Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2013, Article ID 207141, 9 pages
http://dx.doi.org/10.1155/2013/207141

Research Article

Recovery and Resource Allocation Strategies to Maximize Mobile Network Survivability by Using Game Theories and Optimization Techniques

Pei-Yu Chen[1,2] **and Frank Yeong-Sung Lin**[1]

[1] *Department of Information Management, National Taiwan University, Taipei 106, Taiwan*
[2] *CyberTrust Technology Institute, Institute for Information Industry, Taipei 106, Taiwan*

Correspondence should be addressed to Pei-Yu Chen; d96006@im.ntu.edu.tw

Received 19 April 2013; Revised 2 August 2013; Accepted 6 August 2013

Academic Editor: Anyi Chen

With more and more mobile device users, an increasingly important and critical issue is how to efficiently evaluate mobile network survivability. In this paper, a novel metric called Average Degree of Disconnectivity (Average DOD) is proposed, in which the concept of probability is calculated by the contest success function. The DOD metric is used to evaluate the damage degree of the network, where the larger the value of the Average DOD, the more the damage degree of the network. A multiround network attack-defense scenario as a mathematical model is used to support network operators to predict all the strategies both cyber attacker and network defender would likely take. In addition, the Average DOD would be used to evaluate the damage degree of the network. In each round, the attacker could use the attack resources to launch attacks on the nodes of the target network. Meanwhile, the network defender could reallocate its existing resources to recover compromised nodes and allocate defense resources to protect the survival nodes of the network. In the approach to solving this problem, the "gradient method" and "game theory" are adopted to find the optimal resource allocation strategies for both the cyber attacker and mobile network defender.

1. Introduction

Network security problems are often challenging given that the growing complexity and interconnected nature of IT systems lead to a limited capability of observation and control. This is especially the case for mobile networks, in which the cycle time of decision making is reduced from enterprise having access to real-time data. As the enterprise systems are widely relayed on mobile networks, the services are disrupted whenever the network suffers a disruption, such as from physical damage or malicious attacks. Compared to wired network system, mobile network systems are much more vulnerable to security problems [1]. For example, insofar as there is not a precisely defined physical boundary of the mobile network, as soon as an adversary comes in the radio range of a node, he can communicate with that node and thus launch a malicious attack on it [2]; these attacks include eavesdropping, phishing, war driving, and denial of service (DoS) attack [3]. As a result, there is a pressing need to design countermeasures for network attacks. Moreover, it is critical for an enterprise to evaluate and allocate its resources to protect it assets, as well as to be able to continuously provide service.

In the past, the security state of systems or infrastructures was classified in terms of two states: safe or compromised [4]. However, networks often face many situations, such as natural disasters, malicious attacks, and random error conditions, which can lead to different outcomes. Network security professionals must also ensure the availability and continuity of services. For these reasons, the binary concept of safe/compromised is insufficient to describe a system's state, with an increasing number of researchers focusing on the issue of network survivability.

There are many quantitative analyses of network survivability, such as connectivity. In [5], the definition of network connectivity is the minimum number of links or

Table 1: The summary of different DOD metrics.

No.	Name	Concept	Original
1	Degree of disconnectivity (DOD)	The DOD value can be explained as measuring the average numbers of the broken nodes in any O-D pair of the network.	[7]
2	Longest damaged path (LDP-DOD)	The LDP-DOD used to measure the damage degree of the network finds the most damaged O-D pair among all the O-D pairs of the network.	[7]
3	Minimal recovery node (MRN-DOD)	The MRN-DOD discovers the minimal numbers of broken nodes that are needed to repair and reconnect all the O-D pairs of the network.	[7]
4	Partial DOD (P-DOD)	Since the important degree of the different network areas is usually unequal, the network defender could assign different DOD requirements to different areas of the network, that is, the P-DOD.	[8]
5	Weight DOD (W-DOD)	Since the significance degree of each O-D pair can be diversified, the network defender can assign different weights to each O-D pair, that is, the W-DOD.	[8]

nodes that must be recovered from a given O-D (original-destination) pair. In general, the greater the number of links or nodes to be recovered to disconnect an O-D pair, the higher the survivability of the network. Thus, there are many studies adopting the concept of network connectivity to do quantitative analyses of network survivability. In [6], the researchers proposed using the network connectivity to measure the network survivability under intentional attacks and random disasters. Furthermore, the authors in [7] employing network connectivity for a quantitative analysis of network survivability proposed a survivability metric called the degree of disconnectivity (DOD) to estimate the residual network survivability after a malicious attack or any network crash incident.

To date, there have been several proposed degree of disconnectivity (DOD) metrics to evaluate network survivability. In [7], two other metrics called longest damaged path (LDP-DOD) and minimal recovery node (MRN-DOD) were proposed. Unlike the DOD metric, the LDP-DOD is used to measure the damage degree of the network by finding the most damaged O-D pairs among all the O-D pairs of the network. Therefore, the larger value of the LDP-DOD could be used to represent the most damage that a network could endure. On the other hand, the MRN-DOD discovers the minimal number of broken nodes that is necessary to be recovered in order to reconnect all the O-D pairs of the network.

In [8], the partial DOD (P-DOD) and weight DOD (W-DOD) metrics were adopted to evaluate network survivability. Because the important degree of the different network areas is usually unequal, the network defender could assign different DOD requirements according to its area, which is defined as the P-DOD. The network defender could then use the P-DOD value to determine the order to recover compromised nodes. Moreover, the significant degree of each O-D pair could be determined by diversity, where the network defender could assign different weights to each O-D pair, that is, the W-DOD. If the more significant O-D pair is cut to increase the degree of damage to the network, the W-DOD will clearly increase. The above DOD metrics are summarized in Table 1.

