Maximization of Multi-Round Network Survivability under Considerations of the Defender's Defensive Messaging Strategies

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

I-Ju Shih
Department of Information Management
National Taiwan University
Taipei, Taiwan, R.O.C.
r99003@im.ntu.edu.tw

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

Abstract—nowadays, enterprises face many challenges of cyber security. How to efficiently allocate defensive resources to reduce damages which are caused by cyber attackers and evaluate system survivability to keeping services operating became important issues. Hence, we develop a scenario of that both cyber attacker and network defender are with incompletely understanding the information about each other is considered. We conduct a mathematical model for analyze this problem for the decision makers to resolve these dilemmas. The Average DOD is then applied to evaluate damage degree of network to estimate all possible strategies which both cyber attacker and network defender would take. Moreover, network defender could release message which might be doing nothing at all, truth, secrecy or deception to confuse cyber attacker to achieve better defense efficiency. In the process of problem solving, the "gradient method" and "game theory" would be used to obtain the optimal resource allocation strategies for both cyber attacker and network defender.

Keyword: Average Degree of Disconnectivity, Average DOD, Gradient Method, Game Theory, Defensive Messaging Strategies, Incomplete Information, Survivability, Optimization, Resource Allocation, Multi-round, Network Recovery

I. INTRODUCTION

A great numbers of users and businesses use smartphones as communication tools but also as a means of planning and organizing their work and private life. These technologies are causing profound changes in the enterprises of information systems and therefore they have become the source of new mobile security risks. Accurately defining the boundary of a mobile n network is a challenge that should not be underestimated. According to ABI Research, the mobile security services market will total around $1.88 billion by the end of 2013[1]. Compared to wired network system, mobile network systems are much more vulnerable to security problems [2]. 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 [3]; these attacks include eavesdropping, phishing, War Driving, and Denial of Service (DoS) attack [4].

In order for any business network to function properly and efficiently, it needs to be protected from all possibly harmful network traffic. Information and applications that are retrieved and transmitted over a mobile network without optimal protection can fall victim to a variety of attacks such as Trojan horses, spyware, self-propagating worms and the exploitation of vendor-specific vulnerabilities. Attacks such as these can hinder connectivity, slow the processing of network traffic into bottlenecks, and even potentially cause damage severe enough to crash an entire system. As a result, there is a pressing need to design countermeasures for network attacks damage. 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 order to keep the service system to steadily contribute, the, the network operator should periodical review the systems security analysis. The systems security analysis is based on the evaluation of network actors' behavior. The enterprise should estimate survivability considering the network information in the target network. However, network operator would utilize their resources or assets to defend their network being attacked. There are methods for defender to secure the network. In the past, most literatures indicated that truthful disclosure of defense should often be preferred to secrecy [5][6][7]. Publicizing defensive information could deter attackers to launch attacks. Moreover, most literature indicated that truthful disclosure could shift attacks to less valuable targets or allow the defender to have first-mover advantage [8].

The results of above literatures indicated that a defender to disclose his defensive information, because these literatures' models were assumed having complete information. This assumption was not precise in reality. It is reasonable for a defender to figure out all information about cyber attacker such as the capability of the attacker or his resources. Similarly, it is impossible for an attacker to understand all information about a defender such as the defender's defense or defense efficiency.

MOBILWARE 2013, November 11-12, Bologna, Italy

DOI 10.4108/icst.mobilware.2013.254294

Traditionally, security-related information such as defensive resource allocations was often keeping secret, which could avoid attackers getting more information about a defender, and let the defender to fell more security than disclosure. Deceptive technique was often used in military field on the other hand.

There are increasing numbers of researchers starting to focus the issue of incomplete information of interactions between attackers and defenders. However, there are still some gaps between research and the reality. In [9], it demonstrated that secrecy or deception was preferred to truthful disclosure for the defender with private information. Though incomplete information is considered in this model, the defender only had single asset. In fact, there are assets in the network, for example, web servers, email servers, file servers or databases. Moreover, some research discuss incomplete information between the attacker and the defender [10][11][12], but the network scenario those research are considered in one-round. In a real world, the defender and the attacker interacted repeatedly until one of them give up or strike a balance.

In the past, most literatures often considered the interaction between an attacker and a defender interact only one-round [13][14]. In [15][16] and [16] these papers considered a multi-round model, but [15] did not consider a situation which a defender could recover node in his network or patch vulnerabilities. On the other hand, in [16], only one target is considered. In fact, a multi-round model of attack and defense is much more general. In addition, most literature in economics and political science is applied game theory to multi-round interactions. The game theory effectively addresses multi-period problems where multiple players with different objective compete and interact with each other on the same system [17].

There are many studies adopting the concept of network connectivity to do quantitative analyses of network survivability. In [18], the researchers proposed using the network connectivity to measure the network survivability under intentional attacks and random disasters. In [19], the definition of network connectivity is the minimum numbers of links or nodes that must be recovered from a given O-D (Original-Destination) pair. In general, the greater the numbers of links or nodes to be recovered to disconnect an O-D pair, the higher the survivability of the network.

