2008 International Conference on Computational Intelligence and Security

A Near-Optimal Redundancy Allocation Strategy that Minimizes a System's Vulnerability to Hazardous Events and Malicious Attacks

Frank Yeong-Sung Lin
Department of Information Management
National Taiwan University
yslin@im.ntu.edu.tw

Po-Hao Tsang
Department of Information Management
National Taiwan University
d91002@im.ntu.edu.tw

Kun-Dao Jiang
Department of Information Management
National Taiwan University
r94018@im.ntu.edu.tw

Abstract

Delivering continuous services in information infrastructures is a major challenge. For system or network administrators, redundancy allocation is one of the best strategies to ensure service continuity in the context of risk management, where the ultimate goal is to reduce potential threats to an acceptable level with limited resources. In this paper, we address the problem of reducing the vulnerability of a network to hazardous events and malicious attacks. We analyze the problem as a mixed, nonlinear, integer programming optimization problem with a min-max format. The solution approach, which is based on Lagrangean Relaxation and a subgradient method, solves this complicated problem effectively. We evaluate the scalability and applicability of the proposed heuristic via computational experiments on different network topologies and scales.

1. Introduction

Modern organizations are becoming increasingly reliant on information infrastructures, especially the Internet, to run their daily business operations and services. The goal of delivering continuous services, however, poses a major challenge. Apart from the threat of malicious attacks, hazardous events, such as earthquakes, flooding, blizzards, and hurricanes, can have a strong impact on information security. Hence, from a business perspective, information security has expanded toward risk management and evolved into a brand-new concept of survivability, which focuses on the availability of systems and the continuity of services [1].

The advantage of fault tolerance is that system or network administrators can deploy redundant components. This is one of the best strategies to ensure service continuity in the context of risk management, where the ultimate goal is to reduce potential threats to an acceptable level with limited resources. The objective of the redundancy allocation problem (RAP) is to determine an optimal design strategy to maximize system survivability and reliability under the consideration of system constraints. In general, RAP is classified as NP-hard in terms of computational complexity due to its nonlinearity, nonconvexity, and integrality [2].

Many researchers have considered RAP under different scenarios, assumptions, constraints, and solution approaches. For example, the discrete optimization model proposed in [3] allocates redundancy to critical IT functions for disaster recovery planning, while the model in [4] comprises multiple, functionally equivalent components available for use in the system. Ha et al. propose a new heuristic based on a tree structure to solve the general RAP in reliability optimization [5]. All the above works formulate RAP as a maximization problem, where the objective is to maximize system reliability. However, Jose et al. formulate RAP from a different perspective in that the objective is to maximize the minimized subsystem reliability in a series-parallel system [6].

In the realm of RAP, most studies focus on parallel-system design or disaster recovery plans without considering network configuration. Moreover, they seldom consider the impact of malicious attacks, which have different characteristics from natural disasters. To address this research gap, we propose a novel redundancy allocation scheme, which considers the impact of targeted malicious attacks, and apply the concept to network configuration design. To the best of our knowledge, this is one of the first papers to model malicious attacks with traditional RAPs. Previous research has shown that attempts to model attack-defense scenarios in an abstract, mathematical way are non-trivial [7, 8]. In addition, the issues remain unsolved [9].

The remainder of this paper is organized as follows. In Section 2, we formulate the primal RAPMA (Redundancy Allocation Problem considering Malicious Attacks) and ARS (Attack Redundancy Strategy) problems. In Section 3, we propose a Lagrangean Relaxation-based solution approach to the problems. The results of computational experiments conducted to evaluate the proposed solution are reported in Section 4. Finally, in Section 5, we summarize our conclusions and indicate possible future research directions.

