Maximization of Network Survivability under Malicious and Epidemic Attacks

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

Hui-Yu Chung
Department of Information Management
National Taiwan University
Taipei, Taiwan, R.O.C.
r99035@im.ntu.edu.tw

Jia-Ling Pan
Department of Information Management
National Taiwan University
Taipei, Taiwan, R.O.C.
r98041@im.ntu.edu.tw

***Abstract*—Due to the Internet's scalability and connectivity, enterprises and organizations increasingly rely upon it to provide services for customers. However, attackers intelligently attack enterprises and organizations through continuous vulnerability exploitation and advanced malware. Recently, assailants have applied the characteristics of fast propagation and epidemic attack infection to launch more deliberate attacks, by using obtained network topology information. This paper examines malicious and epidemic attacks, taking into account various defense mechanisms. Attackers are assumed to only have incomplete information regarding the target network, which raises the difficulty of solving this problem and renders the nature of the problem non-deterministic. Our purpose is to help defenders evaluate average network survivability when making defense-related decisions. This scenario is modeled as a mathematical formulation, and through our simulation results, meaningful and useful defense guidelines are proposed.**

Keywords: Defense Strategies; Survivability; Epidemic Attack; Incomplete Information;

I. INTRODUCTION

Due to the Internet's scalability and connectivity, enterprises can do business and provide services for their customers and business partners without geographic restrictions and time constraints. However, the losses owing to attacks rise quickly.

Given these challenges, how to evaluate the security status of certain systems becomes the first step of studying security-related issues. Many metrics, such as survivability, reliability, and dependability, are widely used. In this paper, we select survivability as the key metric to describe system status, because according to the definition, it adheres to a continuous viewpoint, rather than the binary form applied by traditional system security [1].

Our definition of survivability stems from [1], where the authors define survivability as "the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents...we use the term system in the broadest possible sense, including networks and large-scale systems of systems."

As mentioned previously, many enterprises nowadays create profit mainly by providing services, which is also the scenario considered in this paper; the metric of evaluating service status should take a continuous form [1] since the deterioration of service quality as a result of attack is not a binary form. Therefore, survivability is an ideal metric to evaluate system status in this paper.

In previous studies regarding survivability, many either consider a relatively simple topology structure or assume the attacker has complete information on the target network. For instance, in [2], the authors propose an optimal distribution of defense resources in a series system, rather than a network topology. Regarding [3], 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. This complete information assumption, although it helps a defender evaluate the worst case scenario, is unrealistic. In the real world, defenders face scenarios where they are surrounded by numerous attackers that vary by type and attributes. Thus, an assumption of incomplete information helps defenders evaluate a more realistic, common scenario. Although this assumption made in our paper raises the difficulty of the problem, since it makes the problem non-deterministic, it can help defenders evaluate average system survivability, which is an important metric for decision making.

Attack and defense mechanisms are another important issue. From an attack perspective, recent technological developments have allowed attackers to more efficiently and quickly compromise important hosts or networks by using malware with the ability to automatically send copies of itself to other computers on the network without any user intervention [4]. One instance of this is a worm, which is a self-replicating malicious computer program. By using a worm, attackers can obtain information about the targeted network in a short time period.

Fortunately from a defensive perspective, modern advances have also created mechanisms to deal with these threats. This paper examines several of these mechanisms, starting with a distributed information system that generates and distributes worm signatures [5] [6]. Other options include a containing technique named rate limiting, which filters suspicious traffic, and a trace back technique called worm origin identification [7] [8]. Furthermore, a defender can dynamically adjust the linking status by reconfiguring topology settings [9] [10] or raising the security level of their firewall, depending on the situation. However, for these mechanisms there are also unavoidable negative effects, such as false positives and negatives. Thus, in this paper, corresponding penalties are also considered. A detailed description of the above techniques is presented in the next section.

Given these problems, this paper first identifies the defense guidelines for defense resource allocation, as well as considers various attack/defense mechanisms and the quality of service constraints within attack and defense scenarios. It then provides a more realistic attack scenario by assuming that attackers have incomplete information on the target network.