Furthermore, the authors in [20] employing network connectivity for a quantitative analysis of network survivability proposed a survivability metric to estimate the residual network survivability after a malicious attack or any network crash incident. The metric proposed in [20] 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 is 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 is adopted to calculate the attack success probability of each node. 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. Furthermore, the Average DOD is used in this model to evaluate the damage degree of network. The larger value of the Average DOD is, the bigger damage degree of network is. This metric reflects the aim of an attacker to separate the target network into pieces, which enables the indication of the damage of the residual networks.

II. Problem Description

Base on [21], we develop a scenario considering the defender could choose message which might be truth, secrecy, deception or doing nothing at all to each node in each round. The defender could manipulate his private information by releasing these messages to confuse the attacker to increase defense efficiency.

The defensive messaging is dividing a node's information into some parts and according to the importance of different part to release messages by the defender. Assuming the information of each node is a collection and the defender could choose a part of information from a node according to his strategy to release truthful message, deceptive message and secrecy or do nothing at all as shown in Figure I. In each round, the defender could choose different part of each node's information to release different message.

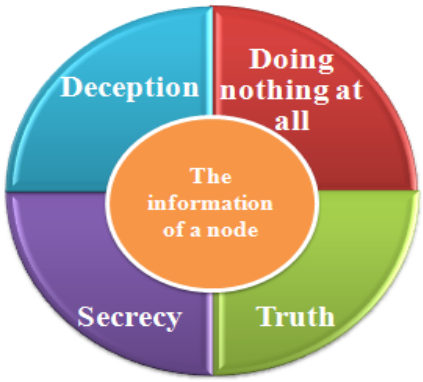

Figure I An example of the message releasing

The defender chose doing nothing at all if and only if the defender did not publicize message. The defender chose truthful message if and only if the public message equaled to actual information; the defender chose secrecy if and only if the message is secret; the defender choses deceptive message if and only if the message not equaled to actual information. The cost of releasing truthful message is lower than the costs of releasing secrecy and deception, respectively. Also, the cost of releasing secrecy is of a successful deception required to keep the truth secret and release the deceptive information. Besides, the cost of truthful, secret and deceptive message is higher than doing nothing at all respectively.

In the proposed model, there are only two players which are an attacker and a defender. The defender determining strategy and choosing message which might be truth, secrecy, deception or doing nothing at all to each node in each round is considered.

In the attack-defense scenario both a defender and an attacker have their respective objectives. Also, the defender and the attacker have to use some strategies to achieve their goals, respectively. From the defender's view, the defender intends to minimize the damage degree of network. On the other hand, from the attacker's view, the attacker plans to maximize the damage degree of network. Nevertheless, both the defender and the attacker are limited by finite resources. Therefore, both the defender and an attacker are concerned about the issue of how to optimally allocate resources on each node in different round. Hence, a mathematical model is developed to help both the defender and an attacker to optimally allocate resources on each node in different round.

It is impossible for a defender to realize all information about cyber attacker in reality, and vice versa. So, incomplete information is considered in this model. Moreover, the interaction between an attacker and a defender would not be only one round. Because in reality an attacker and a defender interact repeatedly such as the attacker collecting information about the defender or probing systems before the attacker launching attacks.

Both a defender and an attacker would use some strategies to achieve their objectives. In the following, the notations of given parameter and decision variable in this model are listed in Table I.