2. Problem Formulation

2.1 Problem Description and Assumptions

978-0-7695-3508-1/08 $25.00 © 2008 IEEE
DOI 10.1109/CIS.2008.142

The problem we address is: How can network administrators deploy redundant components to minimize the vulnerability of a network to hazardous events and malicious attacks? The ultimate goal is to provide continuous services and improve survivability by deploying redundant components. Obviously, an attacker will try to compromise as many network nodes as possible with limited attack resources. Research shows that attackers and defenders constantly change their respective strategies – a process that can be likened to the use of a lance and a targe.

We model the defined problem as a min-max problem in order to formulate attack-defense scenarios. The inner problem, defined by the ARS model, represents that an attacker tries to maximize a network's vulnerability to hazardous events by identifying attack targets and formulating efficient attack budget allocation strategies. The outer problem, defined by the RAPMA model, represents that, to minimize the maximized total vulnerability, a defender must deploy redundant components to provide continuous services.

We assume that each node in a network is composed of just one primary component and several redundant components. To compromise a node, an attacker must find a suitable path to it and compromise all the intermediate nodes on that path. Furthermore, a node is considered compromised if and only if the primary component of the node has been compromised by applying an attack budget that is equal to or more than a predefined threshold. Note that an attacker will never try to compromise redundant components if the associated primary component has not been compromised. To consider the worst case scenario, we assume both the attacker and the defender are smart enough to obtain complete information about the targeted network in advance.

2.2 Problem Formulation for the RAPMA Model

We now define the notations used in this paper and formulate the problem.

Table 1.
Given Parameters

Notation	Description
N	The index set of all nodes in the network
B	The defender's total budget
A	The attacker's total budget
W	The index set of all Origin-Destination (O-D) pairs, where the origin is the node s that the attacker occupies and the destination is a node i in the network (where $i, s \in N$)
P_w	The index set of all candidate paths for an O-D pair w, where $w \in W$
δ_{pi}	The indicator function, which is 1 if node i is on path p, and 0 otherwise (where $i \in N$, $p \in P_w$)
D	The index set of all potentially hazardous events with probability P_d, where $P_d \in (0, 1)$, $\sum P_d = 1$
r_i	The index set of all components that provide the same service function in node i, where $i \in N$
$level_i$	The minimum number of redundancy levels of node i predefined by the defender, where $i \in N$
c_{im}	The cost of component m of node i, where $i \in N$, $m \in r_i$
$g_{im}(c_{im})$	The minimum threshold of the attack budget required to compromise a component m of node i, where $i \in N$, $m \in r_i$

Table 2.
Decision Variables

Notation	Description
α_{im}	1 if a component m of node i is selected to play the role of primary component for the provision of services, and 0 otherwise (where $i \in N$, $m \in r_i$)
β_{im}	1 if a component m of node i is selected as a redundant component to provide the function of fault tolerance, and 0 otherwise (where $i \in N$, $m \in r_i$)
g_{im}	The attack budget allocated to a component m of node i, where $i \in N$, $m \in r_i$
$f_{imd}(g_{im})$	The vulnerability of a component m of node i to a hazardous event d, where $i \in N$, $m \in r_i$, $d \in D$, $f_{imd}(g_{im}) \in (0, 1)$
y_i	1 if the node i is compromised, and 0 otherwise (where $i \in N$)
x_p	1 if the path p is selected as the attack path, and 0 otherwise (where $p \in P_w$)

Objective function:

$$\min_{\alpha_{im},\beta_{im}} \max_{g_{im}} \sum_{d \in D} P_d \left(1 - \sum_{i \in N} \left(1 - \prod_{m \in r_i} f_{imd}(g_{im})^{\alpha_{im}+\beta_{im}}\right)\right) \quad \text{(IP 1)}$$

subject to:

$$\sum_{w \in W} \sum_{p \in P_w} x_p \delta_{pi} \le \left(|N| - 1\right) y_i \qquad \forall i \in N \quad \text{(IP 1.1)}$$

$$\sum_{p \in P_w} x_p = y_i \qquad \forall i \in N, w = (s, i) \quad \text{(IP 1.2)}$$