The DOD metric proposed in [7] assumed that the cyber attacker would launch the attack either successfully or unsuccessfully. However, this assumption is limited since the attack might not be perfectly successful or even completely unsuccessful. Motivated by previous works, the Average Degree of Disconnectivity (Average DOD) is developed to carry out a quantitative analysis of network survivability, combining the concept of probability as calculated by the contest success function [9] with the DOD metric, thus becoming the Average DOD. When the number of the Average DOD value is large, the damage to the network will be greater.

According to the allocated resources on each node from both cyber attacker and network defender, the contest success function is adopted to calculate the attack success probability of each node. The attack success probability of each node is calculated based on the concept of contest success function, where S_i represents the attack success probability of node i:

$$S_i\left(T_i, t_i\right) = \frac{T_i}{T_i + t_i} = \frac{1}{1 + t_i/T_i}. \tag{1}$$

In [7], the DOD metric is used to measure the damage degree of the network, such that the larger the DOD value, the more the damage degree of the network. The definition of the DOD value (D) is as function (2). In this metric, W is the index set of all given critical O-D pairs, while t_{wi} is the shortest path of O-D pairs w, where $w \in W$; $|W|$ is the O-D pair number of W. The total shortest path cost of each O-D is calculated first. Here, c_i represents the transmission cost of a node i, where a large number M represents the link disconnection:

$$D = \frac{\sum_{w \in W} \sum_{i \in V} t_{wi} c_i}{|W| \, M}. \tag{2}$$

The calculated DOD value could be explained as measuring the average numbers of broken nodes in any O-D pair of the network.

Theoretical models at the system level play an increasingly important role in network security and provide a scientific basis for high-level security-related decision making. To enhance or reduce network survivability, both network defender and cyber attacker usually need to invest a limited number of resources in the network. In these models, the decision makers in network security problems play the role

Table 2: Given parameters.

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

of either the attacker or the defender. They often have conflicting goals, in that a cyber attacker attempts to breach the security of the system to disrupt or cause damage to network services, whereas a defender takes appropriate measures or strategies to enhance the system security design or response. Traditionally, although the attack-defense resource allocation problem is usually discussed for only one round [7, 10–12], the interaction frequency between cyber attacker and network defender is usually more than one time in real world. For this reason, several researchers are beginning to discuss multiround attack-defense resource allocation issues [8, 13, 14]. However, most of the existing solutions to multiround attack-defense resource allocation are still not suitable to the field of the network security, because they almost solely focus on the attack-defense problem of the parallel systems [13, 14] and serial systems [15]. In reality, the topology of the network is usually more complicated than the topology of the parallel, serial, or even serial-parallel systems. Thus, a new multiround attack-defense model to solve the resource allocation problem for both cyber attackers and network defenders is needed and developed in this study.

2. Problem Formulation

2.1. The Average DOD. The DOD metric proposed in [12] assumed that the cyber attacker launches the attack either successfully or unsuccessfully, but this binary assumption is limited in its inability to describe attack results that are neither perfectly successful nor unsuccessful. Therefore, the concept of the probability calculated by contest success function combined with the DOD metric was forwarded as a new survivability metric called the Average DOD. According to the allocated resources on each node of both cyber attacker and network defender, the contest success function would be adopted to calculate the attack success probability of each node. The attack success probability of each node is demonstrated, where S_i represents the attack success probability of node i. After each attack-defense interaction, there are 2^V configurations of a given network, where V means the total number of network nodes, and j is the configuration index. For example, in Table 2, the total number of possible configurations of a network is 2^9, and the configuration index j is $1, 2, \ldots, 512$.

In addition, each possible network configuration has a probability P_j, which is related to the safe or compromised state of the configuration. This probability is determined by the attack success probability S_i of each node. For example, if a 9-node network is completely 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 the 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 a different damage degree of the network. The degree of disconnectivity (DOD) having been introduced in the preceding part can be adopted to measure the damage degree of network. For example, if all the nodes of the network are still functional, the DOD value would be 0. The probability and DOD value of each kind of network configuration are calculated with the concept of expectation value. The predicted mean value of the result of a statistical experiment would be adopted to evaluate the damage degree of the whole network. The calculated expectation value is defined as the Average DOD $\overline{D}$ here, which is shown in (3):

$$\overline{D} = \sum_{j=1}^{j\in J} D_j P_j. \tag{3}$$

The Average DOD value is influenced by the attack success probability calculated by the resource allocation of both the cyber attacker and network defender. Therefore, the Average DOD value could be induced from the damage degree of the network. The calculation of an Average DOD 9-node-network example is demonstrated in Table 3. In this example, probability P_1 of configuration 1 is $\prod_{i=1}^{9}(1 - S_i)$, since all nodes of this configuration are functional. In (2), the DOD value is the recovered nodes in any given compromised O-D pair; there is no compromised node in configuration 1. Therefore, the DOD value D_1 here is 0.

2.2. Problem Description. In this attack-defense problem, both cyber attacker and network defender employ certain strategies to attain their goals. From the perspective of the network defender, the defender usually aims to minimize the damage degree of the target mobile network. On the other hand, the cyber attacker hopes to maximize the damage degree of the network. However, given that both 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. Meanwhile, in the real world, it is impossible that there will only be a one-time interaction between the cyber attacker and network defender, and as such, a multiround attack-defense problem in this mathematical model needs to be considered. A mathematical model to support both cyber attacker and network defender in making the optimal decision is thus developed to solve this problem.