TABLE I. GIVEN PARAMETERS AND DECISION VARIABLES

Given parameter	
Notation	Description
V	Index set of nodes
V_r	Index set of nodes of the attacker knowing in round r, where $r \in R$ and $V_r \subseteq V$
R	Index set of rounds in the attack and defense actions
F	Index set of all nodes' system vulnerability
F_{Ar}	Index set of system vulnerability of the attacker knowing in round r, where $r \in R$ and $F_{Ar} \subseteq F$
F_{Dr}	Index set of system vulnerability of the defender knowing in round r, where $r \in R$ and $F_{Dr} \subseteq F$
$\hat{A}$	Total budget of the attacker
$\hat{B}$	Total budget of the defender
θ_{Di}	Existing defense resources allocated on node i, where $i \in V$
θ_{Ai}	Existing attack resources allocated on node i, where $i \in V_r$
e_{ri}	Repair cost of defender when node i is dysfunctional in round r, where $i \in V$ and $r \in R$
λ_{rj}	The cost of the defender only patches the j-th type of system vulnerability in round r, where $j \in F_{Dr}$ and $r \in R$
μ_{rj}	The cost of the defender uses penetration test to patch the j-th type of system vulnerability in round r, where $j \in F_{Dr}$ and $r \in R$
π_{mri}	m = 0,1, 2 and 3 represents the cost of doing nothing at all and the cost of defensive messaging of truth, secrecy, deception on node i by defender in round r respectively, where $i \in V$, $r \in R$ and $m \in \{0, 1, 2, 3\}$
d_{ri}	The discount rate of defender reallocates resources on node i in round r, where $i \in V$ and $r \in R$
C_{ri}	The discount rate of defender recycles resources on node i in round r, where $i \in V$ and $r \in R$
$h_{ri}(t)$	The discount rate of attacker accumulated resources is increased with time t on node i, where $i \in V_r$ and $r \in R$
U_i	The discount rate of attacker controls the resources of node i by using system vulnerabilities to compromise node i, where $i \in V_r$
ε	The cost of attacker updating information
δ_{ri}	1 if node i is compromised by attacker in round r-1, 0 otherwise where $i \in V_r$ and $r \in R$
γ_{ij}	The reward of the attacker uses the j-th type of system vulnerability on node i to attack node i, where $i \in V$ and $j \in F_{Ar}$
η_{rij}	1 if the attacker considers that the node i still has the j-th type of system vulnerability in round r, 0 otherwise where $i \in V_r$, $j \in F_{Ar}$ and $r \in R$
ζ_{rij}	The system vulnerability status on node i in round r. 1 if the node i has the j-th type of system vulnerability in round r, 0 otherwise where $i \in V$, $j \in F$ and $r \in R$ (Once the defender finds the j-th type of system vulnerability in round r, the ζ_{rij} value of the nodes, which have the j-th type of system vulnerability, are 1 in round r.)
Decision variable	
Notation	Description
A_r	Attacker's attack budget in round r, where $r \in R$
B_r	Defender's defense budget in round r, where $r \in R$
$\overrightarrow{a_r}$	Attacker's budget allocation, which is a vector of attack cost a_{r1}, a_{r2} to a_{ri} in round r, where $i \in V_r$ 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 $r \in R$
x_{ri}	Attacker's budget allocation on node i in round r, where $i \in V_r$ and $r \in R$
y_{ri}	Defender's budget allocation on node i in round r, where $i \in V$ and $r \in R$
$\overrightarrow{s_r}$	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 $r \in R$
s_{ri}	1 if node i is repaired by defender in round

	r, 0 otherwise where $i \in V$ and $r \in R$
α_{ri}	The proportion of resources on node i is reallocated by defender in round r, where $i \in V$ and $r \in R$
β_{ri}	The proportion of resources on node i is recycled by defender in round r, where $i \in V$ and $r \in R$
p_{mri}	m = 0,1, 2 and 3 represents the information proportion or probability of defender doing nothing at all, using truthful, secrecy, deceptive message on node i in round r respectively, which falls in (0,1), where $i \in V$, $r \in R$ and $m \in \{0, 1, 2, 3\}$
q_{rij}	1 if the attacker uses the j-th type of system vulnerability on node i to attack node i in round r, 0 otherwise where $i \in V_r$, $j \in F_{Ar}$ and $r \in R$
φ_{rij}	1 if the defender only patches the j-th type of system vulnerability on node i in round r, 0 otherwise where $i \in V$, $j \in F_{Dr}$ and $r \in R$
τ_{rij}	1 if the defender uses penetration test to patch the j-th type of system vulnerability on node i in round r, 0 otherwise where $i \in V$, $j \in F_{Ar}$ and $r \in R$
$\overline{D}(\overrightarrow{a_r}, \overrightarrow{b_r})$	The Average DOD, which is considering under attacker's and defender's budget allocation are $\overrightarrow{a_r}$ and $\overrightarrow{b_r}$ in round r, where $r \in R$

The problem is then formulated as the following.

Objective function:

$$\min_{\overrightarrow{b_r}} \max_{\overrightarrow{a_r}} \sum_{r \in R} \overline{D}(\overrightarrow{a_r}, \overrightarrow{b_r}) \quad \text{(IP 1)}$$

Subject to:

$$\begin{aligned} &\sum_{i \in V_r} x_{ri} + \varepsilon \\ &\leq A_r \\ &+ \sum_{i \in V_r} U_i \theta_{Di} \sum_{r \in R} (\delta_{ri} \\ &- s_{ri}) \sum_{j \in F_{Ar}} q_{(r-1)ij} \left(\zeta_{rij} - \varphi_{rij}\right. \\ &\left. - \tau_{rij}\right) + \sum_{i \in V_r} \theta_{Ai} h_{ri}(t) \\ &+ \sum_{i \in V_r} \sum_{j \in F_{Ar}} q_{rij} \gamma_{ij} \eta_{rij} \left(\zeta_{rij} - \varphi_{rij}\right. \\ &\left. - \tau_{rij}\right) \end{aligned} \qquad \forall r \in R \quad \text{(IP 1.1)}$$

$$\begin{aligned} &\sum_{i \in V} y_{ri} + \sum_{i \in V} e_{ri} s_{ri} \\ &+ \sum_{i \in V} \sum_{m \in \{0,1,2,3\}} p_{mri} \pi_{mri} \\ &+ \sum_{i \in V} \sum_{j \in F_{Dr}} \lambda_{rj} \varphi_{rij} \zeta_{rij} \\ &+ \sum_{i \in V} \sum_{j \in F_{Dr}} \mu_{rj} \tau_{rij} \zeta_{rij} \\ &\leq B_r \\ &+ \sum_{i \in V} \theta_{Di} (d_{ri} \alpha_{ri} \\ &+ C_{ri} \beta_{ri}) \sum_{r \in R} [1 - (\delta_{ri} - s_{ri})] \end{aligned} \qquad \forall r \in R \quad \text{(IP 1.2)}$$