II. RELATED WORK

A. Network attack and defense

In previous studies of network attack and defense, the determination of whether a node is compromised depends on the contest success function, originating from the rent-seeking problem of economic theory [11] [12]. The form of this contest success function is $\frac{T^m}{T^m + t^m}$ where t and T are the resources invested by each opposing player respectively and m is the contest intensity that determines the nature of the attack and defense scenario. In [13], the authors note that when $m < 1$, it belongs to a "fight to win or die" circumstance. When m increases, the effectiveness of the resources invested by both players also increases, until m approaches infinity. In the case of $m \to \infty$, this represents a "winner takes all" situation [11].

In adapting the contest success function for information warfare, the authors of [2] and [3] use it to determine whether a target node is compromised. T represents resources invested by an attacker, t stands for the defense resources deployed by the defender, and m remains the contest intensity.

All of the defense and attack mechanisms considered in this paper originate from either academia or the security industry. For instance, inspired by [9] and [10], the authors propose a mechanism for dynamically manipulating the connection status of a network to maximize network survivability.

Aligning with this concept, in this work, defenders can apply this technique to adjust the linking status of each node dynamically. In other words, when the attacker is approaching one of the core nodes, the defender can temporarily disconnect some links between certain nodes depending on the situation. However, in such cases the quality of service is clearly jeopardized by the disconnection. Thus a defender must evaluate carefully before activating this technique.

B. Epidemic attacks and defense

A network worm is a piece of malicious code that propagates over a network without human assistance and can actively initiate attacks independently or depending on file-sharing. Besides, according to [4], among attack types, worms have increased the most in prevalence over the past year.

Early worms were usually employed by attackers to jam and congest networks. With the development of more advanced programming techniques and vulnerability exploitation tools however, the functionality of worms can be very diverse and powerful. Worms nowadays not only propagate but also collect and transmit information back to the attacker [16].

After introducing the basic function of worms, the propagation model is the next important issue. There are many models originating from epidemiology, named epidemic models, that describe the propagation conditions or infection states of contagious diseases in a large community. Given various choices, this paper selects the Two-Factor model as a worm propagation model, because it is generic and widely applied [14].

III. PROBLEM FORMULATION

A. Problem Description

From the perspective of a defender, the objective is to protect provided services with a predefined level of quality of service by effectively allocating finite defense resources and timely launching defense mechanisms. Here, there are two stages of defense to consider: the planning stage and the defending stage.

In the planning stage, a defender can allocate general defense resources like a firewall, anti-virus software or intrusion detection system on each node to increase its robustness. During this stage, the locations of the distributed information sharing system should also be determined based on the number of hosts within an AS node.

In the defending stage, defenders can activate the unknown worm signature generation and distribution function, rate limiting mechanism, worm origin identification, firewall reconfiguration, and dynamic topology reconfiguration. However, generating signatures consumes defense resources, while the other four techniques decrease the quality of service because false positives can occur regardless of the technique, and thus reduce service quality. Therefore, a defender should deliberate carefully before activating them.

A common location to place a worm signature generation and distribution is a network boundary, such as a gateway or edge router. At a network boundary a detection system can inspect all traffic in and out of the network to discover any suspicious activity [16] [17]. Therefore, in this paper, worm-related defense mechanisms are constructed on an Autonomous System (AS) node. In other words, the network is viewed at the AS level.

For every defense mechanism applied in this work, the negative effects caused by a false positive and false negative are considered. The specific probability of a false positive and false negative regarding different defense techniques are referenced from previous studies, which are cited in the related work and computational experiments sections of this paper.

From the perspective of an attacker, the objective is to compromise services. During this process, worms are applied by attackers to clearly map topology and acquire defense related information. Inspired by [18], the attributes of attackers include budget, capability and aggressiveness, where budget is the total attack resources, capability stands

for the professions of each attacker, and aggressiveness is the preferred success probability when an attacker targets a certain node.

