Effective Network Defense Strategies against Malicious Attacks with Various Defense Mechanisms under Quality of Service Constraints

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

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

Yu-Pu Wu
Department of Information Management
National Taiwan University
Taipei, Taiwan, R.O.C.
r99012@im.ntu.edu.tw

Chia-Yang Hsu
Department of Information Management
National Taiwan University
Taipei, Taiwan, R.O.C.
r98033@im.ntu.edu.tw

***Abstract*—How to apply timely and effective defense strategies against attackers while maximizing system survivability is a critical issue for a defender. This paper mathematically models attack and defense scenarios, using various defensive mechanisms during both the planning and defending stages and under quality of service constraints. This model incorporates high degrees of randomness, as attackers are assumed to have incomplete information. Given such non-deterministic problems, this paper identifies the appropriate time for applying defense in depth or resource concentration strategy.**

Keywords: Network Survivability; Defense Strategies; Mathematical Programming; Incomplete Information;

I. INTRODUCTION

The losses caused by cyber-attacks are a critical issue for business enterprises. In State of Enterprise Security [1], the authors note that the top costs of cyber-attacks include lost productivity, lost revenue and the loss of customer trust. Similarly, the 2011 Global State of Information Security Survey [2] also listed financial losses, theft of intellectual property, and a compromised brand or reputation as the top three consequences of cyber-attacks.

The first step in discussing cyber-attack-and-defense is to determine how to measure the defensive status of a given system. There are many ideal metrics within the existing literature that are widely used to describe system status, for example, survivability, availability, reliability and dependability. In this work, we focus specifically on survivability for measuring network systems. We adopt the definition from [3] and define survivability as "the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents, where system is defined in the broadest possible sense, including networks and large-scale systems of systems." In this way, our adopted definition not only follows a system perspective, but also a service perfective which focuses on maintaining the quality of service.

Maintaining a focus on service is important because while defending against malicious attacks, the defender must maintain provided services smoothly. In other words, the defender must not only protect the system, but also simultaneously serve legitimate users at a certain level of QoS (Quality of Service). Therefore, survivability is an ideal metric for judging defensive capabilities.

In our previous network attack and defense studies, models are often configured so that attackers can compromise target nodes only if their spent resources are greater than the defensive resources deployed on nodes. However, such models are too simple to reflect real world scenarios since it is deterministic. One solution to this problem is to adopt the contest success function. In [4], the contest success function is applied from economics to determine each player's probability of winning as a function of all players' efforts. The form of the contest success function is $\frac{T^m}{T^m + t^m}$ where T and t denote resources that each player has invested respectively, and m denotes contest intensity. In [5] and [6], the authors adopt the contest success function for network attack and defense scenarios, where T refers to resources that the attacker spends on the target node and t stands for the defensive resources deployed on the same node. In this work, the contest success function is also utilized for determining the probability of an attacker successfully compromising one node.

Defenders often act reactively in network attack and defense scenarios. However, as technology progresses, defense solutions are no longer bounded by general defense resources such as firewalls or IPS (Intrusion Prevention System). Now, there are also mechanisms like dynamic topology reconfiguration [7] [8], cloud computing security services (i.e. Security as a Service, SaaS) [9] [10], and attack signatures that help grant immunity to certain types of attacks.

Moreover, as cloud computing increases in popularity, virtualization techniques have garnered more attention. Many defense solutions are developed based on these technologies, such as the Virtual Machine Monitor Intrusion Prevention System (VMM-IPS), which is an intrusion prevention system embedded in the VMM that controls all corresponding virtual machines [11] [12].

However, time and improved techniques have not only resulted in improved defenses, but also improved attacks. Attack tools and equipment have continually evolved not only in quantity but also quality. Before launching an attack, attackers spend a certain portion of their budget to acquire attack tools as preparation. This includes buying ready-made tools, reconstructing tools based on ready-made examples, and self-development projects. Intuitively, buying ready-made tools costs less since attackers can spend less time configuring them. However, they are also easily blocked by security tools such as intrusion prevention systems, since the

signatures of the ready-made tools may already be well known. Furthermore, ready-made tools tend to be lower in quality than self-developed alternatives. Higher-quality attack tools often more effectively utilize the full budget of an attacker.