$$\sum_{r \in R} A_r \leq \hat{A} \quad \text{(IP 1.3)}$$

$$\sum_{r \in R} B_r \leq \hat{B} \quad \text{(IP 1.4)}$$

$$\sum_{r \in R} s_{ri} \leq \sum_{r \in R} \delta_{ri} \qquad \forall i \in V_r \quad \text{(IP 1.5)}$$

$$\sum_{m \in \{0,1,2,3\}} p_{mri} = 1 \qquad \forall r \in R, i \in V \quad \text{(IP 1.6)}$$

$$0 \leq \alpha_{ri} \qquad \forall r \in R, i \in V \quad \text{(IP 1.7)}$$

$$0 \leq \beta_{ri} \qquad \forall r \in R, i \in V \quad \text{(IP 1.8)}$$

$$\alpha_{ri} + \beta_{ri} \leq 1 \qquad \forall r \in R, i \in V \quad \text{(IP 1.9)}$$

$$\sum_{r \in R} \varphi_{rij} \leq \sum_{i \in V_r} \sum_{r \in R} q_{rij} \qquad \forall i \in V_r, j \in F_{Dr} \quad \text{(IP 1.10)}$$

$$\sum_{r \in R} \varphi_{rij} + \sum_{r \in R} \tau_{rij} + \zeta_{rij} \leq 1 \qquad \forall r \in R, i \in V, j \in F_{Dr} \quad \text{(IP 1.11)}$$

The objective function is to minimize the maximum sum of the product of Average DOD in each round.

(IP 1.1) Describing the sum of the allocated attack budgets in each node and the cost of updating information should not exceed the sum of attack budgets, the collection of compromised nodes' resources, accumulated resources and the reward of using system vulnerability to attack in that round.

(IP 1.2) Describing the sum of the allocated defense budgets in each node, repaired cost of the compromised nodes, the cost of releasing messages, the cost of only patching and the cost of using penetration test to patch system vulnerability in each node should not exceed the sum of the new allocated, reallocated and recycled budgets in that round.

(IP 1.3) Describing the sum of the allocated attack budgets in each round should not exceed the total budget of the attacker.

(IP 1.4) Describing the sum of the allocated defense budgets in each round should not exceed the total budget of the defender.

(IP 1.5) Describing only after the nodes are compromised by the attacker, the nodes could be repaired by the defender.

(IP 1.6) Describing the sum of the information

proportion or probability of defender using different message on node *i* in round *r* should be 1.

(IP 1.7) Describing the proportion of resources on node *i* is reallocated by defender in round *r* should between 0 and 1.

(IP 1.8) Describing the proportion of resources on node *i* is recycled by defender in round *r* should between 0 and 1.

(IP 1.9) Describing the sum of the proportion of resources reallocated and resources recycled on node *i* in round *r* should between 0 and 1.

(IP 1.10) Describing once after the attacker used the *j*-th type of system vulnerability on node *i* to attack node *i*, the *j*-th type of system vulnerability is patched by the defender.

(IP 1.11) Describing the sum of the number of only patching, the number of using penetration test to patch the *j*-th type of system vulnerability on node *i* in each round and the system vulnerability status of node *i* in round *r* should not exceed 1.

III. Solution Approach

In this paper, we combine game theory and gradient method to find the optimal resource allocation strategy on each node in each round for both cyber attacker and network defender. The detailed process is shown in Figure II.

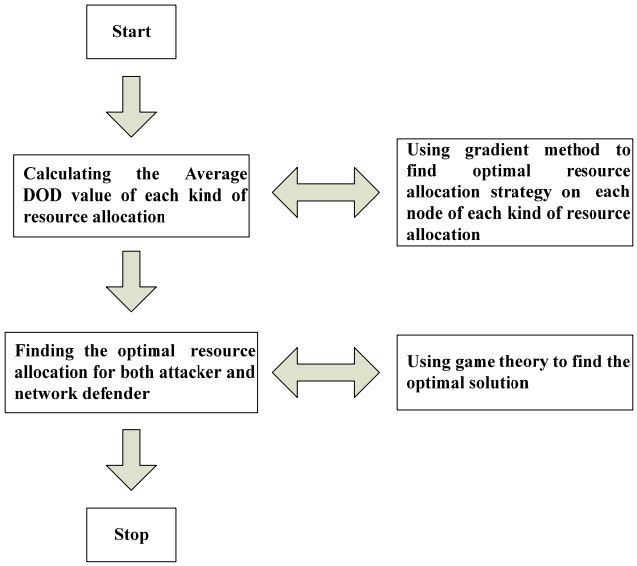

FIGURE II THE SOLUTION PROCEDURE OF THIS MODEL

The gradient method is a general framework for solving optimization problems to maximize or minimize functions of continuous parameters. The problem in this model is a min-max formulation and both cyber attacker and network defender are assumed that they could allocate continuous budgets on each node in each round. Therefore, the gradient method is suitable for solving this problem.