$$\sum_{p \in P_w} x_p \le 1 \qquad \forall w \in W \quad \text{(IP 1.3)}$$

$$\sum_{m \in r_i} \frac{\alpha_{im} g_{im}}{g_{im}(c_{im})} \ge y_i \qquad \forall i \in N \quad \text{(IP 1.4)}$$

$$x_p = 0 \text{ or } 1 \qquad \forall p \in P_w, w \in W \quad \text{(IP 1.5)}$$

$$y_i = 0 \text{ or } 1 \qquad \forall i \in N \quad \text{(IP 1.6)}$$

$$\alpha_{im} = 0 \text{ or } 1 \qquad \forall i \in N, m \in r_i \quad \text{(IP 1.7)}$$

$$\beta_{im} = 0 \text{ or } 1 \qquad \forall i \in N, m \in r_i \quad \text{(IP 1.8)}$$

$$\alpha_{im} + \beta_{im} \le 1 \qquad \forall i \in N, m \in r_i \quad \text{(IP 1.9)}$$

$$\sum_{m \in r_i} \alpha_{im} = 1 \qquad \forall i \in N \quad \text{(IP 1.10)}$$

$$\sum_{m\in r_i} \beta_{im} \geq level_i \qquad \forall i \in N \qquad \text{(IP 1.11)}$$

$$0 \leq \sum_{m\in r_i} c_{im}\left(\alpha_{im}+\beta_{im}\right) \leq B \qquad \forall i \in N \qquad \text{(IP 1.12)}$$

$$\sum_{i\in N}\sum_{m\in r_i} c_{im}\left(\alpha_{im}+\beta_{im}\right) \leq B \qquad \text{(IP 1.13)}$$

$$\sum_{i\in N}\sum_{m\in r_i} g_{im} \leq A \qquad \text{(IP 1.14)}$$

$$0 \leq g_{im} \leq A \qquad \forall i \in N, m \in r_i \qquad \text{(IP 1.15)}$$

From the defender's perspective, the objective function is to minimize the network's maximized vulnerability to hazardous events. Constraints (IP 1.1) ~ (IP 1.6) jointly require that when a node is chosen for attack, there must be exactly one path from the attacker's initial position, *s*, to that node, and each node on the path must have been compromised. These constraints are called "continuity constraints." Constraint (IP 1.4) stipulates that a node is considered to be compromised if and only if the attack budget applied to it is more than or equal to the minimum threshold. Constraint (IP 1.9) requires that the roles of components are mutually exclusive. The other constraints are straightforward.

2.3 Problem Formulation for the ARS Model

To solve the primal RAPMA problem, we first analyze its inner problem, denoted as (IP 2), and the ARS model. The given parameters and decision variables of the ARS model are the same as those of the RAPMA model, except that the decision variables α_{im} and β_{im} become given parameters in the ARS model. Constraints (IP 2.1)~(IP 2.6) and (IP 2.7)~(IP 2.8) of the ARS model are the same as (IP 1.1)~(IP 1.6) and (IP 1.14)~(IP 1.15) respectively.

3. Solution Approaches

3.1 Solution Approach for the ARS Model

The original objective function in (IP 2) is a value calculated by a series of products, which makes the problem complicated due to its non-linearity. Hence, we transform it into logarithmic form without changing its optimality. We also assume that $f_{imd}(g_{im})$ follows an exponential distribution with λ, which indicates that the marginal vulnerability will be reduced by the additional budget allocated to a component. The transformation procedure and the result are as follows:

$$\max_{g_{im}} \sum_{d\in D} P_d\left(1-\sum_{i\in N}\left(1-\prod_{m\in r_i} f_{imd}(g_{im})^{\alpha_{im}+\beta_{im}}\right)\right)$$

$$= \min_{g_{im}} -\left(\sum_{d\in D} P_d\left(1-\sum_{i\in N}\left(1-\prod_{m\in r_i} f_{imd}(g_{im})^{\alpha_{im}+\beta_{im}}\right)\right)\right)$$