Obtaining attack tools allows an attacker to launch an attack, however in most cases; attackers do not have complete information regarding the target network, like the exact location of core nodes and defense configuration. They can only collect information during an attack. The incomplete information assumption makes the attack-defense scenario more realistic but raises the difficulty in solving the problem. As a result, much previous research must assume that attackers have perfect knowledge regarding target networks [5] [6] [13].

Although the defender can apply diverse defense mechanisms, some of these solutions have negative effects on the quality of service. For instance, dynamic topology reconfiguration may increase the number of hops (i.e., intermediate nodes) that legitimate users experience. Therefore, defenders must deliberately apply defense strategies to minimize the attackers' success probability.

For defense resource allocation, there are two well-known strategies defenders can apply: resource concentration and defense in depth strategy. However, these strategies are not universal. It is extremely important to determine under what conditions resource concentration or defense in depth strategy perform better in terms of survivability.

Given these problems, this paper provides several contributions to the existing literature. It first examines the robustness of grid, random, and scale free networks. It then identifies the proper time and conditions for resource concentration and defense in depth strategies, as well as considers various attack/defense mechanisms and the quality of service constraints within attack and defense scenarios. Lastly, it provides a more realistic attack scenario by assuming that attackers have incomplete information on the target network.

II. RELATED WORK

As mentioned above, the determination of whether an attacker compromises a node is based on the contest success function, originating from economics. The major characteristic of this function is contest intensity. As an exponent, the value significantly influences the result. According to previous research [14] [15], the different values of contest intensity reflect distinct real world battle scenarios. When contest intensity lies from $0 < m \leq 1$, it represents "fight to win or die" circumstances. With respect to $1 < m < \infty$, it stands for the effectiveness of resources each player invested is exponentially increasing since contest intensity is the exponent of contest success function. When $m \to \infty$, it depicts "winner takes all" circumstance.

In most attack and defense scenario studies, researchers either consider few defense mechanisms in a simple system or assume the attacker has complete information on the target network [5] [6] [13]. For example, in [5], the authors propose an optimal distribution of defense resources in a series system, rather than a network topology. Regarding [6], the authors assume that the defender only has one single object that can be destroyed by the attacker. Such an assumption is not suitable for the service-providing scenario considered in this work, since it results in poor quality of service. Lastly, with [13], the authors assume the attacker has complete information on the target network and that the attacker collects every detail of the defense configuration before launching their assault.

The defense mechanisms considered in this work are all referenced from either academic or practical domains. For instance, in [4] and [5], the authors apply the concept of rotating servers to improve system survivability. Extending this ideal, with the help of the Security Operation Center (SOC), the defender is capable of dynamically regulating the network's topology, such as the connections between nodes. Once there is a detected compromised node, the defender can filter out the traffic sourced from that node. Here, this kind of defense strategy is denoted as "Dynamic Topology Reconfiguration." Although this technique is effective in stalling attackers, it may severely jeopardize the quality of service. Therefore, a defender should carefully consider their options before applying this defense mechanism.

Other options involve virtualization techniques, which allow underlying physical resources to be shared between different Virtual Machines (VMs). The firmware that provides this virtualization is called a Virtual Machine Monitor (VMM). Since all access to hardware resources must go through the VMM, it becomes an ideal place to implement the Intrusion Prevention System (IPS) [11] [12] [16]. Therefore, the term VMM-IPS denotes an intrusion prevention system constructed within a VMM, protecting all VMs governed by the same VMM. For instance, a VMM can filter out malicious traffic to protect the system. However, this kind of mechanism, called local defense, may also result in false positives that filter out legitimate users. Therefore, it is assumed that there is a certain probability that this local defense service has a negative effect on quality of service.

Furthermore, while under attack using a VMM, the defender is able to request from a third party security service provider the signature of the attack. Once the signature is updated, all VMs and VMMs are immune to this particular attack. Nevertheless, because the VMM has total control of its VMs, compromising the VMM is the same as compromising all the VMs governed by it.

In addition to the signature, the concept of service oriented perspective is increasingly popular within the security domain. Providers are gradually preferring to perform security services remotely rather than selling local products. For example, in [17], the provider performs different levels of traffic inspection and filtering services from a cloud environment. Nonetheless, similar to local defense services, there are still chances that false positives will occur. Thus it is assumed that there is a certain probability that this strategy will still jeopardize QoS.