The gradient method can be classified into two types, one is the gradient descent and the other is the gradient ascent. The gradient descent method is used to solve optimization minimization problem and the optimization maximization problem can be solved by the gradient ascent method. The concept of gradient descent and gradient ascent is similar, so both of them could adopt the following algorithm:

Initially, to get a start point. The selection of start point is critical, because it influences the result and computational efficiency. To determine a direction, it could be positive or negative. If a maximization problem is solved, a positive direction should be chosen. On the other hand, a negative direction is another choice which could be used to solve minimization problem.

The gradient method adopted a step-by-step method to find the optimization. Therefore, the step size which is the move size in each step should be determined. To determine the next dimension to move, the gradient method with the derivative method to find the dimension which is most influenced, move a step in the most impact dimension and set the new position to be the next start point. And then repeats step 4 until stopping criterion is satisfied.

Accelerating Calculation of the Average DOD Value

In this problem, the Average DOD value is used to evaluate damage degree of network. In order to calculate Average DOD, we should consider all possible network configurations. Once the number of network node is too huge, it takes times to calculate the Average DOD value. Hence, the method to accelerate calculation of the Average DOD value is proposed.

Average DOD value is calculated by the DOD value and probability of each possible network configuration. Therefore, when the probability is larger, the possibility of network configuration occurring is bigger. The calculation of the probability is easier than the calculation of the DOD value, so we used the probability value of each network configuration to reduce complexity of the calculation of the Average DOD value.

When the probability of network configuration occurring is extremely low, the influence on Average DOD value would also low. For example, if the probability of network configuration is equaled to 0.00000000001 and the DOD value equals to 10000 or 1, the product of probability and the DOD value in two different situations are almost identical. This method is applied to reduce complexity in this model.

The Calculation of Average DOD Value in Multi-Round

In this section, we introduce how to use the Average DOD value to evaluate damage degree of network in multiple rounds. In each round, both the defender and the attacker use gradient method to find the optimal strategy. Besides, both of them have to allocate resources in each node. Therefore, each node would have a compromised probability which is calculated by contest success function. So, the probability of different states of network configuration is calculated by the product of compromised probability of each node. There are multiple likelihoods in next round, and consequently the concept of the expected value is used to calculate the Average

DOD value in next round. Finally, combining the Average DOD value with the weight of each round is the final damage degree of the network. As a result, the final Average DOD value is calculated as following.

The final Average DOD value would be = $\bar{D}_1 + \sum_{r=2}^{n}\sum_{j=0}^{m}\left(\bar{D}_{rj} \times P_{(r-1)j}\right)$

($\bar{D}_{rj}$ is the Average DOD value of the configuration *j* in round *r* and $P_{(r-1)j}$ is the incidence of the configuration *j* in previous round)

Using Game Theory to Find the Optimal Solution

In this problem, both cyber attacker and network defender need to determine how to allocate resources efficiently on each node in each round. Besides, in this model we assume the defender determining strategy and choosing message which might be truth, secrecy, deception or doing nothing at all to each node in each round. Moreover, we assume both the defender and the attacker having incomplete information about each other. Though this model is a problem of incomplete information, the definition of complete information game in [22] is "Every player knows both the strategies and payoffs of all players in the game, but not necessarily the actions." Basically, the defender and the attacker in this problem understand both the strategies and payoffs of each other, but the actions are not. Therefore, this problem is viewed as a complete information game.

However, how to find the optimal strategies in the game theory is another issue. Therefore, the solution approach of this game is introduced in the following [23].

1. Finding out dominant strategy. The dominant strategy is always better than other strategies no matter what kind of strategy the opponent to take.
2. If only one strategy is remained of each player, it would be the optimal strategy. Otherwise, go to step 3.
3. Using the min-max strategy to find the optimal strategy of each player. If min-max strategy still could not find the optimal strategy, go to step 4.
4. Using the mixed strategy (Linear programming) to find the optimal strategy of each player.

For example, both cyber attacker and network defender have 3 different strategies about allocating different resources percentage in each round as shown in Table II. In addition, the combined results of different percentage resource allocation strategies for both cyber attacker and network defender are calculated by the Average DOD.

1. Finding out dominant strategy. From the view of the attacker, the attacker wanted to maximize the damage degree (Average DOD) of the network, so the S_{13} is the optimal strategy. On the other hand, the defender intends to minimize the damage degree of network, resulted that the S_{21} is the optimal strategy.
2. Because only one result is remained for each player, it is regarded as the optimal solution for both parties. The optimal strategy of the attacker is S_{13} and the optimal strategy of the defender is S_{21}. Finally, the result of this example is 3.

TABLE II. AN EXAMPLE OF GAME THEORY

Strategy		Attacker		
		S_{11}	S_{12}	S_{13}
Defender	S_{21}	3	2	3
	S_{22}	2	2	5
	S_{23}	2	1	4

IV. COMPUTATIONAL EXPERIMENTS

■ *Experiment Environment*

The proposed solution approach is implemented in Eclipse and run on the PC with AMD Phenom(tm) IIX4 B40 Processor 3.00 GHz, 6 GB RAM, and on the OS of the MS Windows 7.