In this model, the damage degree of the mobile network can be evaluated by the Average DOD value. The cyber attacker needs to determine how to allocate resources to attack the targeted network, since the strategies of both cyber attackers and network defenders are usually constrained by the allocated resources in each round. On the other hand, the network defender can choose to reallocate the existing resources in the mobile network, but the problem regarding

Table 3: Calculation of an example of the Average DOD value.

Configuration j	Network configuration*	Probability P_j of configuration j	DOD value D_j on configuration j	Probability $P_j \times$ DOD value D_j
1	1, 2, 3, 4, 5, 6, 7, 8, 9	$\prod_{i=1}^{n}(1-S_i)$	D_1	0
2	$\underline{1}$, 2, 3, 4, 5, 6, 7, 8, 9	$S_1\prod_{i=2}^{n}(1-S_i)$	D_2	$D_2S_1\prod_{i=2}^{v}(1-S_i)$
3	1, $\underline{2}$, 3, 4, 5, 6, 7, 8, 9	$(1-S_1)\,S_2\prod_{i=3}^{n}(1-S_i)$	D_3	$D_3\,(1-S_1)\,S_2\prod_{i=3}^{v}(1-S_i)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
512	$\underline{1}$, $\underline{2}$, $\underline{3}$, $\underline{4}$, $\underline{5}$, $\underline{6}$, $\underline{7}$, $\underline{8}$, $\underline{9}$	$\prod_{i=1}^{n}S_i$	D_4	$D_4\prod_{i=1}^{n}S_i$

*$\underline{i}$ means the node i is compromised in configuration j.

the discount factor of those reallocated resources also needs to be considered here. As a result, the total number of resources that the defender could use would be the newly allocated and reallocated resources in each round, and those resources could be used to recover the compromised nodes and to protect the mobile network survival nodes.

In the following, the notations of given parameter and decision variable in this model are listed in Tables 4 and 5.

Using the above notations of the given parameter and decision variable, the problem is formulated as follows:

Objective Function

$$\min_{\overrightarrow{b}_r}\max_{\overrightarrow{a}_r} \quad \sum_{r\in R} w_r \overline{D}\left(\overrightarrow{a_r},\overrightarrow{b_r}\right) \qquad \text{(IP 1)}$$

$$\text{subject to} \quad \sum_{i\in V} b_{ri} + \sum_{i\in V} e_{ri} z_{ri} \le B_r + \sum_{i\in V}\theta_i d_{ri} \quad r\in R, \qquad \text{(IP 1.1)}$$

$$\sum_{i\in V} a_{ri} \le A_r \quad r\in R, \qquad \text{(IP 1.2)}$$

$$\sum_{r\in R} A_r \le \widehat{A}, \qquad \text{(IP 1.3)}$$

$$\sum_{r\in R} B_r \le \widehat{B}. \qquad \text{(IP 1.4)}$$

Explanation of the Objective Function

(IP 1) The purpose of the objective function is to minimize both the maximum sum of the product of the Average DOD and the different weight in each round.

Explanation of the Constraint Function

(IP 1.1) The sum of the allocated defense budgets in each node and repaired cost of the compromised nodes should not exceed the sum of the new allocated and reallocated budgets in that round.

(IP 1.2) The sum of the allocated attack budgets in each node should not exceed the attack budgets in that round.

(IP 1.3) The sum of the allocated defense budgets in each round should not exceed the total budget of the defender.

Table 4: Given parameter.

Notation	Description
V	Index set of nodes
R	Index set of rounds in the attack and defense actions
$\widehat{A}$	Total budget of attacker
$\widehat{B}$	Total budget of defender
w_r	The weight of the Average DOD in round r, where $r \in R$
θ_i	Existing defense resources allocated on node i, where $i \in V$
e_{ri}	Repair cost of defender when node i is dysfunctional in round r, where $i \in V$ and $r \in R$
d_{ri}	The discount rate of defender reallocate resources on node i in round r, where $i \in V$ and $r \in R$

Table 5: Decision variable.

Notation	Description
$\overrightarrow{a}_r$	Attacker's budget allocation, which is a vector of attack cost a_{r1}, a_{r2} to a_{ri} in round r, where $i \in V$ and $r \in R$
$\overrightarrow{b}_r$	Defender's budget allocation, which is a vector of defense cost b_{r1}, b_{r2} to b_{ri} in round r, where $i \in V$ and $r \in R$
a_{ri}	Attacker's budget allocation on node i in round r, where $i \in V$ and $r \in R$
b_{ri}	Defender's budget allocation on node i in round r, where $i \in V$ and $r \in R$
$\overrightarrow{z}_{ri}$	Defender's node recovery status, which is a vector of repaired status z_{r1}, z_{r2} to z_{ri} in round r, where $i \in V$ and $r \in R$
z_{ri}	1 if node i is repaired by defender in round r, 0 otherwise, where $i \in V$ and $r \in R$
A_r	Attacker's attack budget in round r, where $r \in R$
B_r	Defender's defense budget in round r, where $r \in R$
$\overline{D}\left(\overrightarrow{a}_r, \overrightarrow{b}_r\right)$	The Average DOD among r rounds, considering that it is under the attacker's and defender's budget allocations, is $\overrightarrow{a}_r$ and $\overrightarrow{b}_r$ in round r, where $r \in R$

(IP 1.4) The sum of the allocated attack budgets in each round should not exceed the total budget of the attacker.

3. Solution Approach

Combining game theory with the gradient method is our proposal to solve the optimal resource allocation strategy for both cyber attackers and network defenders. The gradient method 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. Game theory is adopted to find the optimal percentage resource allocation in each round for both cyber attacker and network defender. Further details are presented in the following sections.