III. PROBLEM FORMULATION

A. Problem Description

In order to improve network survivability, the defender allocates finite resources on nodes during the planning phase, including installing a virtualization environment, setting up cloud security service software and establishing the VMM-IPS. While under attack, the defender is capable of immediately applying some defense strategies, such as requesting an attack signature, under quality of service constraints.

The defender may be an enterprise or a government administrator, and there are several core nodes providing services with different priorities. The detailed assumptions are listed in table 1.

TABLE I: PROBLEM ASSUMPTIONS

1.	There are multiple core nodes and services in the network.
2.	Each core node can provide only one specific service.
3.	Each service has different weight determined by the defender.
4.	There is a Security Operation Center (SOC) governing the network.
5.	The defender has perfect knowledge of network and can allocate resources or adopt defense solutions by the SOC.
6.	Attackers only have incomplete information about the network.
7.	Whether a node is compromised or not is determined by the revised contest success function.
8.	Only malicious nodal attacks are considered.

For attackers, each carries a distinct budget, capability and aggressiveness that match a general distribution. While selecting the next candidate to compromise, attackers depend on the situation at the moment to adopt corresponding criteria. According to [18], the authors propose several attack strategies, most of which are implemented in the attackers' selecting criteria which is used to choose next victim to compromise.

B. Mathematical Formulation

Based on the problem description, a corresponding mathematical formulation is proposed. The given parameters are listed in table 2, and the decision variables are presented in table 3. Since the previously discussed scenario is non-deterministic and involves significant amounts of randomness, it is quite difficult to formulate purely using mathematics. Consequently, the proposed model includes verbal notations, which are listed in table 4.

TABLE II: GIVEN PARAMETERS

Given Parameters	
Notation	Description
N	The index set of all nodes
C	The index set of all core nodes
L	The index set of all links
M	The index set of all level of virtual machine monitors (VMMs)
H	The index set of all level of cloud security services
S	The index set of all kinds of services
Q	The index set of all candidate nodes equipped with cloud security agent
B	The defender's total budget
E	All possible defense configurations, including defense resources allocations and defending strategies
Z	All possible attacker categories, including attacker attributes, corresponding strategies and transition rules
$\overline{A_{ij}}$	An attack configuration, including the attributes, corresponding strategies and transition rules of the attacker launches j^{th} attack on i^{th} service, where $i \in S$, $1 \le j \le F_i$
F_i	The total attacking times on i^{th} service for all attackers, where $i \in S$
w	The cost of constructing one intermediate node
o	The cost of constructing one core node
p	The cost of constructing each virtual machine (VM)
k_i	The maximum number of virtual machines on VMM level i, where $i \in M$
α_i	The weight of i^{th} service, where $i \in S$
c	The cost of setting a cloud security agent to one node
d	The ratio of defense enhanced on VMs and VMM when local defense is activated
r_i	The ratio of defense enhanced by applying level i cloud security services, where $i \in H$

TABLE III: DECISION VARIABLES

Decision Variables	
Notation	Description
$\overline{D_i}$	A defense configuration, including defense resource allocation and defending strategies on i^{th} service, where $i \in S$
$T_{ij}(\overline{D_i}, \overline{A_{ij}})$	1 if the attacker can achieve his goal successfully, and 0 otherwise, where $i \in S$, $1 \le j \le F_i$
n_i	The general defense resource allocated to node i, where $i \in N$
e	The total number of intermediate nodes
q_{ij}	The capacity of direct link between node i and j, where $i \in N$, $j \in N$
l_i	The number of VMs and level i VMM purchased, where $i \in M$
$v(l_i)$	The cost of constructing a level i VMM with l_i VMs, where $i \in M$
x_i	1 if node i is equipped with the cloud security agent, 0 otherwise, where $i \in N$
B_{NL}	The budget of constructing nodes and links
$B_{general}$	The budget of general defense resource
$B_{special}$	The budget of special defense resources
$B_{virtualization}$	The budget of virtualization
$B_{cloud\ agent}$	The budget of equipping cloud agents