With the time complexity analysis, we know this problem is an extremely complicated problem. It costs eight days to get the results of one experiment considering three kinds of topology, three rounds and nine nodes. Therefore, 9 nodes and three-round interaction between the attacker and the defender in the experiments are considered. Moreover, we consider three kinds of network topology including the grid network (GD), random network (RD) and scale-free network (SF). The GD is really regular network. The SF is a kind of network whose degree distribution follows a power law. And, the RD is connected with other nodes randomly. Computational Experiment of (IP 1)

The solution approach is used to solve this problem. There are ten different kinds of resource allocation strategy in three rounds for both cyber attacker and network defender in this experiment. The gradient method is used to calculate the final Average DOD vale in 100 different payoff values. Therefore, the results are demonstrated in the following. The strategies (*A, B, C, D, E, F, G, H, I, J*) represents ((0, 0, 1), (0, 0.3, 0.7), (0, 0.6, 0.4), (0, 1, 0), (0.3, 0, 0.7), (0.33, 0.33, 0.33), (0.3, 0.6, 0.1), (0.6, 0, 0.4), (0.6, 0.3, 0.1), (1, 0, 0)) separately.

TABLE III. THE RESULTS OF THE INCOMPLETE INFORMATION EXPERIMENT UNDER THE DEFENSIVE MESSAGING (GRID NETWORK)

Grid network												
Strategy		**Attacker**										
		A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**MAX**
Defender	**A**	0.32	1.94	1.87	1.55	2.94	4.56	4.46	2.87	4.34	2.53	4.56
	B	0.27	0.89	0.59	0.52	1.97	2.56	3.21	2.82	3.32	2.42	3.32
	C	0.29	0.75	0.84	0.63	1.73	2.13	2.2	2.16	2.38	2.23	2.38
	D	0.31	0.69	0.94	0.73	1.78	1.73	1.86	1.89	1.84	1.95	1.95
	E	0.27	0.92	0.72	0.57	1.83	1.76	2.23	2.04	2.77	0.89	2.77
	F	0.29	0.85	0.66	0.51	1.02	1.37	1.29	0.77	0.76	0.72	**1.37**
	G	0.4	0.61	0.93	0.59	0.99	0.88	1.64	1.29	1.53	0.71	1.64
	H	0.3	0.68	0.56	0.59	0.94	1.74	1.62	1.82	2.57	0.73	2.57
	I	0.32	0.78	0.89	0.56	0.78	1	1.14	1.06	1.47	0.71	1.47
	J	0.35	0.78	1.02	0.55	0.72	1.13	1.31	1.12	1.7	1.47	1.7
	MIN	0.27	0.61	0.56	0.51	0.72	0.88	**1.14**	0.77	0.76	0.71	

The game theory is adopted to find the optimal resource allocation strategy for both cyber attacker and network defender. According to the solution procedure of game theory, the dominant strategy eliminating method and min-max method could not be used to find the optimal resource allocation strategy for both cyber attacker and network defender in this experiment. Therefore, the mixed strategy is adopted to find the optimal percentage resource allocation strategy for both cyber attacker and network defender. The optimal solution of the probability of each strategy that the attacker would take is {(0.3, 0.6, 0.1), (0.6, 0.3, 0.1)} = {(0.83, 0.17)}. In addition, the optimal solution of the probability of each strategy that the defender would take is {(0.6, 0.3, 0.1), (0.33, 0.33, 0.33)} = {(0.62, 0.38)}. The final average DOD value is 1.2.

■ *Discussion of Results*

The defensive messaging could aim at different information on a node to release messages. So, the protective effect is stronger than the second kind of situation of defensive messaging. Hence, the attacker would choose to allocate some resources in the first round to collect information, and allocate more resources in the second round to attack. In the view of the defender, in order to reduce the information which the attacker could collect the defender would choose to allocate more resources in the first round to reduce the damage. The results of random network are demonstrated in the Table IV.

TABLE IV. THE RESULTS OF THE INCOMPLETE INFORMATION EXPERIMENT UNDER THE DEFENSIVE MESSAGING (RANDOM NETWORK)

Random network												
Strategy		Attacker										
		A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**MAX**
Defender	**A**	0.34	2.49	2.28	1.91	3.73	5.65	5.55	3.52	5.4	3.1	5.65
	B	0.35	1.29	0.85	0.75	2.56	3.29	3.63	3.49	4.08	3.03	4.08
	C	0.37	0.86	1.13	0.62	2.11	2.63	3.14	2.56	2.93	2.7	3.14
	D	0.41	0.86	1.09	0.99	2.27	2.31	2.36	2.56	2.31	2.32	2.56
	E	0.36	0.91	0.96	0.72	2.25	2.54	3.03	1.39	1.85	1.1	3.03
	F	0.39	0.94	1.19	0.67	1.45	1.83	1.91	0.96	1.17	0.99	**1.91**
	G	0.4	0.83	1.01	0.73	1.22	1.14	1.96	0.94	1.69	0.94	1.96
	H	0.39	1.04	0.72	0.68	1.1	2.32	1.93	2.13	3.16	0.86	3.16
	I	0.42	1.08	1.29	0.67	0.99	1.29	1.43	1.51	1.91	0.83	1.91
	J	0.45	1.13	1.64	0.64	0.99	1.52	1.95	1.26	1.8	1.72	1.95
	MIN	0.34	0.83	0.72	0.62	0.99	1.14	**1.43**	0.94	1.17	0.83	