3.1. Game Theory. Game theory provides the mathematical tools and models for investigating multi-player strategic decision making, where the rational players compete for restricted resources [9]. This demonstrates the modeling situations of conflict and predicts the behavior of the different players. Security games and their solutions are used not only as a basis for formal decision making and algorithm development but also for predicting attacker and defense behavior [16]. The weakness of traditional network security solutions is that they lack a quantitative decision framework [17]. As a result, researchers are starting to advocate the utilization of game theory approaches. According to the surveys in [18, 19], several game theory approaches have in recent years been proposed to address network security issues. In these frameworks, a network administrator and an attacker can be viewed as two competing players participating in a game, with the added benefit that game theory has the capability of examining hundreds of thousands of possible scenarios before taking the best action.

The primary components of the game theory are player, strategy, payoff, and information. In this model, there are the two players: cyber attacker and network defender; strategy means the possible moves that the players would take; the payoff value means the positive or negative reward to the player from a specific strategy; finally, the information can be categorized into two types, one is complete information, and the other one is perfect information, with the former meaning that every player knows both the strategies and payoff values of all players in the game, and the latter meaning that each player is aware of the moves of all players that have already taken place. The nominal definitions of game theory are summarized in Table 6.

Table 6: The nominal definition of the game theory.

Noun	Definition
Player	A basic entity in a game with making choices for actions
Strategy	The possible motion that the players take
Payoff	The positive or negative reward to the player on the specific strategy
Complete information	Every player knows both the strategies and payoffs of all players in the game
Perfect information	Each player is aware of the moves/strategies of all other players that have already taken place

According to the move order, the game can be categorized into simultaneous games (i.e., static games) and sequential games (i.e., dynamic games). If the all the players move simultaneously, this game is called a simultaneous game, in contrast to a sequential game in which players move in a sequence. And depending on whether the game repeats or not, it will be categorized as either a one-shot or repeat game: the former is a game played only one time, whereas the latter is a game that repeats. The game can be further categorized into zero-sum or nonzero sum game, based on whether the gain or loss of one equals the gain or loss of the other. Finally, according to the definition of the complete and perfect information, game theory is categorized into four types: complete and perfect information games, incomplete and perfect information games, complete and imperfect information games, and incomplete and imperfect information games.

In this paper, since both cyber attacker and network defender need to determine how to efficiently allocate resources simultaneously in each node in each round before the attack-defense game, this problem can be viewed as a simultaneous or imperfect information game. Moreover, insofar as both cyber attacker and network defender have complete information about the strategies and payoff values (the Average DOD value) of each other, this problem is regarded as a complete information game. Therefore, a two-player (cyber attacker and network defender), zero-sum, complete, and imperfect information game is used to solve this problem.

3.2. Gradient Method. The gradient method is a general framework used to resolve the optimization problems of how to maximize or minimize functions of continuous parameters. The proposed model in this paper is a min-max formulation, and both cyber attacker and network defender are assumed to be able to allocate continuous resources to each node. Here, the gradient method is adopted to solve this problem. The gradient method can usually be categorized into two types: one is gradient descent and the other one is gradient ascent [14]. The gradient descent method can be used to solve the optimal minimization problem. To find a local minimum of a function using gradient descent, one takes steps proportional to the negative of the gradient (or of the approximate gradient) of the function at the current point. On the other hand, if instead one takes steps proportional to the positive of the gradient, one approaches a local maximum of that function; the procedure is then known as gradient ascent. The concepts of gradient descent and gradient ascent are extremely similar.

3.3. The Proposed Heuristic. We here describe the detailed process of combining game theory with the gradient method [20] is adopted to find the optimal resource allocation strategy in each node in each round for both cyber attacker and network defender. The gradient method is used to calculate the Average DOD value and to find the optimal resource allocation strategy in each node. Given that how to allocate resources in each round is another issue, game theory is adopted to determine the optimal percentage resource

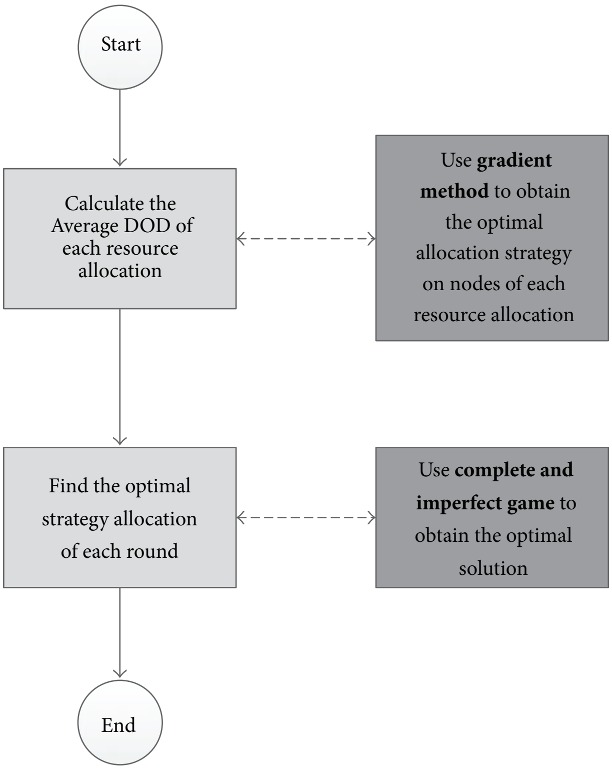

Start
Calculate the Average DOD of each resource allocation
Use **gradient method** to obtain the optimal allocation strategy on nodes of each resource allocation
Find the optimal strategy allocation of each round
Use **complete and imperfect game** to obtain the optimal solution
End

Figure 1: The proposed heuristic.

```
Step 1. an initial point
Step 2. Determine a positive or negative direction
Step 3. Determine a step size
Step 4. Do {
            Find the most impact of all dimensions
            Move a step of the most of all dimensions
            Update an initial point
            } While (a Given Stop Criterion)
```

Algorithm 1: The algorithm of the gradient method.