TABLE IV: VERBAL NOTATIONS

Verbal Notations	
Notation	Description
G_{core_i}	Residual loading of each core node i, where $i \in C$
U_{link_i}	Link i utilization, where $i \in L$
K_{effect}	Negative effect caused by applying flawed signature
I_{effect}	Negative effect caused by applying dynamic topology reconfiguration
J_{effect}	Negative effect caused by applying flawed local defense
P_{effect}	Negative effect caused by applying cloud security service
O_{tocore}	The number of hops that legitimate users experienced from one of the edge nodes to core nodes
Y	The total compromise events
$W_{threshold}$	The predefined QoS threshold
W_{final}	The final QoS level at the end of an attack
$W(\cdot)$	The value of QoS determined by G_{core_i}, U_{link_j}, K_{effect}, I_{effect}, J_{effect} and O_{tocore}, where $i \in C$, $j \in L$
$\rho_{defense}$	The total defense resource of the shortest path from detected compromised nodes to one core node divided by total defense resource
τ_{hops}	The minimum number of hops from detected compromised nodes to one core node divided by the maximum number of hops from attacker's starting point to one core node
ω_{degree}	The link degree of one core node divided by the maximum link degree among all nodes in the topology
$s_{priority_i}$	The priority of service i divided by the highest priority of service in the network, where $i \in S$
$\beta_{threshold}$	The risk threshold of core nodes

$\beta(\cdot)$	The risk status of each core node which is the aggregation of defense resource, number of hops, link degree and service priority

The objective function (IP 1) stands for the defender's objective, which is to minimize the weighted service compromise probability by effectively adjusting the defense configuration. Evidently, any defense configuration that the defender applies should come out of all possible defense configurations; the corresponding constraint is (IP 1.1). Alternatively, (IP 1.2) represents a similar ideal for the attackers' side. (IP 1.3) means that the link capacity must be a positive quantity.

(IP 1.4) ~ (IP 1.9) jointly describe that the cost of constructing nodes, links, virtual machines, cloud security agents and deploying general defense resources during the planning phase should not violate budget limitations. (IP 1.10) ~ (IP 1.14) are integral and numerical constraints.

Objective Function:

$$\min_{\overline{D_i}} \frac{\sum_{i\in S}\left[\alpha_i \times \sum_{j=1}^{F_i} T_{ij}(\overline{D_i}, \overline{A_{ij}})\right]}{\sum_{i\in S}[\alpha_i \times F_i]} \quad \text{(IP 1)}$$

Constraints:

$$\overline{D_i} \in E \quad \forall i \in S \quad \text{(IP 1.1)}$$

$$\overline{A_{ij}} \in Z \quad \forall i \in S, 1 \le j \le \sum_{k\in S} F_k \quad \text{(IP 1.2)}$$

$$q_{ij} \ge 0 \quad \forall i, j \in N \quad \text{(IP 1.3)}$$

$$B_{NL} + B_{general} + B_{special} \le B \quad \text{(IP 1.4)}$$

$$B_{virtualization} + B_{cloudagent} \le B_{special} \quad \text{(IP 1.5)}$$

$$w \times e + o \times \|C\| + \frac{\sum_{i\in N}\sum_{j\in N} g(q_{ij})}{2} \le B_{NL} \quad \text{(IP 1.6)}$$

$$\sum_{i\in N} n_i \le B_{general} \quad \text{(IP 1.7)}$$

$$\sum_{i\in M} v(l_i) + p \times \sum_{i\in M} l_i \times k_i \le B_{virtualization} \quad \text{(IP 1.8)}$$

$$\sum_{i\in N} x_i \times c \le B_{cloudagent} \quad \text{(IP 1.9)}$$

$$g(q_{ij}) \ge 0 \quad \forall i, j \in N \quad \text{(IP 1.10)}$$

$$n_i \ge 0 \quad \forall i \in N \quad \text{(IP 1.11)}$$

$$v(l_i) \ge 0 \quad \forall i \in M \quad \text{(IP 1.12)}$$

$$e \ge 0 \quad \text{(IP 1.13)}$$

$$x_i = 0 \text{ or } 1 \quad \forall i \in N \quad \text{(IP 1.14)}$$

Verbal constraints :

$$\frac{\int_{y=1}^{Y}[W(G_{core_i}, U_{link_j}, K_{effect}, I_{effect}, J_{effect}, P_{effect}, O_{ncore})]\,dy}{Y} \ge W_{threshold}, \text{ where } i \in C, j \in L \quad \text{(IP 1.15)}$$

$$W_{final} \ge W_{threshold} \quad \text{(IP 1.16)}$$

The total cost of applying defending phase solutions must not violate budget limitation (IP 1.17)

$$\beta(\rho_{defense}, \tau_{hops}, \omega_{degree}, s_{priority_i}) \ge \beta_{threshold}, \text{ where } i \in S \quad \text{(IP 1.18)}$$

Beyond those constraints that are well-modeled mathematically, there are still some constraints that must be described verbally. (IP 1.17) refers to the budget constraint of the defense phase. While adopting any defense solution, the defender must consider related budget limitations. (IP 1.18) describes how all defending phase solutions are activated only if the risk level is higher than a predefined threshold.