$$\Rightarrow \min_{g_{im}} -\left(\sum_{d\in D} P_d\left(1-\sum_{i\in N}\left(1-\sum_{m\in r_i}(\alpha_{im}+\beta_{im})\ln(f_{imd}(g_{im}))\right)\right)\right)$$

$$\Rightarrow \min_{g_{im}} -\left(\sum_{d\in D} P_d\left(1-\sum_{i\in N}\left(1-\sum_{m\in r_i}(\alpha_{im}+\beta_{im})\ln(1-e^{-\lambda_{imd}g_{im}})\right)\right)\right)$$

By applying the Lagrangean relaxation method [10] with a vector of Lagrangean multipliers, we can transform (IP 2) into the following Lagrangean relaxation problem (LR 1), where constraints (IP 2-1), (IP 2-2), and (IP 2-4) are relaxed.

$$\begin{aligned} &Z_D(\mu_1,\mu_2,\mu_3) \\ &= \min_{g_{im}} -\left(\sum_{d\in D} P_d\left(1-\sum_{i\in N}\left(1-\sum_{m\in r_i}(\alpha_{im}+\beta_{im})\ln(1-e^{-\lambda_{imd}g_{im}})\right)\right)\right) \\ &+\sum_{i\in N}\mu_i^1\left[\sum_{w\in W}\sum_{p\in P_w} x_p\delta_{pi} - (|N|-1)y_i\right] + \sum_{i\in N}\mu_i^2\left[\sum_{p\in P_{(s,i)}} x_p - y_i\right] \\ &+\sum_{i\in N}\mu_i^3\left[y_i - \sum_{m\in r_i}\frac{\alpha_{im}g_{im}}{\hat{g}_{im}(c_{im})}\right] \end{aligned} \qquad \text{(LR 1)}$$

subject to:

$$\sum_{p\in P_w} x_p \leq 1 \qquad \forall w \in W \qquad \text{(LR 1.1)}$$

$$x_p = 0 \text{ or } 1 \qquad \forall p \in P_w, w \in W \qquad \text{(LR 1.2)}$$

$$y_i = 0 \text{ or } 1 \qquad \forall i \in N \qquad \text{(LR 1.3)}$$

$$\sum_{i\in N}\sum_{m\in r_i} g_{im} \leq A \qquad \text{(LR 1.4)}$$

$$0 \leq g_{im} \leq A \qquad \forall i \in N, m \in r_i \qquad \text{(LR 1.5)}$$

By definition, μ_1, μ_2, and μ_3 are the vectors of $\{\mu_i^1\}$, $\{\mu_i^2\}$, and $\{\mu_i^3\}$ respectively, where μ^1 and μ^3 are non-negative and μ^2 is unrestricted. To solve (LR 1) optimally, we decompose it into three independent and easily solvable subproblems as follows.

Subproblem 1 (related to decision variable x_p)

$$\min \sum_{i\in N}\sum_{w\in W}\sum_{p\in P_w} \mu_i^1 x_p\delta_{pi} + \sum_{i\in N}\sum_{p\in P_{(s,i)}} \mu_i^2 x_p \qquad \text{(SUB 1)}$$

subject to (LR 1.1) and (LR 1.2).

As shown in TABLE I, each O-D pair *w* originates from an attacker's position, *s*, and ends at a target node *i*, where *i*, *s*$\in$*N*. Therefore, (SUB 1) can be transformed to (SUB 1') as follows.

$$\min \sum_{i\in N}\sum_{w\in W}\sum_{p\in P_w} \mu_i^1 x_p\delta_{pi} + \sum_{w\in W}\sum_{p\in P_w} \mu_i^2 x_p + \sum_{p\in P_{(s,s)}} \mu_s^2 x_p \qquad \text{(SUB 1')}$$

subject to (LR 1.1) and (LR 1.2).