Table 7: The game matrix.

Strategy		Player 1				
		S_{11}	S_{12}	S_{13}	S_{14}	S_{15}
Player 2	S_{21}	U_{11}	U_{12}	U_{13}	U_{14}	U_{15}
	S_{22}	U_{21}	U_{22}	U_{23}	U_{24}	U_{25}
	S_{23}	U_{31}	U_{32}	U_{33}	U_{34}	U_{35}
	S_{24}	U_{41}	U_{42}	U_{43}	U_{44}	U_{45}
	S_{25}	U_{51}	U_{52}	U_{53}	U_{54}	U_{55}

allocation in each round. The proposed heuristic, with its two major steps, is illustrated in Figure 1.

First, the gradient method is adopted to find an optimal strategy for each node in the given configuration. Initially, it is assumed that the cyber attacker and network defender would evenly allocate their limited resources on each survival node. The cyber attacker has limited resources in each round, and as a result, the cyber attacker would choose the gradient ascent method to maximize damage degree of the network. At the same time, the defense resources are also limited in each round, leading the network defender to use the gradient descent method to find the minimization solution. The detailed process flow of the gradient method is described in Algorithm 1. The selection criterion of the start point is critical, because it influences the quality of the computational efficiency. Moreover, a positive or negative direction results from the maximization or minimization problem. If the maximization problem is to be solved, the positive direction must be chosen. The gradient method adopts a step-by-step method to find the optimization result.

Here, the derivative method is adopted in Step 4 in Algorithm 1, which is designed to find the most important node in the given configuration. The derivative of the Average DOD value is $\widehat{D_i}$, shown in (4), which represents the importance of the node i; r_i represents the resources on node i. The player would move more resources from the less important to the most important nodes. The procedure is stopped when the resource movement is not significant to the Average DOD. After this, the optimal resource allocation strategy for both cyber attacker and network defender in each node is obtained:

$$\widehat{D_i} = \lim_{h \to 0} \frac{\overline{D}(r_i + h) - \overline{D}(r_i)}{h}. \tag{4}$$

The second part of the proposed heuristic involves game theory, which is adopted to efficiently allocate resources in each round for both cyber attacker and network defender. For two players, the strategy of one is represented in a column, whereas the strategy of the other is represented in a row of a matrix. For example, in Table 7, both players have five different strategies (S_{11} to S_{15} and S_{21} to S_{25}), with the combination of the two players' different strategies resulting in 25 (U_{11} to U_{55}) values (the Average DOD values).

In this paper, the cyber attacker and network defender strategies involve different percentages of resource allocation in each round and can be formulated in a matrix. The payoff of all the resource allocation strategies of each participant is calculated by the Average DOD. The analysis of the complete and imperfect information game is conducted via heuristics. The solution procedure of the complete and imperfect information game [18] is shown in the following steps.

Step 1. Dominant strategy elimination, which means that no matter what kind of strategy the opponent takes, it is better than the other strategies.

Step 2. If only one strategy is left for each participant, it is the optimal strategy. Otherwise, go to Step 3.

Step 3. Use the min-max strategy to find the optimal strategy of each participant. If the min-max strategy still cannot find the optimal strategy, go to Step 4.

Step 4. Use the mixed strategy (linear programming) to find the optimal strategy for each participant.

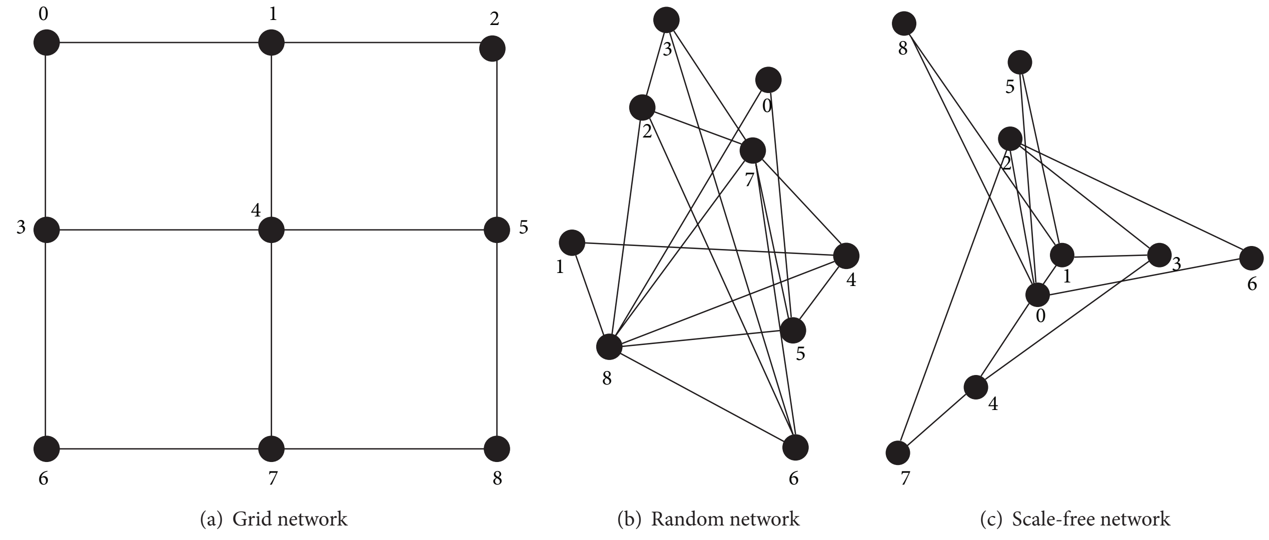


Figure 2: Mobile network topology.