IV. Computational Experiments

A. Simulation Environment

All simulations are programmed in the C language. The system parameters are listed in table 5. The evaluation times for each attack and defense scenario are determined by simulations, which are presented in the next section.

For defender-related parameters, grid, random and scale free topologies are applied to network types. The constructing algorithms of random and scale free networks are cited from [19] and [20]. The remaining parameters are presented in table 6.

For attacker-related parameters, three important attributes are considered, including total budget, capability, and aggressiveness. All of these attributes shown in table 7 are determined by a general distribution. In the following simulations, a normal distribution is applied for deciding the value of each attribute.

TABLE V. System Parameters

Parameter	Value
Compiler	GNU GCC
Evaluation Times for each Attack and Defense Scenario	70,000

TABLE VI: Defender Parameters

Parameter	Value	
Topology Type	Grid, Random, Scale-Free	
Topology Scale	Small	Medium
Number of Nodes	9	25
Number of Service(s)	1	2
Number of Total Core Node(s)	1	3
Total Budget for Network Construction and defense	500,000	1,000,000

TABLE VII: Attacker Parameters

Parameter	Value
Total Budget	Normal distribution with boundary (300,000 ~ 1,500,000)
Capability	Normal distribution with boundary (0 ~ 1)
Aggressiveness	Normal distribution with boundary (0 ~ 1)

B. Simulation Results

1) Convergence

In this work, the convergence of data is considered as the numerical stability. While the magnitude of data vibrations is within the acceptable interval, for example, 0.2%, the corresponding number of simulation times is set to be the evaluation times for each attack and defense scenario.

For each simulation, the horizontal axis represents the evaluation time, and the vertical axis stands for the network system compromise probability, which is the objective function of the proposed mathematical model. Figure 1 demonstrates that when the attack and defense scenario takes place on a 9 node grid network, the contest intensity equals 2. The fluctuation of the network compromise probability is less than 0.2% when evaluation times exceed 69,000. Based on this result, the evaluation time for each attack and defense scenario is determined to be 70,000.

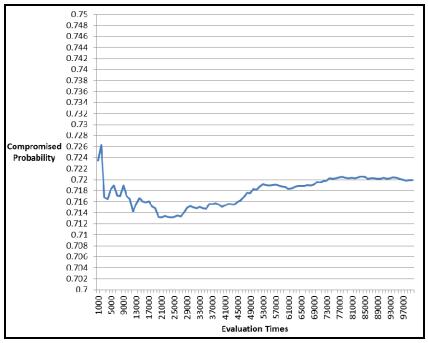

Figure 1. Convergence experiment on a 9 nodes grid network

2) Influence of Contest Intensity and Aggressiveness

As mentioned in the problem description, the contest intensity greatly influences the nature of an attack and defense scenario. However, there is no obvious trend for system compromise probability through different values of contest intensity [5] [6].

The result of these simulations is consistent with previous research [5], [6]. In figure 2, a 9 nodes scale free network is taken for example. As the value of contest intensity increases, the system compromise probability does not show an increasing or decreasing trend. Instead, the compromise probability is low when contest intensity equals 0.5 and 1.5. While the intensity is 1 and 2, the probability is high.

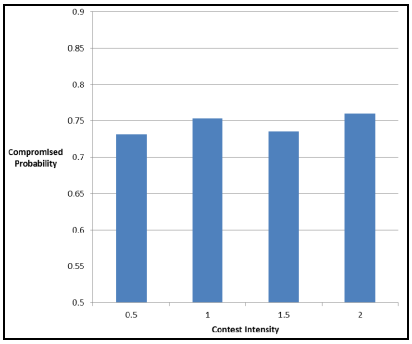

Figure 2. Influence of contest intensity on a 9 nodes scale-free network

However, if the influences of contest intensity and attacker aggressiveness are jointly considered, there are some interesting results that must be explained. As shown in figure 3, the attack and defense scenario is constructed on a 25 nodes grid network. If attacker aggressiveness is determined by a normal distribution with lower boundary 0.1 and upper boundary 0.9, there is no trend on compromise probability. Nevertheless, if the normal distribution of attacker aggressiveness is bounded by 0.1 ~ 0.5 or 0.5 ~ 0.9, there are obvious trends.