The last term can be ignored because no path starts and ends at the same node. After the transformation, (SUB 1') can be decomposed into a series of |*W*| independent subproblems whose objective functions take the following form:

$$\min \sum_{p \in P_w} \left(\sum_{j \in N} \mu_j^1 \delta_{pj} + \mu_i^2\right) x_p \qquad \text{(SUB 1'')}$$

(SUB 1'') can be considered a minimum cost path problem with node costs ($\mu_j^1 \delta_{pj} + \mu_i^2$). Because of the non-negative costs, we can apply Dijkstra's shortest path algorithm to optimally solve this subproblem. The time complexity of (SUB 1) is $O(|N|^2)$ because the source of each path is the same and Dijkstra's algorithm only needs to be implemented once.

Subproblem 1.2 (related to decision variables y_i)

$$\min \sum_{i \in N} -\left(\mu_i^2 + \mu_i^3 - \mu_i^1 \left(|N| - 1\right)\right) y_i \qquad \text{(SUB 2)}$$

subject to (LR 1.3).

(SUB 2) can be further decomposed into a series of $|N|$ independent subproblems that can be solved optimally. Obviously, to obtain the optimal solution to this subproblem, we only set the value of y_i with a corresponding negative coefficient to 1. The time complexity of (SUB 2) is $O(|N|)$.

Subproblem 1.3 (related to decision variables g_{im})

$$\min_{g_{im}} -\left(\sum_{d \in D} p_d \left(1 - \sum_{i \in N}\left(1 - \sum_{m \in r_i} (\alpha_{im} + \beta_{im}) \ln\left(1 - e^{-\lambda_{ind} g_{im}}\right)\right)\right)\right) - \sum_{i \in N} \mu_i^3 \sum_{m \in r_i} \frac{\alpha_{im} g_{im}}{\hat{g}_{im}(c_{im})} \qquad \text{(SUB 3)}$$

subject to (LR 1.4) and (LR 1.5).

(SUB 3), is a typical fractional (continuous) knapsack problem, which we solve optimally by using the dynamic programming technique. Initially, the problem is divided into A phases and exactly one unit of the attack budget is allocated in each phase. Obviously, a "precious" resource will be allocated to a component that can contribute the greatest value to the objective function in each phase. The solution procedure is repeated until all of the attacker's resources are exhausted. The total time complexity of (SUB 3) is $O(A|C|)$, where C is the number of components and A is the total attack budget.

According to the weak Lagrangean duality theorem [10], the optimal value of the problem (LR 1) is, by its nature, the lower bound (for minimization problems) of the objective function's value in the primal problem (IP 2). The tightest Lagrangean lower bound can be derived by tuning the Lagrangean multipliers, i.e., by maximizing the (LR 1) problem. Although there are several ways to solve this problem, the subgradient optimization technique [10] is the most popular.

Getting Primal Feasible Solutions

The solutions to (LR 1) and the multipliers provide some hints about deriving a heuristic to improve the solution quality of (IP 2). Here, we describe our proposed heuristic. The solution of (SUB 1) is considered as an initial attack strategy for sequential adjustment. If the strategy satisfies all constraints on an attacker's behavior, it will form the trunk of the ultimate attack tree. However, if the attack strategy violates any of the problem's constraints, the wasted attack budget, which has been allocated to a leaf node, will be recycled and reallocated to uncompromised nodes according to the associated weight

$$\sum_{i \in N} \sum_{w \in W} \sum_{p \in P_w} x_p \delta_{pi} .$$

After the main attack tree has been constructed, any residual attack budget will be allocated to the reachable redundant components, which are associated with the compromised nodes, according to each node's side effect on the objective function. Finally, a collection of primal feasible solutions is found.

3.2 Solution Approach for the RAPMA Model

Since it is assumed that an attacker and a defender have complete information about the "battle", each one is capable of maximizing his benefits based on his opponent's strategy. In the ARS model, all decision variables about the defense strategy are assumed to be known in advance; therefore, the attacker can launch malicious attacks to paralyze the network system. After the ARS model is solved, its solution, which can be regarded as the attacker's behavior, becomes the input of the RAPMA model. In this phase, all decision variables related to the attacker's behavior become known; as a result, the defender can dynamically deploy redundant components to strengthen the survivability of the whole network.