The cost of compromising a node is determined according to the aggressiveness and contest success function. Highly aggressive attackers tend to spend large amounts of attack resources to compromise the target node with a high success probability. Alternatively, less aggressive attackers prefer to invest few resources and accept the risk of failure.

While spreading worms, aggressive attackers tend to deploy high propagation speed worms, which help attackers rapidly gather topology and defense information but are easily detected and immured by the distributed information system. Less aggressive attackers prefer to deploy low propagation speed worms, which gather information slowly, but are relatively difficult to detect and immure.

Another attack type considered in this paper is social engineering, which is becoming increasingly popular. Here, before launching an attack, attackers spend resources to obtain information on the number of edge nodes or number of hops from each edge node to core nodes through social engineering.

Once an attacker compromises the target node successfully, he/she can determine whether to inject worms for gathering more topology information. The detailed assumptions for the scenario are listed in table 1.

Table 1: Problem Assumptions

Assumptions:

1. The network is viewed at the AS level.
2. The defender has complete information about the network.
3. There is an overlay network connecting distributed information sharing systems.
4. Attackers only have incomplete information about the target network.
5. A node is subject to attack only if a path exists from the attacker's position to that node, and all the intermediate nodes on the path have been compromised.
6. Whether a node is compromised is determined by the contest success function.
7. Attackers may inject the same worm if it has not yet be detected.
8. The statuses of all nodes are susceptible (*S*) before new types of worm are detected.
9. Only a nodal attack is considered.

B. Problem Formulation

The attack and defense scenario is formulated as a mathematical model. The corresponding given parameters and decision variables are shown in table 2 and table 3 respectively.

Table 2: 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
Q	The index set of all candidate nodes that is appropriate to deploy the distributed information sharing system
S	The index set of all types of services
α_i	The weight of i^{th} service, where $i \in S$
B	The defender's total budget
$B_{defending}$	The budget applied for defending stage.
$\mathcal{W}$	The cost of constructing one intermediate node
O	The cost of constructing one core node
d	The cost of deploying a distributed information sharing system to one node
E	All possible defense configurations, including defense resources allocation and defending strategies
Z	All possible attack configurations, including attacker's attributes, corresponding strategies and transition rules
$\overrightarrow{A_{ij}}$	An attack configuration, including attacker's 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 $i \in S$

Table 3: Decision Variables

Notation	Description
$\overrightarrow{D_i}$	An defense configuration, including defense resources allocation and defending strategies on i^{th} service, where $i \in S$
$T_{ij}(\overrightarrow{D_i}, \overrightarrow{A_{ij}})$	1 if the attacker achieve his goal successfully, and 0 otherwise, where $i \in S$, $1 \le j \le F_i$
$B_{nodelink}$	The budget spent on constructing nodes and links.
$B_{general}$	The budget spent for general defense resource
$B_{special}$	The budget spent for special defense resource
e	The total number of intermediate nodes
n_i	The general defense resources allocated to node i, where $i \in N$
x_i	1 if node i is equipped with the distributed information sharing system , and 0 otherwise, where $i \in Q$
q_{ij}	The capacity of direct link between node i and j, where $i \in N$, $j \in N$
$g(q_{ij})$	The cost of constructing a link from node i to node j with capacity q_{ij}, where $i \in N$, $j \in N$

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 4: Verbal Notations

Verbal Notations	
Notation	Description
G_{core_i}	Loading of each core node i, where $i \in C$
U_{link_i}	Link utilization of each link i, where $i \in L$
O_{tocore}	The number of hops legitimate users experienced from one boundary node to destination
I_e	Negative effect caused by applying dynamic topology reconfiguration
F_e	Negative effect caused by applying firewall reconfiguration
R_e	Negative effect caused by applying rate limiting
FP_e	Negative effect caused by false positive of worm detection
Y	The total compromise events
$W_{threshold}$	The predefined threshold regarding quality of service
W_{final}	The level of quality of service at the end of an attack
$W(\cdot)$	The value of quality of service is determined by G_{core_i}, U_{link_j}, O_{tocore}, I_e, F_e, R_e, and FP_e, where $i \in C$, $j \in L$
$\rho_{defense}$	The 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 position 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 provided by core nodes divided by the maximum service priority among core nodes in the topology, 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
$rate_{out}(A_i)$	The output traffic rate to node i, $i \in N$
$rate_{in}(A_i)$	The input traffic rate to node i, $i \in N$
$confidence$	The limit ratio of traffic rate