Table 8: Experiment parameters settings.

Parameters	Value
Network topology	(1) Grid, in Figure 2(a) (2) Random, in Figure 2(b) (3) Scale-free, in Figure 2(c)
The number of rounds	2
The number of nodes	9
The number of links	24~36
The total resources of both players	20

4. Computational Experiments

The proposed solution approach is implemented on a PC with AMD Athlon X3 440 CPU 3.00 GHz, 2 GB RAM, and on the OS of MS Windows 7.

The parameters used in the experiments are shown in Table 8.

Because of the complexity of this problem, the number of mobile network nodes considered in the experiments is only 9, and the number of attacker-defender interactions covers only two rounds. Considering the variety of the distributions of mobile nodes, three types of mobile network topologies have been selected to act as attack-defense nodes: the grid network (GD), the scale-free network (SF), and the random network (RD). These three topologies are shown in Figure 2.

Both cyber attacker and network defender would attach a different level of importance to each round, so the different weight of each round would be considered. In this model, given that the weight in the two rounds is (a, b), the first round weight is a, while the second round weight is b. In this paper, we maintain that the importance of these two rounds is equally important, from which we induce the weight to be 0.5.

In this model, three kinds of node recovery policies are proposed. First, in NR1, the defender would choose to recover all the compromised nodes when the resources are sufficient. If the resources are insufficient, they would be used to protect the survival nodes. The second recovery policy is the defender choosing not to recover any compromised node (NR2). Finally, because the defense resources are limited, the third policy determines the order to recover compromised nodes by τ_i in (5) (NR3). Given that e_{ri} is the repair cost of the defender when node i is dysfunctional in round r, where $i \in V$ and $r \in R$, $|W_i|$ is the number of node i on O-D pair w, where $w \in W$:

$$\tau_i = \frac{|W_i|}{e_{ri}} \tag{5}$$

(once the unit cost recovers a larger number of the O-D pairs, this means that this node is more important. For this reason, the above formulation could be used to determine the order to recover compromised nodes).

4.1. The Experiments. There are several different kinds of strategies that the attacker and defender could implement, which result in various possible attack-defense situations. However, insofar as the defense resources are usually limited with resources usually being used to not only protect survival nodes but also recover compromised nodes, three kinds of different node recovery policies, that is, NR1, NR2, and NR3, are proposed in this paper and will be the subject of the following section.

4.2. Experiment Results. The purpose of this experiment is to compare the results from different kinds of node recovery policies (NR). To compare the three different kinds of node recovery policies, it is assumed that in the resource reallocation policy of the defender, the defense resources of each round would not be accumulated (RR1). Further, the weight of two rounds would be (0.5, 0.5). The total resources of players, that is, the attacker and defender, are held to

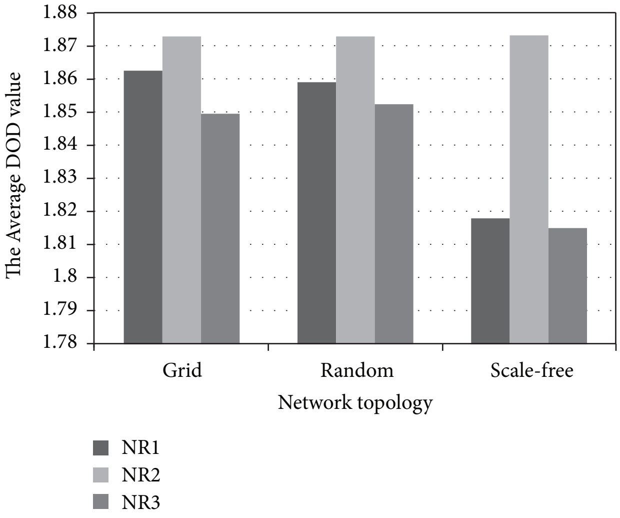


Figure 3: The different node recovery policies in the different network topologies.

Table 9: The experiment results in different kinds of node recovery policy.

Network topology	NR1	NR2	NR3
Grid	1.8626	1.8729	1.8496
Random	1.8592	1.873	1.8525
Scale-free	1.8180	1.8733	1.8151

be equal. The experiment results are listed in Table 9. The different results of the different node recovery policy for the three kinds of network topology are also compared in Figure 3.

4.3. Discussion of Results. The experiment results of the different node recovery policies of the defender have been described. In the following, the results are further discussed.

(i) The recovery policy is advantageous insofar as it improves the Average DOD of the defender. The experiment shows that when the defender has the ability to recover compromised nodes (NR1 and NR3), the Average DOD value is less than when the defender cannot recover any compromised nodes (NR2). Once the defender implements node recovery policies to recover compromised nodes, this decreases the value of the Average DOD. Therefore, when the defender takes node recovery policies to recover certain compromised nodes (NR1 and NR3), the Average DOD value is less than when the defender cannot recover any compromised nodes (NR2).

