Resource Allocation Strategies to Maximize Network Survivability Considering of Average DOD

Frank Yeong-Sung Lin[1], Pei-Yu Chen[2], Quen-Ting Chen[3]

Department of Information Management, National Taiwan University[123] Taipei, Taiwan, R.O.C.

CyberTrust Technology Institute, Institute for Information Industry[2] Taipei, Taiwan, R.O.C.

yslin@im.ntu.edu.tw, d96006@im.ntu.edu.tw, r98043@im.ntu.edu.tw

Abstract. In this paper, an innovative metric called Average Degree of Disconnectivity (Average DOD) is proposed. The Average DOD combining the concept of the probability calculated by contest success function with the DOD metric would be used to evaluate the damage degree of network. The larger value of the Average DOD, the more damage degree of the network would be. An attack-defense scenario as a mathematical model would be used to support network operators to predict that all the likelihood strategies both cyber attacker and network defender would take. The attacker could use the attack resources to launch attack on the nodes of network. On the other hand, the network defender allocates existed resources of defender to protect survival nodes of network. In the process of problem solving, the "gradient method" and "game theory" would be adopted to find the optimal resource allocation strategies for both cyber attacker and network defender.

Keywords: Average Degree of Disconnectivity, Average DOD, Contest Success Function, Gradient Method, Network Survivability, Optimization, Game Theory, Resource Allocation, Network Attack and Defense

1. Introduction

In the past, the security state of systems or infrastructures was classified in terms of two states: safe or compromised [1]. However, the network often faces many situations such as natural disasters, malicious attacks, and random error conditions which could result in different outcomes. Network security professionals must ensure the available and continuous services. Therefore, the binary concept is insufficient to

[2] Correspondence should be sent to d96006@im.ntu.edu.tw.

describe a system's state. As a result, more and more researchers studied the issue of network survivability.

Traditionally, when measuring the survivability of a network, some researchers use the concept of Greatest Residual Region (GRR, or the largest component in remaining network). After partial of the network are disabled by attacks or failures, GRR is then used to assess the impact in terms of the proportion of nodes in the largest region of a broken network. However, this metric is insufficient to describe the sensibility of partial dysfunctional network yet.

In [2], this paper proposed another metric of the network survivability which is called the Degree of Disconnectivity (DOD). The DOD metric could be used to evaluate the partial damage degree of network. The calculated value seems to be effectively represented the damage degree of network. However, there is still a disadvantage to DOD, which has assumed that the attacker would launch the attack either successfully or unsuccessfully. This assumption is limited, since the attack might not be 100% successful or unsuccessful. As a result, in this paper, an evolved DOD metric is proposed, which is narrated the average probability of each attack and defense case, the more details is explained in the next sections.

Moreover, the interaction between cyber attackers and network defenders is similar to information warfare. The cyber attackers expect to minimize the degree of network survivability. On the other hand, the network defenders always expect to maximize the degree of network survivability. This attack-defense situation would become a min-max or max-min problem. The researchers solve this kind of attack-defense problem of network security by mathematical programming approach, such as game theory [3], Lagrangean Relaxation Method. [4] is considering one or several important nodes or systems in the topology. However, this assumption restricts to evaluate the generalize situation in the network. To enhance or reduce network survivability, both network defender and cyber attacker usually need to invest the fixed number of resources in the network. In the end, it would be a significant issue about how to efficiently allocate resources to the network both cyber attacker and network defender. The more details are described in the following.

2. Problem Formulation and Notations

The DOD metric, proposed in [3], assumed that the cyber attacker launches the attack either successfully or unsuccessfully, but this assumption is limited to describe the attack result that might not be completely compromised, which is a disadvantage to this metric. To improve this problem, we propose a new metric of the network survivability which is called Average DOD. Average DOD combined the concept of probability calculated by the contest success function [5] with the DOD metric. The definition of contest success function is showed in Table 1 and equation (1).