For the lower interval of attacker aggressiveness, the system compromise probability shows a decreasing trend through the value of contest intensity from 0.5 to 2. With regard to the higher interval of attacker aggressiveness, the compromise probability displays an increasing tendency.

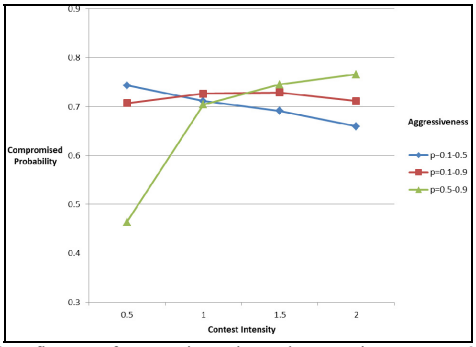

Figure 3. Influence of contest intensity and aggressiveness on a 25 nodes grid network

The same results can be observed in scale free and random networks. Corresponding data is shown in figure 4 and 5.

This result is because once the attacker determines his/her aggressiveness to a certain node, the corresponding cost can be calculated by the contest success function. With different values of contest intensity, the cost that one attacker must spend for compromising each node is distinct. In other words, when the value of contest intensity increases, the cost of compromising one node for a certain attacker exponentially decreases.

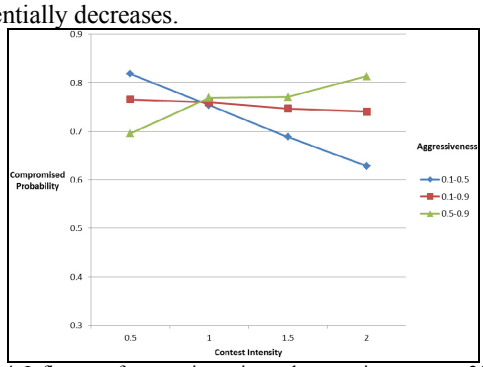

Figure 4. Influence of contest intensity and aggressiveness on a 25 nodes scale-free network

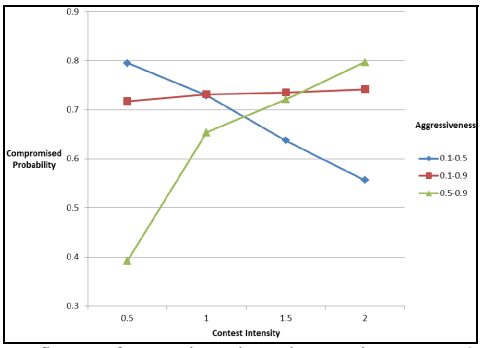

Figure 5. Influence of contest intensity and aggressiveness on a 25 nodes random network

Therefore, when the value of contest intensity is small, attackers with a high value of aggressiveness must spend a large portion of their budget to compromise every target. More specifically, attackers with high aggressiveness will

exhaust their budget at an early stage. They consume more resources to compromise fewer nodes with high success probability. Consequently, the system compromise probability is low.

In contrast, when the value of contest intensity is large, the cost of compromising each node for attackers with a high degree of aggressiveness is far lower than the scenario with a small value of contest intensity. Hence, even for attackers with high degrees of aggressiveness, the cost of compromising the whole system is affordable.

For attackers with low levels of aggressiveness, the system compromise probability is higher when the degree of contest intensity is small. Although these attackers may suffer from many attack failures and have to compromise again, the total attack cost is still lower than attackers with a high value of aggressiveness.

V. Discussion of Results

- *Defense in depth strategy is advantageous for defenders facing less aggressive attackers with "fight to win or die" circumstances*

Less aggressive attackers tend to spend small amounts of resources on compromising their target nodes. They prefer opportunism; failure in compromising intermediated nodes is acceptable. Spending large amounts of resources for compromising targets is not a proper strategy for such attackers.

While under "fight to win or die" circumstances (i.e., contest intensity is small [14]), the effectiveness of defensive resources exponentially decreases. Thus, a resource concentration strategy results in poor survivability.

Therefore, for the defender facing less aggressive attackers with "fight to win or die" circumstances, a defense in depth strategy maintains a better degree of survivability than resource concentration strategies.