Because this experiment could not find pure strategy, the mixed strategy is adopted to find the optimal percentage resource allocation strategy for both cyber attacker and network defender. The optimal solution of the probability of each strategy that the attacker would take is {(0.3, 0.6, 0.1), (0.6, 0.3, 0.1)}={(0.61, 0.39)}. In addition, the optimal solution of the probability of each strategy that the defender would take is {(0.6, 0.3, 0.1), (0.33, 0.33, 0.33)}={(0.61, 0.39)}. The final average DOD value is 1.62.

■ *Discussion of Results*

The defensive messaging could aim at different information on a node to release messages. So, the protective effect is stronger than the second kind of situation of defensive messaging. Hence, the attacker would choose to allocate some resources in the first round to collect information, and allocate more resources in the second round to attack. Because the distribution of important nodes is random and scattered in random network, local nodes damage would cause network fragmentation. In the view of the defender, in order to avoid the network would become fragmentation the defender would choose to allocate more resources in the first round. Moreover, in order to enhance the survivability in remaining rounds, the defender would allocate resources in these rounds. The results of scale-free network are demonstrated in the Table V.

TABLE V. THE RESULTS OF THE INCOMPLETE INFORMATION EXPERIMENT UNDER THE DEFENSIVE MESSAGING (SCALE-FREE NETWORK)

Scale-free network												
Strategy		Attacker										
		A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**MAX**
Defender	**A**	0.23	1.74	1.7	1.33	2.68	4.81	4.44	2.56	4.31	2.15	4.81
	B	0.25	0.96	0.64	0.47	1.75	3.18	3.24	2.57	3.02	2.17	3.24
	C	0.26	0.68	0.82	0.45	1.5	2.4	2.69	1.78	2.66	1.93	2.69
	D	0.29	0.74	1.15	0.67	1.78	1.57	1.84	1.78	1.9	1.68	1.9
	E	0.25	0.69	0.58	0.51	1.85	2.11	2.82	0.99	1.44	0.65	2.82
	F	0.27	0.79	1.03	0.46	0.92	1.57	1.59	0.7	0.96	0.58	**1.59**
	G	0.29	0.68	0.87	0.47	0.91	0.82	1.81	0.69	0.82	0.58	1.81
	H	0.27	0.66	0.81	0.5	0.76	1.87	1.75	1.81	3.1	0.61	3.1
	I	0.29	0.7	0.93	0.46	0.77	0.89	1.22	1.15	1.73	0.65	1.73
	J	0.32	0.84	1.03	0.51	0.76	1.25	1.56	1.11	1.94	1.34	1.94
	MIN	0.23	0.66	0.58	0.45	0.76	0.82	**1.22**	0.69	0.82	0.58	

Because this experiment could not find pure strategy, the mixed strategy is adopted to find the optimal percentage resource allocation strategy for both cyber attacker and network defender. The optimal solution of the probability of each strategy that the attacker would take is {(0.3, 0.6, 0.1), (0.6, 0.3, 0.1)} = {(0.68, 0.32)}. In addition, the optimal solution of the probability of each strategy that the defender would take is {(0.6, 0.3, 0.1), (0.33, 0.33, 0.33)} = {(0.55, 0.45)}. The final average DOD value is 1.39.

■ *Discussion of Results*

The defensive messaging could aim at different information on a node to release messages. The protective effect is stronger than the second kind of situation of defensive messaging. The attacker would choose to allocate some resources in the first round to collect information, and allocate more resources in the second round to attack. Because the core nodes damage in scale-free network 1 would cause network fragmentation, in order to avoid the network would become fragmentation the defender would choose to allocate more resources in the first round. Moreover, in order to enhance the survivability in remaining rounds, the defender would allocate resources in these rounds

V. CONCLUSION

In this paper, two issues are considered. First, an incomplete information attack-defense problem is proposed. In addition, how to efficiently allocate resources on each node in multiple rounds for both cyber attacker and network defender is needed to be solved.

The main contributions of this work are as follows:

■ *An incomplete information attack-defense problem*

In reality, the attacker owns information which is often limited. It is impossible for the attacker to know the whole information about the defender. In other words, the information between the attacker and the defender is not always symmetric. Therefore, an incomplete information attack-defense problem is considered. Moreover, we also considered the defender releasing message which might be truth, secrecy, deception or doing nothing at all to each node in each round to increase defense efficiency.

■ *Solving a multi-round attack-defense problem*

A new min-max mathematical formulation is proposed. Moreover, both cyber attacker and network defender could take lots of different policies. From the view of the attacker, the accumulated experiences and vulnerability attacks is considered. On the other side, the resource reallocation or recycle, node recovery, system vulnerability patch and message releasing problem is considered for the defender.