The problem is modeled into a mathematical formulation. The objective function represents the weighted service compromise probability. The denominator stands for the weighted value of each service attacked multiplied the weight of itself. The numerator is the weighted value of the services that have been compromised. The goal of the defender is to minimize this probability.

Objective function:

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

Mathematical constraints:

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

$\overrightarrow{A_{ij}} \in Z \quad \forall i \in S, 1 \le j \le F_i$ (IP 1.2)

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

$x_i = 0 \text{ or } 1 \quad \forall i \in N$ (IP 1.4)

$B_{nodelink} \ge 0$ (IP 1.5)

$B_{general} \ge 0$ (IP 1.6)

$B_{special} \ge 0$ (IP 1.7)

$n_i \ge 0 \quad \forall i \in N$ (IP 1.8)

$w \times e \ge 0$ (IP 1.9)

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

$B_{nodelink} + B_{general} + B_{special} + B_{defending} \le B$ (IP 1.11)

$$w \times e + o \times \|C\| + \frac{\sum_{i\in N}\sum_{j\in N} g(q_{ij})}{2} \le B_{nodelink} \quad \text{(IP 1.12)}$$

$$\sum_{i\in N} n_i \le B_{general} \quad \text{(IP 1.13)}$$

$$\sum_{i\in N} x_i \times d \le B_{special} \quad \text{(IP 1.14)}$$

Verbal constraints:

$$\frac{\int_{y=1}^{Y}[W(G_{core_i}, U_{link_j}, O_{tocore}, I_e, F_e, R_e, FP_e)]\,dy}{Y} \ge W_{threshold}, \ where\ i \in C,\ j \in L \quad \text{(IP 1.15)}$$

The performance reduction caused by compromised core nodes or activating defense mechanisms should not make legitimate users' QoS satisfaction violate IP 1.15. (IP 1.16)

W_{final} should not be lower than $W_{threshold}$ at the end of an attack. (IP 1.17)

when $\beta(\rho_{defense}, \tau_{hops}, \omega_{degree}, s_{priority_i}) \ge \beta_{threshold}$, $where\ i \in S$, the defender is able to activate dynamic topology reconfiguration to avoid the node being compromised. (IP 1.18)

$rate_{out}(A_i) = rate_{in}(A_i) * confidence$ (IP 1.19)

A node is subject to attack only if a path exists from the attacker's position to that node, and all the intermediate nodes on the path have been compromised. (IP 1.20)

IP 1.1 and IP 1.2 represent that both defense configuration and attack strategies should bounded in a feasible region. IP 1.20 is the continuity constraint.

IV. COMPUTATIONAL SIMULATIONS

A. Experiment Environment

In this section, the defender, attacker and system parameters are explained. For the topology generation algorithms, the construction of the random network is referenced from [24] and the scale-free network is referenced from [25]. The detailed parameters are represented in table 5.

Table 5: Defender Planning and Defending Parameters (k: one thousand)

Parameter	Value
Planning Parameters	
Topology Type	Scale-free, Random
Host Number of each AS Node [14]	800k , 900k , 1000k , 1100k , 1200k
Total Number of AS Nodes	25
Number of Service	2
Weight of Each Service	1, 2
Total Budget	1,000k
Defending Parameters	
Message Aggregate Time [5]	1 hour
Signature Generation False Positive Probability [5]	5%~8%
Signature Generation False Negative Probability [5]	1%~5%
Worm Origin Identification Trigger Condition	$\frac{I(t)}{\text{Number of AS node}}$

For attackers, the parameter setting includes profile and attacking stage parameters. Concerning the attackers' profile, inspired by [18], several important attributes are considered, including budget, capability and aggressiveness. All of these values are determined by a normal distribution with different lower and upper bounds. The aggressiveness refers to the preferred success probability of an attacker while compromising a target node.