(ii) Among the three node recovery policies, NR3 is better than the other policies for the grid, random, and scale-free network topologies. NR3 is a strategy for recovering nodes according to their importance. In many experimental cases, the resources are limited and insufficient, thus making it impossible to recover the entire set of compromised nodes. If the resources are restricted, the defender under the NRI policy would use resources to protect survival nodes instead of recovering nodes. However, the node recovery policy is better than the node protection one in improving the network survivability. Hence, the node recovery policy of the NR3 would be better than the NR1 from the view of the defender.

5. Conclusion and Future Works

In this paper, two issues are considered. First, in order to evaluate mobile network survivability, a new survivability metric called Average DOD (degree of disconnectivity) was proposed. In addition, the problem of how to efficiently allocate resources in each node in each round for both cyber attacker and network defender is solved.

This work offers two main contributions. The first was the introduction of the Average DOD metric, which combines the concept of the probability calculated by the contest success function with the DOD metric and which can be a new evaluation tool to demonstrate network survivability. Secondly, a new min-max mathematical formulation was proposed to describe the conflict behavior of a network scenario. Both cyber attacker and network defender could adopt several different policies. The resource reallocation and node recovery problem is considered for the mobile network defender in this paper. As game theory deals with problems in which multiple players with contradictory objectives compete with each other, we developed a combined approach using the gradient method and game theory to resolve the optimal resource allocation for both cyber attacker and network defender in each node in each round. The gradient method can be used to find the optimal resource allocation in each node. Meanwhile, game theory is employed to find the optimal percentage resource allocation in each round. The proposed model provides a mathematical framework for analysing and modeling the posed mobile network security problems.

Although this paper has discussed a two round attack-defense game, it is still difficult to solve the multiround attack-defense scenario because of the complexity of mathematical problem. A possible solution involves the introduction of a threshold for computing or an advanced technology, such as parallel processing systems, in order to improve the efficiency of this model. Furthermore, from the experiment results, compared with the node protection strategy, the node recovery policy is better for defenders to ensure better network survivability. On the other hand, in the multiround attack-defense scenario, the attacker usually gains experience from his previous attack, and as such, the accumulated experience of the attacker should be taken into account in this model. Another consideration is that the resources might have multiple purposes, such as network defenders possibly deploying counterattack strategies to attack the attacker and the cyber attacker possibly using defense strategies to protect his critical information. As a result, since the purpose of resources may not be limited to only one usage for both cyber attacker and network defender, the concept of the multipurpose resources will be further investigated in future research.

Acknowledgment

This research was supported by the National Science Council of Taiwan, Republic of China, under Grant NSC-102-2221-E-002-104.

References

[1] J. M. Kizza, "Security threats to computer networks," in *Guide to Computer Network Security*, pp. 63–88, Springer, London, UK, 2013.

[2] A. K. Rai, R. R. Tewari, and S. K. Upadhyay, "Different types of attacks on integrated MANET-Internet communication," *International Journal of Computer Science and Security*, vol. 4, no. 3, pp. 265–274, 2010.

[3] D. Ferro and A. Salden, "Self-organizing mobile surveillance security networks," in *Proceedings of the 2nd International Conference on Bio-Inspired Models of Network, Information, and Computing Systems (BIONETICS '07)*, pp. 217–227, December 2007.

[4] R. J. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, and T. Longstaff, Survivable network systems: An emerging discipline (No. CMU/SEI-97-TR-013). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 1997.

[5] O. M. Al-Kofahi and A. E. Kamal, "Survivability strategies in multihop wireless networks," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 71–80, 2010.

[6] S. Neumayer and E. Modiano, "Network reliability with geographically correlated failures," in *Proceedings of the IEEE International Conference on Computer Communications (IEEE INFOCOM '10)*, March 2010.

[7] F. Y.-S. Lin, H.-H. Yen, P.-Y. Chen, and Y.-F. Wen, "Evaluation of network survivability considering degree of disconnectivity," in *Hybrid Artificial Intelligent Systems*, pp. 51–58, Springer, Berlin, Germany, 2011.

[8] F. Y.-S. Lin, P.-Y. Chen, Y.-S. Wang, and Y.-Y. Chang, "Network recovery strategies for maximization of network survivability," in *Proceedings of the 7th International Wireless Communications and Mobile Computing Conference (IWCMC '11)*, pp. 1130–1134, July 2011.

[9] S. Skaperdas, "Contest success functions," *Economic Theory*, vol. 7, no. 2, pp. 283–290, 1996.

[10] W. Jiang, Z.-H. Tian, H.-L. Zhang, and X.-F. Song, "A game theoretic method for decision and analysis of the optimal active defense strategy," in *Proceedings of the International Conference on Computational Intelligence and Security (CIS '07)*, pp. 819–823, December 2007.

[11] W. Jiang, B.-X. Fang, H.-L. Zhang, Z.-H. Tian, and X.-F. Song, "Optimal network security strengthening using attack-defense game model," in *Proceedings of the 6th International Conference on Information Technology: New Generations (ITNG '09)*, pp. 475–480, April 2009.

[12] Y.-S. Lin, P.-H. Tsang, C.-H. Chen, C.-L. Tseng, and Y.-L. Lin, "Evaluation of network robustness for given defense resource allocation strategies," in *Proceedings of the 1st International Conference on Availability, Reliability and Security (ARES '06)*, pp. 182–189, April 2006.

[13] G. Levitin and K. Hausken, "Parallel systems under two sequential attacks," *Reliability Engineering and System Safety*, vol. 94, no. 3, pp. 763–772, 2009.

[14] G. Levitin and K. Hausken, "Resource distribution in multiple attacks against a single target," *Risk Analysis*, vol. 30, no. 8, pp. 1231–1239, 2010.