Besides, the gradient method and game theory is adopted to find the optimal resource allocation for both cyber attacker and network defender on each node in each round. The gradient method is used to find the optimal resource allocation on each node. The game theory is adopted to find the optimal percentage resource allocation in each round.

■ *A more realistic network topology*

A complex system with n nodes in different kinds topology is considered. We also consider three kinds of relationships between nodes which included independence, dependence and interdependence to get closer to realistic network topology.

■ *Providing a objective guideline for network operators*

In this multi-round attack-defense problem, we conduct a mathematical model for this problem. Besides, we use Average DOD to evaluate damage degree of network to help network operators to predict all possible strategies which both cyber attacker and network defender would take. As a result, network operators could use this model to take strategies and optimally allocate resources to ensure a prearranged level of system survivability.

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] ABI Research, "BYOD and Increased Malware Threats Help Driving Billion Dollar Mobile Security Services Market", 2013.

[2] J. M. Kizza, "Security Threats to Computer Networks", In Guide to Computer Network Security " , Springer London, pp. 63-88, 2013.

[3] 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, 4(3), 265-274, 2010.

[4] D. Ferro and A. Salden, "Self-organizing Mobile Surveillance Security Networks", In Bio-Inspired Models of Network, Information and Computing Systems, pp. 217-227 , December 2007.

[5] V.M. Bier, S. Oliveros and L. Samuelson, "Choosing What to Protect: Strategic Defensive Allocation Against an Unknown Attacker", Journal of Public Economic Theory, Vol. 9, Issue 4, pp. 563–587, August 2007.

[6] J. Zhuang and V.M. Bier, "Balancing Terrorism and Natural Disasters - Defensive Strategy with Endogenous Attacker Effort", Operations Research, Vol. 55, Issue 5, pp. 976–991, September 2007.

[7] T. Sandler and D.G. Arce, "Terrorism and Game Theory", Simulation & Gaming, Vol. 34, Issue 3, pp.319–337, September 2003.

[8] K. Hausken and V.M. Bier, "Defending against Multiple Different Attackers", *European Journal of Operational Research*, Vol. 211, Issue 2, pp. 370-384, June 2011.

[9] J. Zhuang and V.M. Bier, "Secrecy and Deception at Equilibrium, with Applications to Anti-terrorism Resource Allocation", Defence and Peace Economics, Vol. 22, No. 1, pp. 43-61, February 2011.

[10] N.S. Dighe, J. Zhuang and V.M. Bier, "Secrecy in Defensive Allocations as a Strategy for Achieving More Cost-effective", International Journal of Performability Engineering, Vol. 5, No. 1, pp. 31-43, January 2009.

[11] R. Powell, "Allocating Defensive Resources with Private Information about Vulnerability", American Political Science Review, Vol. 101, No. 4, pp. 799–809, November 2007.

[12] K. Hausken, "Strategic Defense and Attack for Reliability Systems", Reliability Engineering & System Safety, Vol. 93, Issue 11, pp. 1740-1750, November 2008.

[13] M.N. Azaiez and V.M. Bier, "Optimal Resource Allocation for Security in Reliability Systems", European Journal of Operational Research, Vol. 181, Issue 2, pp. 773-786, September 2007.

[14] F.Y.S. Lin, P.H. Tsang, P.Y. Chen and H.T. Chen, "Maximization of Network Robustness Considering the Effect of Escalation and Accumulated Experience of Intelligent Attackers", Proc. World Multiconference on Systemics, Cybernetics and Informatics, 2009.

[15] G. Levitin and K. Hausken, "Resource Distribution in Multiple Attacks Against a Single Target", Risk Analysis, Vol. 30, No. 8, pp. 1231–1239, August 2010.

[16] T. Alpcan and T. Baser, "A Game Theoretic Analysis of Intrusion Detection in Access Control Systems", Proceeding of the 43rd IEEE Conference on Decision and Control, 2004.

[17] S. Skaperdas, "Contest Success Functions", Economic Theory, 1996.

[18] S. Neumayer and E. Modiano, "Network Reliability with Geographically Correlated Failures", In INFOCOM, 2010 Proceedings IEEE, pp. 1-9, 2010, March.

[19] O. M. Al-Kofahi and A. E. Kamal, "Survivability Strategies in Multihop Wireless Networks", Wireless Communications, IEEE, 17(5), 71-80, 2010.

[20] F. Y. S. Lin, H. H. Yen, P. Y. Chen, and Y. F. Wen,, "Evaluation of Network Survivability Considering Degree of Disconnectivity, Hybrid Artificial Intelligent Systems, pp. 51-58, 2011.

[21] N.C. Rowe, "Deception in Defense of Computer Systems from Cyber Attack", Cyber Warfare and Cyber Terrorism, pp. 97-104, 2008.

[22] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya and Q. Wu, "A Survey of Game Theory as Applied to Network Security", Proceedings of the 43rd Hawaii International Conference on System Sciences, 2010.

[23] G. Owen, "Game Theory, 3rded", Academic Press, 2001.