During the attacking stage, there are two trigger conditions. The first is when the ratio of removed AS nodes in time *t* and all infected AS nodes in time *t* has increased to reach a certain threshold. The second trigger is when the ratio of the infection rate in time *t* and initial infection rate has decreased to reach a certain threshold. When both conditions are satisfied, the attacker prefers to inject a new worm type in the AS network. The corresponding parameter settings are listed in table 6.

Table 6: Attacker Preparation and Attack Parameters

Parameter	Value
Attackers Profile	
Budget	Normal distribution with lower bound 300k and upper bound 1,500k
Capability	Normal distribution with lower bound ε and upper bound 1
Aggressiveness	Normal distribution with lower bound ε and upper bound 1
Attacking Stage Parameters	
Time Estimation	
Node Attacking Time [19]	Normal distribution with lower bound 19 hours and upper bound 29 hours and mean is 24 hours
Node Infected Time [15]	Normal distribution with lower bound 5 hours and upper bound 11 hours and mean is 8 hours
Worm Injection Trigger Condition	
Inject New Worm	$\frac{R(t)}{I(t)+R(t)} \& \frac{\beta(t)}{\beta(0)}$
Inject Old Worm	$\frac{\beta(t)}{\beta(0)}$

For the system parameters presented in table 7, the value of contest intensity is adopted from [2]. The total evaluation times for one attack and defense scenario is determined by experiment. The details are discussed in the next section.

Table 7: System Parameters

Parameter	Value
Evaluation Times for each Attack and Defense Scenario (*M*)	30,000
Values of Contest Intensity (*m*)	0.5, 1, 1.5, 2

B. Simulation Results

Convergence is a critical issue in simulation experiments; According to [2], there is no ideal value of contest intensity for either the defender or attacker. Nonetheless, if the attackers' aggressiveness is jointly taken into consideration, there are some interesting observations.

1) Convergence

In this work, convergence is considered as numerical stability. If the perturbation of data is within an acceptable interval, for instance, 0.5%, the quantity of simulation times is large enough to make correct and meaningful conclusions.

As to the following figures in this subsection, for presentation purpose, one thousand evaluation results are summarized into a chunk and presented as one data point. The horizontal axis represents the total number of chunks, and the vertical axis stands for the network system

compromise probability, which is also the objective function of the proposed mathematical model. The contest intensity *m* is set to 2; attackers' aggressiveness is determined by a normal distribution with lower bound 0.1 and upper bound 0.9. Medium-size scale free topology is applied for the target network.

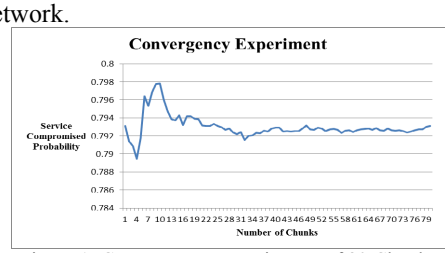

Figure 1: Convergence Experiments of 80 Chunks

An experiment of 80 chunks is constructed and corresponding results are demonstrated in figure 1. there is a stable trend around the 30th chunk. Accordingly, the ideal number of chunks for evaluation is set to 30, which means 30,000 evaluations for each attack and defense scenario. Thus, the value of *M* is determined to be 30,000.

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 [2].

If the influences of contest intensity and attacker aggressiveness are jointly considered, there are some interesting results that must be explained. A high value for contest intensity means a "winner takes all" circumstance, while a low value corresponds to "fight to win or die" circumstances [11] [13].

For figure 2 to figure 5, three value intervals of aggressiveness governed by a normal distribution are divided for comparison. For the interval with lower bound 0.1 and upper bound 0.5, corresponding attackers tend to spend less resource on compromising nodes and take the risk of failure. As to the interval with lower bound 0.5 and upper bound 0.9, corresponding attackers prefer spend more resources for a one shot compromise. Lastly, the interval with lower bound 0.1 and upper bound 0.9 is implemented as an average case for comparison.