[15] K. Hausken and G. Levitin, "Protection vs. false targets in series systems," *Reliability Engineering and System Safety*, vol. 94, no. 5, pp. 973–981, 2009.

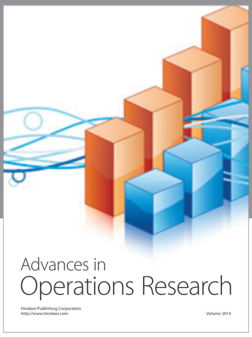
[16] X. Liang and Y. Xiao, "Game theory for network security," *IEEE Communications Surveys & Tutorials*, vol. 15, pp. 472–486, 2013.

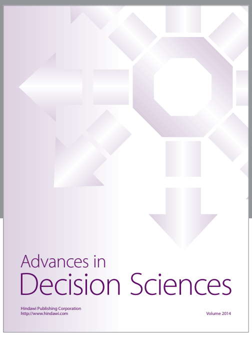
[17] T. Alpcan and T. Basar, "An intrusion detection game with limited observations," in *Proceedings of the 12th International Symposium on Dynamic Games and Applications*, Sophia Antipolis, France, July 2006.

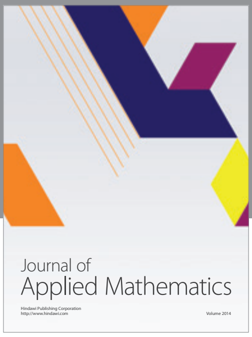
[18] R. Machado and S. Tekinay, "A survey of game-theoretic approaches in wireless sensor networks," *Computer Networks*, vol. 52, no. 16, pp. 3047–3061, 2008.

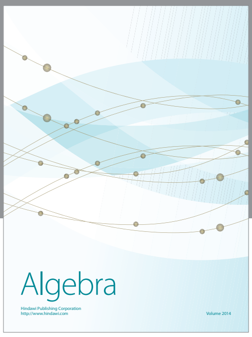
[19] M. H. Hassoun, *Fundamentals of Artificial Neural Networks*, MIT Press, 1995.

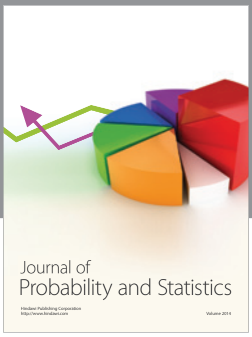
[20] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *Proceedings of the 43rd Annual Hawaii International Conference on System Sciences, HICSS-43*, pp. 51–58, January 2010.


Advances in
Operations Research

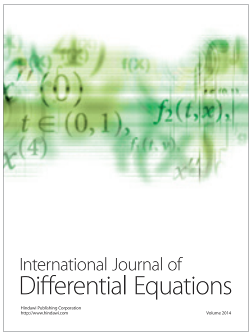

Advances in
Decision Sciences


Journal of
Applied Mathematics

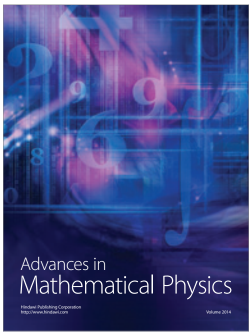

Algebra

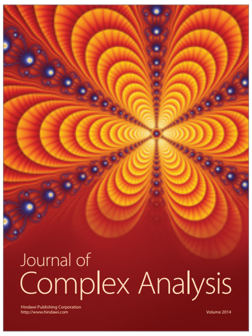

Journal of
Probability and Statistics

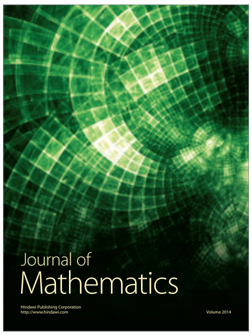
The Scientific
World Journal

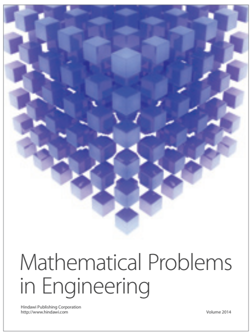

International Journal of
Differential Equations

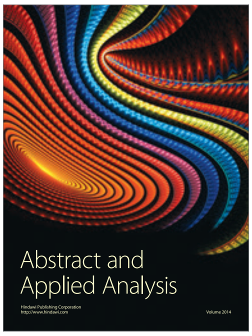
International Journal of
Combinatorics

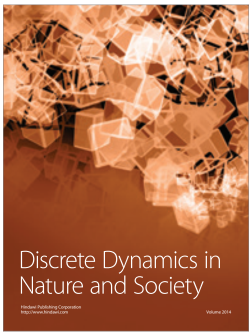

Advances in
Mathematical Physics

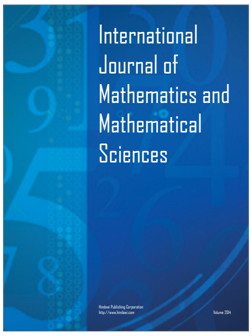

Journal of
Complex Analysis


Journal of
Mathematics


Mathematical Problems
in Engineering

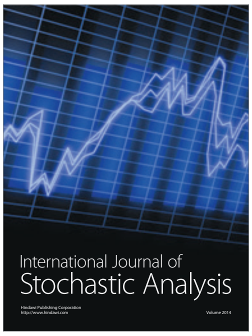

Abstract and
Applied Analysis


Discrete Dynamics in
Nature and Society


International
Journal of
Mathematics and
Mathematical
Sciences

Journal of
Discrete Mathematics

Journal of
Function Spaces


International Journal of
Stochastic Analysis

Journal of
Optimization