To solve the RAPMA model, we propose a degree-based algorithm. Initially, all nodes are sorted in descending order according to the associated weight

$$\sum_{i \in N} \sum_{w \in W} \sum_{p \in P_w} x_p \delta_{pi} .$$

A node with a higher weight indicates that the node is relatively important to the attacker when he launches an attack on the network. If the attacker successfully compromises the node, we upgrade its protection level, i.e., more defense budget will be allocated to it; otherwise, we downgrade it and recycle the allocated defense budget. After the amount of defense budget allocated to the primary components has been determined, any residual budget will be allocated to redundant components to maximize their survivability according to their contribution to the network's protection.

4. Computational Experiments

4.1 Experiment Environments

We choose six popular network topologies, i.e., grid, cellular, random, ring, tree, and star networks, for our experiments to verify the scalability and applicability of our proposed solution approach. The experiments can be divided into two parts; those for the ARS model and those for the RAPMA model. In the first part, we compare the performance of two simple algorithms, namely a minimum cost spanning tree algorithm (SA1) and a greedy-based algorithm (SA2), with that of our proposed heuristic. In the second part, we compare a uniform-based budget allocation strategy (B1) and a damage-based budget allocation strategy (B2) with our proposed heuristic.

4.2 Experiment Results for the ARS Model

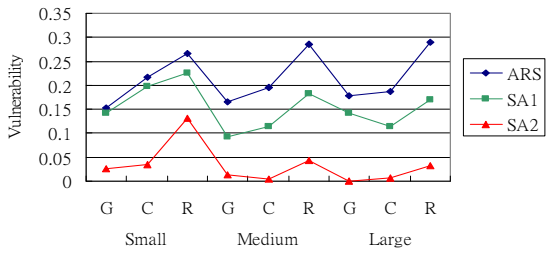

Figure 1. Vulnerability of Different Network Topologies at Different Scales to Verify Scalability (G: Grid, C: Cellular, R: Random; Small: 16 nodes, Medium: 64 nodes, Large: 196 nodes)

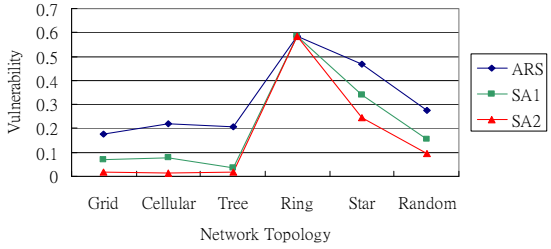

Figure 2. Vulnerability of Different Medium-size Network Topologies (49 nodes) to Verify Applicability

In Figures 1 and 2, "Vulnerability" represents the possibility that hazardous events might cripple the whole network. From Figure 1, we observe that, in every network topology and at every scale, our proposed heuristic outperforms SA1 and SA2, which only consider local information. The reason is that our proposed heuristic makes use of hints provided by Lagrangean Relaxation to constantly adjust its direction based on a global perspective. Hence, the solution quality is definitely better than that of the two simple algorithms. The graph in Figure 2 shows that our heuristic is applicable to a variety of topologies. We also observe that SA1, SA2, and our heuristic adopt the same attack strategy in a ring network. This may because, in a ring network, each node only has one adjacent neighbor; therefore, no matter which heuristic (with the same total attack budget) we adopt, only one kind of solution will be obtained.