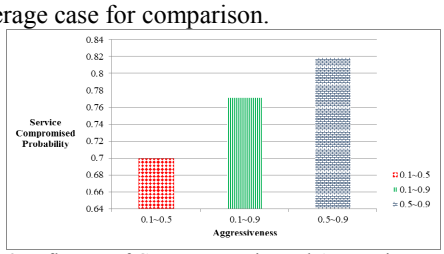

Figure 2: Influence of Contest Intensity and Aggressiveness under Contest Intensity Equals to 2

For a relatively high value of contest intensity, as shown in figure 2 and 3, aggressive attackers have more edge than less aggressive ones. Aggressive attackers tend to spend more resources, therefore achieving higher success probability.

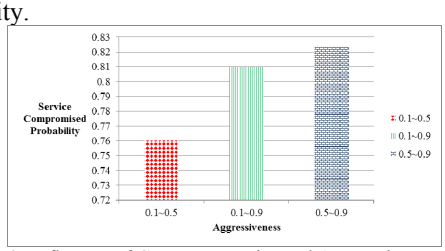

Figure 3: Influence of Contest Intensity and Aggressiveness under Contest Intensity Equals to 1.5

Also, when the contest intensity becomes smaller, as in the results shown in figure 2 and 3, the differences among each aggressiveness type decrease.

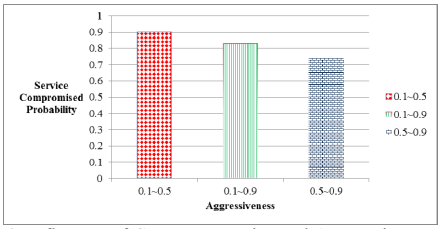

Figure 4: Influence of Contest Intensity and Aggressiveness under Contest Intensity Equals to 1

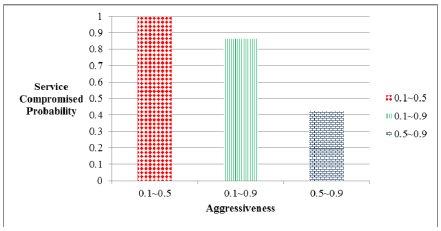

Figure 5: Influence of Contest Intensity and Aggressiveness under Contest Intensity Equals to 0.5

As a result, for relative small values of contest intensity, shown in figure 4 and 5, less aggressive attackers achieve higher success probability. Additionally, the significance of resources invested by either the defender or attacker is insignificant, which provides leverage to less aggressive attackers. The synergy of worms and the corresponding information relayed to attackers is discussed in the next section.

V. DISCUSSION OF THE RESULTS

According to the simulation results, this section proposes several meaningful defense strategies for defender to maximize the survivability of the network.

- *The defender should focus on defending aggressive attackers under "winner takes all" circumstances, since the synergy of worm and topology information is significant to these attackers*

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 [11]), the effectiveness of resources invested either by a defender or attacker is significant. Structure information on topology plays an important role. With a clear map of routes from compromised nodes to core nodes, the attackers can determine and choose the most advantageous path, for instance, the path with minimum defense resources allocated.

Through worms, attackers can gather topology information during an attack. The synergy is significant to aggressive attackers under "winner takes all" circumstances, since the cost of compromising target nodes with high success probability is affordable for attackers.

Hence, under "winner takes all" circumstances, the defender should focus on defending against aggressive attackers, since the synergy of worm and topology information is significant to them.

- *The defender should focus on defending less aggressive attackers under "fight to win or die" circumstances since the synergy of worm and topology information is significant to these attackers*

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.

Under "fight to win or die" circumstances (i.e., contest intensity is small [13]), the effectiveness of defensive resources exponentially decreases. Although topology information still plays a critical role, the synergy is significant for less aggressive attackers rather than aggressive attackers. Even if aggressive attackers figure out the shortest path to the core nodes, the corresponding cost of compromising nodes with high success probability is unaffordable.