According to the definition of contest success function, if the attacker allocated more resource on a node, the more probability of the attacker could compromise the node. Similarly, if the defender allocated more resource on a node, the more

probability of the defender could protect the node. Besides, *m* is a parameter which describes the intensity of the contest [6]. Here, we demonstrate an example to describe Average DOD. In a network, each network configuration would have a probability determined by the attack success or failure probability of each node; the method to calculate the probability of each kind of network configuration would be to multiply the attack success or failure probability of each node. If all the nodes of network are compromised by the attacker, the probability of this network configuration would be $\prod_{i=1}^{9} S_i$ (Where S_i means the attack success probability of the node *i*). However, if all the nodes of network are still functional, the probability of this network configuration would be $\prod_{i=1}^{9} (1-S_i)$. Furthermore, each kind of network configuration would lead to different damage degree of network. The Degree of Disconnectivity (DOD) could be adopted to measure the damage degree of network. If all the nodes of network are still functional, the DOD value would be 0.

The concept of expectation value the predicted mean value of the result of an experiment of statistics would be adopted to evaluate average damage degree of whole network. The calculated expectation value is defined as the Average DOD here. The larger number of the Average DOD value is, the more damage degree of the network would be. Meanwhile, the Average DOD value is influenced by the attack success probability calculated by the resource allocation of both cyber attacker and network defender. Therefore, the Average DOD value could be adopted to measure the damage degree of the network and find the optimal resource allocation in each node for both cyber attacker and network defender.

Table 1. Given Parameters and Decision Variables

Given parameter Notation	Description
$S_i(T_i, t_i))$	the attack successful probability on node *i*
T_i	the attack resource allocated on node *i*
t_i	the defensive resource allocated on node *i*
m	contest intensity

$$S_i(T_i,t_i) = \frac{T_i^m}{T_i^m + t_i^m}, where \frac{\partial S}{\partial T} \geq 0, \frac{\partial S}{\partial t} \geq 0, m \geq 0 \quad (1)$$

2.1 Problem Description

Cyber attacker and network defender are always limited by the invested resources. How to make the decision to efficiently allocate resources to each node is an extremely significant issue for both cyber attacker and network defender. We proposed a new mathematical model to support both cyber attack and network

defender to make the optimal decision. In this model, the damage degree of network is evaluated by the Average DOD value.

In this attack-defense problem, cyber attacker and network defender are through some strategies to attend their goals. From the perspective of network defender, the defender is usually looking forward to minimizing the damage degree of network. On the other hand, the cyber attacker expects to maximize the damage degree of network. Both of them could take some strategies to attend their goal. It is usually constrained by the allocated resources. The cyber attacker needs to determine how to allocate resources to attack targeted network. Besides, the attacker could accumulate some experience that could help the attacker having higher probability to compromise network in next time.

2.2 Problem Formulation

The above problem is formulated as a maximization mathematical model as follows. Note that the network discussed here is at the AS level. Both the attacker and the defender have complete information about the targeted network topology and the budget allocation is assumed. 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 2.

Table 2. Given Parameters and Decision Variables

Given parameter	
Notation	Description
V	Index set of nodes
$\hat{A}$	Total budget of attacker
$\hat{B}$	Total budget of defender
θ_i	Existing defense resource allocated on node i, where $i \in V$
d_{ri}	The discount rate of defender reallocate resources on node i in round r, where $i \in V$ and $r \in R$
Decision variable	
Notation	Description
$\vec{a}$	Attacker's budget allocation, which is a vector of attack cost a_1, a_2 to a_i, where $i \in V$
$\vec{b}$	Defender's budget allocation, which is a vector of defense cost a_1, a_2 to a_i, where $i \in V$
a_i	Attacker's budget allocation on node i, where $i \in V$
b_i	Defender's budget allocation on node i, where $i \in V$
$\bar{D}(\vec{a},\vec{b})$	The Average DOD, which is considering under attacker's and defender's budget allocation are $\vec{a}$ and $\vec{b}$

The problem is then formulated as the following problem:

Objective function:

$$\min_{\vec{b}} \max_{\vec{a}} \bar{D}(\vec{a}, \vec{b}), \quad \text{(IP 1)}$$

Subject to:

$$\sum_{i \in V} b_i \le \hat{B} + \sum_{i \in V} \theta_i d_i \quad \text{(IP 1.1)}$$

$$\sum_{i \in V} a_i \le \hat{A}. \quad \text{(IP 1.2)}$$

The objective function is to minimize the maximum the Average DOD. IP 1.1 describes the sum of the allocated defense budgets in each node should not exceed the sum of the new allocated and reallocated budgets in that round. IP 1.2 calculates the sum of the allocated attack budgets in each node should not exceed the attack budgets in that round.

3. Solution Approach

Here, how to optimize resource allocation in each node for both cyber attacker and network defender and to evaluate damage degree of network by the Average DOD value would be introduced. The gradient method [7] is used to calculate the Average DOD value and to find the optimal resource allocation strategy in each node for both cyber attacker and network defender. The detailed solution procedure would be discussed in first section. In addition, the concept of gradient method and the detailed method to calculate the Average DOD value would be introduced in second part. Finally, the time complexity of the solution approach would be analyzed.

3.1 Gradient Method

The gradient method is a general framework used to solve the optimization problems what is to maximize or minimize functions of continuous parameters. This problem is a min-max formulation and both cyber attacker and network defender are assumed that they could allocate continuous resources in each node. Here, the gradient method is adopted to solve this problem.

The gradient method usually could be categorized into two types, one is gradient descent and the other one is gradient ascent [9]. The gradient descent method could be used to solve the optimal minimization problem. On the other hand, the optimal maximization problem could be solved by the gradient ascent method. The concept of gradient descent and gradient ascent is extremely similar, so both of them could adopt the following algorithm: The detailed process flow of the gradient method is also described in Table 3.

Table 3: The Algorithm of the Gradient Method

Step1.Get a start point
Step2.Determine a positive or negative direction
Step3.Determine a step size
Step4.Repeat
a. Find the most impact of all dimensions
b. Move a step of the most of all dimensions
c. Update the start point
Until a stop criterion is satisfied

3.2 Using Game Theory to Find the Optimal Solution

In this paper both cyber attacker and network defender need to determine how to efficiently allocate resources simultaneously in each node. This problem could be viewed as a simultaneous or imperfect information game. In addition, both cyber attacker and network defender have complete information about the strategies. Hence, this problem also could be regarded as a complete information game. Here, two players (cyber attacker and network defender), zero-sum, complete and imperfect information game would be used to solve this problem.

The representation of game theory normally has two types, one is the extensive form and the other one is the normal form. The normal form would be introduced to solve this problem in this model, which is represented by a matrix which shows the players, strategies, and payoff values. For example, two players, one is on the first column and the other one is on the first row of the matrix, own lots of different strategies, respectively. For example, both two players have five different strategies (S_{11} to S_{15} and S_{21} to S_{25}). The combination of two players with different strategies would produce 25 (U_{11} to U_{55}) different results (the Average DOD value).

Both cyber attacker and network defender have different strategies about the percentage resource allocation in each stage. In addition, the results of each kind of percentage resource allocation of each player would be calculated by the Average DOD. The solution approach of the complete and imperfect information game would be introduced in the following. Generally, the solution procedure of the complete and imperfect information game is shown as following.

Step1. Dominant strategy eliminating. The dominant strategy means that no matter what kind of strategy that the opponent to take is better than other strategies.

Step2. If only one strategy is left of each player, it would be the optimal strategy. Otherwise, go to step 3.

Step3. Using the minmax strategy to find the optimal strategy of each player. If minmax strategy still could not find the optimal strategy, go to step4.

Step4. Using the mixed strategy (Linear programming) to find the optimal strategy of each player.

