilon \text{ or } M \qquad \forall i \in V. \qquad \text{(IP 1.12)}$$

By applying the Lagrangean Relaxation Method [6], the inner problem of (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 inner problem of (IP 1) is transformed. (LR 1) is decomposed into three independent and easily solvable subproblems, as the following shows in more detail.

Subproblem 1.1 (related to decision variable $x_p$):

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

Subject to: (IP 1.8), (IP 1.9).

Dijkstra's shortest path algorithm can be applied to (Sub 1.1) since the node weight $\mu^3_{wi}$ 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 $y_i$):

$$Z_{\text{Sub 1.2}}(\mu^1, \mu^4) = \min \sum_{i \in V} \left[ \mu^1_i (\varepsilon - M) + \mu^4 a_i (b_i + d_i) \right] y_i \quad , \qquad \text{(Sub 1.2)}$$

Subject to: (IP 1.7), (IP 1.10).

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

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

$$Z_{\text{Sub 1.3}}(\mu^1, \mu^2, \mu^3) = \min \sum_{i \in V} \left\{ \left[ \mu^1_i - \sum_{w \in W} \sum_{p \in P_w} \mu^2_{wp} \delta_{pi} + \sum_{w \in W} \left( \frac{-1}{|W| \times M} + \sum_{p \in P_w} \mu^2_{wp} \right) t_{wi} \right] c_i - \sum_{w \in W} \mu^3_{wi} t_{wi} \right\}, \qquad \text{(Sub 1.3)}$$

Subject to:

$$t_{wi} = 0 \text{ or } 1 \qquad \forall i \in V,\ w \in W \qquad \text{(Sub 1.3.1)}$$

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

In (Sub 1.3), both decision variable $t_{wi}$ 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 [7], 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.

The dual problem can be solved in many ways; here the subgradient method is adopted to solve the dual problem.

### 3.1.2 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 inner 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 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.

## 3.2 Solution Approach for Solving (IP 1)

The result of the inner 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 intentional attacks. Therefore, the outcome of the inner problem can be used as the input of the outer problem for developing a better budget allocation policy. 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 inner 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, 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 value), 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.

# 4 Computational Experiments

## 4.1 Experiment Environment

For the proposed Lagrangean Relaxation algorithm, two simple algorithms were 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.

## 4.2 Computational Experiment of (IP 1)

To prove the effectiveness of the Lagrangean Relaxation algorithm and the proposed heuristic, two simple algorithms were developed, introduced in Table 2 and Table 3 respectively for comparison purposes.

**Table 2.** $SA_1$ Algorithm

```
//initialization
total_attack_cost = 0;
sort all nodes by their attack cost in ascending order;
for each node i { //already sorted
        if ( total_attack_cost + attack_cost _i <= TOTAL_ATTACK_BUDGET
        AND (node i is not compromised OR compromised but repaired)){
                compromise node i;
                total_attack_cost += attack_cost_i;
        }
}
calculate DOD;
return DOD;
```

**Table 3.** $SA_2$ Algorithm

```
//initialization
total_attack_cost = 0;
sort all nodes by their node degree in descending order;
for each node i { //already sorted
        if ( total_attack_cost + attack_cost _i <= TOTAL_ATTACK_BUDGET
        AND (node i is not compromised OR compromised but repaired)){
                compromise node i;
                total_attack_cost += attack_cost_i;
        }
}
calculate DOD;
return DOD;
```

### 4.3 Experiment Results of the Inner Problem of (IP 1)

Fig. 1 compares the performance between the proposed Lagrangean Relaxation algorithm and two simple algorithms ($SA_1$ and $SA_2$); also, the gap between LR (UB) and LB is presented. Each point on the chart represents the DOD value of different node numbers and topologies under degree-based initial budget allocation strategy. The proposed LR algorithm has a better performance than the two competitive algorithms: it always causes the lowest network survivability (highest DOD value) in all network topologies and sizes. Although the gaps between LR and LB are generally small (about 12% on average), when the network size grows, the gap becomes larger, especially in the grid network case. The performance of the simple algorithm 2 ($SA_2$) is better than that of simple algorithm 1 ($SA_1$). The result again shows the importance of allocating more defense resources on vital nodes.