The explanation is that under "fight to win or die" circumstance, if attackers prefer a high success probability, the cost of compromising intermediate nodes increase exponentially since the contest intensity is the exponent of the contest success function. Therefore, aggressive attackers exhaust their budget at an early, stage even though they target the lowest cost path.

In contrast, by targeting the lowest cost path, less aggressive attackers tend to take chances. They expect that the cost of compromising nodes is far lower than aggressive attackers, which is affordable. Therefore, under "fight to win or die" circumstances, the defender should focus on defending less aggressive attackers since the synergy of worm and topology information is significant to them.

VI. Conclusion and Future Work

In summary, this paper examines the non-deterministic problem of considering various defense mechanisms under quality of service constraints. Through the simulation results, effective defense strategies are provided.

For future work, other types of attack (for instance, distributed denial-of-service) and defense mechanisms and attributes (such as deception based mechanisms) may be considered to enrich 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] J. McHugh, N.R. Mead, R.C. Linger, R.J. Ellison and T. Longstaff, "Survivable Network Analysis Method", *Technical Report CMU/SEI-2000-TR-013*, September 2000.

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

[3] 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.

[4] D. Anselmi, J. Kuo, R. Boscovich et al., "Microsoft Security Intelligence Report", *Microsoft*, Volume 9, 2010.

[5] G. Zhang and M. Parashar, "Cooperative detection and protection against network attacks using decentralized information sharing", *Cluster Computing*, Volume 13, Number 1, Pages 67-86, 2010.

[6] R. Moskovitch, Y. Elovici and L. Rokach, "Detection of unknown computer worms based on behavioral classification of the host", *Computational Statistics & Data Analysis*, Volume 52, Issue 9, Pages 4544-4566, May 2008.

[7] Y. Xie, V. Sekar, D.A. Maltz, M.K. Reiter and H. Zhang, "Worm Origin Identification Using Random Moonwalks", *2005 IEEE Symposium on Security and Privacy*, May 2005.

[8] Y. Xie, V. Sekar, M.K. Reiter and H. Zhang, "Forensic Analysis for Epidemic Attacks in Federated Networks", *Proceedings of the 2006 14th IEEE International Conference on Network Protocols*, November 2006.

[9] Y. Huang, D. Arsenault and A. Sood, "Closing Cluster Attack Windows Through Server Redundancy and Rotations", *Proceedings of the 6th IEEE International Symposium on Cluster Computing and the Grid*, 2006.

[10] Y. Huang, D. Arsenault and A. Sood, "Incorruptible Self-Cleansing Intrusion Tolerance and Its Application to DNS Security", *Journal of Networks*, Volume 1, Number 5, Pages 21-30, October 2006.

[11] Jack Hirshleifer "Conflict and rent-seeking success functions – Ratio vs difference models of relative success," Proc. *Public Choice 63*, 1989, pp.101-112

[12] S. Skaperdas, "Contest success functions", *Economic Theory*, Volume 7, Number 2, Pages 283–290, 1996.

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

[14] Eugene H. Spafford, "The Internet Worm Program: An Analysis", *Purdue Technical Report CSD-TR-823*, Pages 1-29, 1988.

[15] C.C. Zou, W. Gong and D. Towsley, "Code Red Worm Propagation Modeling and Analysis", *9th ACM Symposium on Computer and Communication Security*, Pages 138-147, 2002.

[16] P. Li, M. Salour and X. Su, "A Survey of Internet Worm Detection and Containment", *IEEE Communications Surveys & Tutorials*, Volume 10, Issue 1, Pages 20-35, 2008

[17] C. Wong, C. Wang, D. Song, S. Bielski and G.R. Ganger, "Dynamic Quarantine of Internet Worms", *Proceedings of the 2004 International Conference on Dependable Systems and Networks*, 2004.

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

[19] D. J. Leversage and E. J. Byres, "Estimating a System's Mean Time-to-Compromise", *IEEE Security & Privacy*, Volume 6, Number 1, Pages 52-60, January/February 2008.