3.3 Time Complexity Analysis

The time complexity of the algorithm quantifies the amount of time taken by an algorithm to run as a function of the size of the input to the problem. It would influence the efficiency of the proposed algorithm. To calculate the Average DOD value, the gradient method would be used to find the optimal resource allocation in each node. In addition, the DOD value would be used to measure the damage degree of each configuration. The time complexity of the gradient method would be $O(mV)$, since the impact degree of each node would be checked in each round. (Where m is the maximum number of the checked round and V is the node number in the network) In addition, the time complexity of the DOD value of each configuration would be $O(WV^2)$ (Where W is the number of the O-D pair), because the broken nodes of each O-D pair are needed to be checked. The checked method would adopt the Dijkstra's shortest path algorithm, so the time complexity would be $O(V^2)$. However, to compute the Average DOD value, the 2^V different kinds of network configuration would need to be considered. The time complexity to compute the Average DOD value would be $O(2^V WV^2)$. As a result, once the number of node is too huge, it must take much time to compute the Average DOD value.

4. Computational Experiments

Because of the complexity of this problem, the number of network node considered in the experiments is 9. In addition, three kinds of network topology are considered, the grid network (GD), the random network (RD), and the scale-free network (SF). The feature of the GD is really regular network. Besides, the SF is a kind of network whose degree distribution follows a power law. Finally, the RD is randomly connected with other nodes. Three kinds of network topology adopted to take the experiments in this paper are demonstrated in.

4.1 Experiment Environment

To find the optimal resource allocation strategy for both cyber attacker and network defender, there is something needing to be determined firstly. The resource reallocation policy of the defender would be that the defense resources of each stage would not be accumulated (RR1) and node recovery policy of the defender would be that all the compromised nodes would not be recovered (NR2). In addition, the accumulated experience of the attacker would not be considered in this experiment (NAE). The experiment results would be demonstrated in Table 4.

Table 4. The Experiment under Different Topology

Network Topology	Grid	Random	Scale-free
Average DOD	1.49871	1.49876	1.49886
Strategy of Attacker	20	20	20
Strategy of Defender	20	20	20

5. Conclusion

In this paper, we first evaluate the network survivability with a new proposed survivability metric called Average DOD, which is more sensible to respond the largest connected component of the network. The metric combined the concept of the probability calculated by the contest success function with the DOD metric would be as a new tool to evaluate network survivability.

In addition, an efficient attack-defense scenario is formulated. Considering the scenario of both cyber attacker and network defender utilize their resource and in each node are solved. The model is demonstrated under 3 different topologies and discussed. It seems that the grid network is fully connected is more robust among these topologies. However, considering of the interaction of attacker and defender, the model shall improve to solve multi-stage attack-defense issue. Moreover, some advanced technology, such as parallel processing system, could be considered to be adopted to improve efficiency in this model in the future.

Acknowledgments. This research was supported by the National Science Council of Taiwan, Republic of China, under grant NSC-100-2221-E-002-174.

References

1. 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)
2. Lin,F.Y.S, Yen, H.H., Chen, P.Y., and Wen, Y.F.: Evaluation of Network Survivability Considering Degree of Disconnectivity. Lecture Notes in Artificial Intelligence, Vol. 6678, pp. 51-58 (2011)
3. Jiang, W., Fang, B.X., Zhang, H.l., and Tian, Z.H.: Optimal Network Security Strengthening Using Attack-Defense Game Model. Sixth International Conference on Information Technology: New Generations (2009)
4. Lin, Y.S., Tsang, P.H., Chen, C.H., Tseng, C.L., and Lin, Y.L.: Evaluation of Network Robustness for Given Defense Resource Allocation Strategies. Proceedings of the First International Conference on Availability, Reliability and Security (2006)
5. Skaperdas, S.: Contest Success Functions. Economic Theory (1996)
6. Peng, R., Levitin, G., Xie, M., and Ng, S.H.: Defending simple series and parallel systems with imperfect false targets. Reliability Engineering & System Safety, Vol. 95, Issue 6, pp. 679-688, June (2010)
7. Hassoun, H.: Fundamentals of Artificial Neural Networks. MIT Press (1995)