- *Resource concentration strategy is advantageous for defense against aggressive attackers with "winner takes all" circumstances*

Aggressive attackers tend to spend large amounts of resources to compromise their target nodes with high success probability. They prefer pragmatism. A one-shot compromise of the targeted node is an ideal strategy. Spending fewer resources for each attack and accepting risk or failure is not acceptable for this attack type.

With "winner takes all" circumstances (i.e., contest intensity is large [15]), the effectiveness of defense resource is significant. The performance of resource concentration strategy is better than defense in depth strategy.

Hence, for the defender facing aggressive attackers with winner takes all circumstances, concentrating finite defense resources on a few important nodes is a better strategy for achieving higher survivability.

VI. Conclusion and Future Work

In summary, the degree of randomness involved in the problem discussed above creates a non-deterministic situation, for which various defense mechanisms are considered. This paper successfully models the problem as a mathematical formulation. Further, through the simulation results, effective defense strategies are provided to the defender. For future work, other types of defense mechanisms and attributes may be considered to increase the robustness of the modeled scenario.

Acknowledgment

This work was supported by the National Science Council, Taiwan, Republic of China (grant nos. NSC 100-2221-E-002-174).

References

[1] "State of Enterprise Security," Symantec Corporation, *Technical report*, 2010.

[2] "Global State of Information Security Survey," *PwC, Technical report*, 2011.

[3] R. J. Ellison, et al., "Survivable Network Systems: An Emerging Discipline," *Technical Report CMU/SEI-97-TR-013*, 1997 (Revised: May 1999).

[4] S. Skaperdas, "Contest success functions," *Economic Theory*, vol. 7, pp. 283-290, 1996.

[5] K. Hausken and G. Levitin, "Protection vs. false targets in series systems," *Reliability Engineering & System Safety*, vol. 94, pp. 973-981, 2009.

[6] G. Levitin and K. Hausken, "False targets efficiency in defense strategy," *European Journal of Operational Research*, vol. 194, pp. 155-162, 2009.

[7] Y. Huang, et al., "Incorruptible system self-cleansing for intrusion tolerance," *25th IEEE International Conference on Performance, Computing, and Communications (IPCCC)*, pp. 492-496, 2006.

[8] Y. Huang, et al., "Closing Cluster Attack Windows Through Server Redundancy and Rotations," *Sixth IEEE International Symposium on Cluster Computing and the Grid*, vol. 2, pp.21, 2006.

[9] H. E. Schaffer, "X as a Service, Cloud Computing, and the Need for Good Judgment," *IT Professional*, vol. 11, pp. 4-5, 2009.

[10] Johns, "Software as a Service - SaaS:Emerging trends in IT," (http://knol.google.com/k/johns/software-as-a-service-saas/54w8qsaycxa/2), 2008.

[11] VMware, "VMware vShieldTM Product Family," http://www.vmware.com/products/vshield/

[12] Trend Micro, "Trend Micro Deep Security," http://tw.trendmicro.com/tw/products/enterprise/deep-security/index.html

[13] C. Ryu, R. Sharman, H.R. Rao, S. Upadhyaya, "Security protection design for deception and real system regimes: A model and analysis," *European Journal of Operational Research*, Vol. 201, Issue 2, pp. 545-556, 2010.

[14] Jack Hirshleifer "Conflict and rent-seeking success functions - Ratio vs difference models of relative success," *Proc. Public Choice*, pp.101-112, 1989.

[15] Jack Hirshleifer "The Paradox of Power," *Proc. Economics and Politics*, Vol. 3, pp.177-200, 1993.

[16] P. M. Chen and B. D. Noble, "When Virtual Is Better Than Real," *Eighth Workshop on Hot Topics in Operating Systems*, 2001.

[17] Zscaler Products. http://www.zscaler.com/productsataglance.html

[18] F. Cohen, "Managing network security: Attack and defence strategies," *Network Security*, vol. 1999, pp. 7-11, 1999.

[19] J. Blitzstein and P. Diaconis, "A Sequential Importance Sampling Algorithm for Generating Random Graphs with Prescribed Degrees," *Internet Mathematics*, vol. 6, pp. 489-522, 2011.

[20] S. Nagaraja and R. Anderson, "Dynamic Topologies for Robust Scale-Free Networks," *Bio-Inspired Computing and Communication*, vol. 5151, pp. 411-426, 2008.