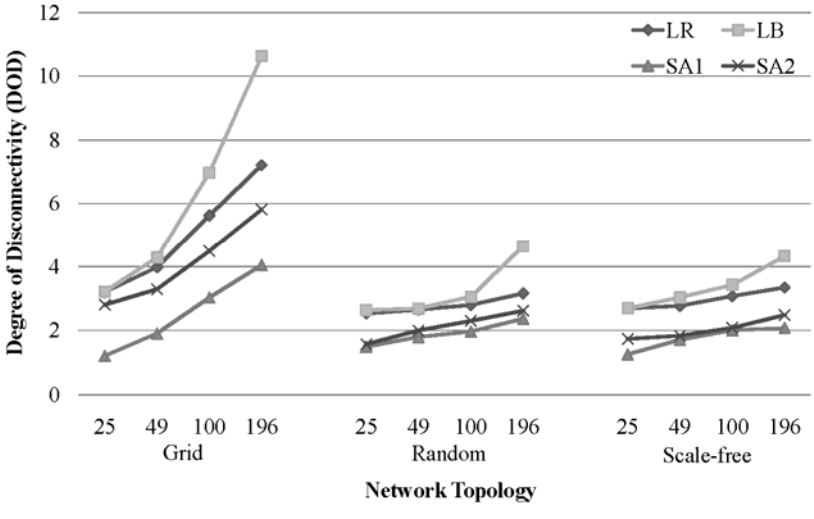


**Fig. 1.** Survivability of Different Network Sizes and Topologies

### 4.4 Experiment Result of (IP 1)

Fig. 2 illustrates the survivability (i.e., DOD value) of the network under different topologies, node numbers and initial budget allocation policies. Networks with a degree-based initial budget allocation strategy are more robust compared to those with a uniform strategy, and the damage of the network was less under the same attack and defense budgets. This finding suggests that the defense resources should be allotted according to the importance of each node in the network. 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 considerably. Random networks have higher survivability compared with scale-free networks because nodes in random networks are arbitrarily connected to each other rather than attached to nodes with a higher degree and therefore have lower damage when encounter intentional attacks.

The survivability of different network topologies, node numbers, and budget reallocation strategies is demonstrated in Fig. 2. From the above bar chart, the subgradient-like heuristic and both budget reallocation strategies perform well in all conditions (approximately 20% improvement on average), and the degree-based budget reallocation strategy is better than the uniform reallocation. However, the difference between two budget allocation strategies is not significant. One possible reason is that in the proposed heuristic, the extracted defense resources are allotted to compromised nodes according to certain strategies. These nodes selected by the attacker already indicate which nodes are more important, although node degree is related to the importance of nodes. As a result, the gap between the two strategies is small.

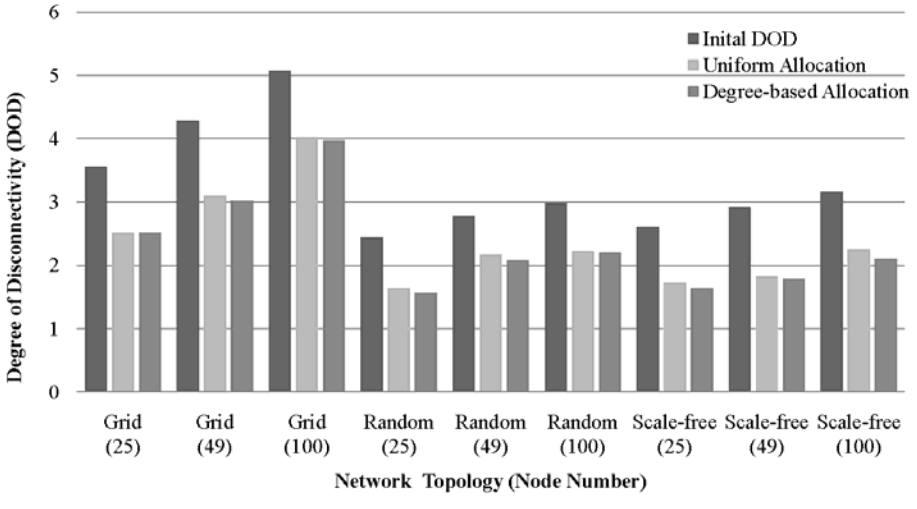


**Fig. 2.** Survivability of Different Networks and Reallocation Strategies

## 5 Conclusion

In this paper, a generic mathematical programming model that can be used for solving network attack-defense problem is proposed 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 thus enhancing their defense capability. In this context, the Degree of Disconnectivity (DOD) is used to measure the damage of the network. The inner problem is solved by a Lagrangean Relaxation-based algorithm, and the solution to min-max 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. The proposed Lagrangean Relaxation-based algorithm and subgradient-like heuristic have been proved to be 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 has been examined. Their survivability can be significantly improved by adjusting the defense budget allocation. From the outcomes of the experiments, the defense resources should be allocated according to the importance of nodes. Moreover, the attack and defense scenarios take rounds to the end. As a result, the number of rounds, e.g., from 1 to *N*, could be further expanded.

**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. Symantec.: Symantec Global Internet Security Threat Report Trends for 2009, Symantec Corporation, vol. XV (April 2010)
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. Jiang, W., Fang, B.X., Zhang, H.L., Tian, Z.H.: A Game Theoretic Method for Decision and Analysis of the Optimal Active Defense Strategy. In: The International Conference on Computational Intelligence and Security, pp. 819–823 (2007)
4. Lin, F.Y.S., Tsang, P.H., Chen, P.Y., Chen, H.T.: Maximization of Network Robustness Considering the Effect of Escalation and Accumulated Experience of Intelligent Attackers. In: The 15th World Multi-Conference on Systemics, Cybernetics and Informatics (July 2009)
5. Lin, F.Y.S., Yen, H.H., Chen, P.Y., Wen, Y.F.: An Evaluation of Network Survivability Considering Degree of Disconnectivity. In: The 6th International Conference on Hybrid Artificial Intelligence Systems (May 2011)
6. Fisher, M.L.: The Lagrangian Relaxation Method for Solving Integer Programming Problems. Management Science 27(1), 1–18 (1981)
7. Geoffrion, M.: Lagrangean Relaxation and its Use in Integer Programming. Mathematical Programming Study 2, 82–114 (1974)