4.3 Experiment Results for the RAPMA Model

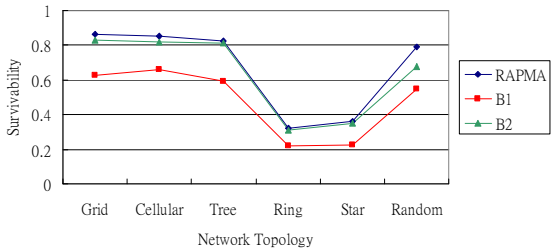

Figure 3. Survivability of Different Network Topologies at Different Scales to Verify Scalability (G: Grid, C: Cellular, R: Random; Small: 16 nodes, Medium: 64 nodes, Large: 196 nodes)

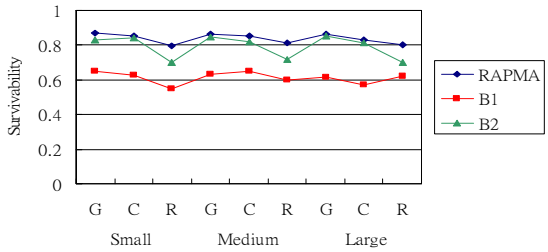

Figure 4. Survivability of Different Medium-size Network Topologies (49 nodes) to Verify Applicability

In Figures 3 and 4, "Survivability" is antithetic to the concept of vulnerability and is calculated by (1-vulnerability). From Figure 3, we observe that our heuristic can handle a large-scale problem and outperforms the compared heuristics in terms of survivability. B1 allocates the same budget to each node in a network; thus, no dynamic adjustment will be made in response to a change in the attack strategy. Meanwhile, B2 increases the survivability of grid and cellular networks, but the solution quality declines for random networks. This may be due to the structure of the random network topology. Grid and cellular networks are relatively robust by nature when targeted by malicious attacks; however, random networks are vulnerable to such attacks. The graph in Figure 4 shows that our heuristic can be applied to various topologies. It is noteworthy that B2 can increase survivability as a near optimal solution, and it is easier to implement in terms of complexity. Therefore, if time is the most important issue in developing a solution approach, B2 would be the more

appropriate budget allocation strategy.

5. Conclusion

We have proposed a new solution approach based on redundancy allocation to protect networks against man-made and natural threats. Although it is impossible to prevent attackers from penetrating networks, by implementing effective redundancy allocation strategies, network administrators can establish solid defense mechanisms to ensure continuity of service. We therefore formulate attack-defense scenarios as a two-level min-max mathematical model, in which an attacker tries to maximize a network's vulnerability to hazardous events. Meanwhile, a defender deploys redundant components to minimize the maximized total vulnerability in order to provide continuous services. In the model, we replace random attacks, which are governed by probability, with malicious targeted attacks launched under continuity constraints to reflect a current attack trend.

The results of computational experiments demonstrate that our proposed solution approaches outperform the compared algorithms. Moreover, the results for scalability and applicability show that our heuristics can handle large-scale problems, adapt to different attack/defense scenarios, and be applied to all kinds of network topologies.

The well-formulated mathematical model represents the major contribution of this work. We have researched the respective strategies of attackers and defenders, and identified their objectives and associated constraints. According to our survey, few works transform attackers' real behavior into mathematical programming problems in the context of survivability. Moreover, in the realm of RAP, few works consider the impact of targeted attacks and hazardous events simultaneously; however, those potential malicious risks indeed bring severe threats. In other words, our model is applicable to a variety of real-world scenarios.

We believe our model can be extended to different attack-defense scenarios in the context of survivability. In our future work, we will investigate the extent to which our methods can be applied to scenarios involving the interactive dependency of network nodes. We will also examine specific application parameters of other real-world network environments, such as wireless sensor networks

References

[1] H. F. Lipson and D. A. Fisher, "Survivability ─ A New Technical and Business Perspective on Security," *Proceedings of the 1999 Workshop on New Security Paradigms,* pp. 33-39, 1999.

[2] M. S. Chern, "On the Computational Complexity of Reliability Redundancy Allocation in A Series System," *Operations Research Letters*, Volume 11, Number 5, pp. 309-315, 1992.

[3] B. B. M. Shao, "Optimal Redundancy Allocation for Information Technology Disaster Recovery in the Network Economy," *IEEE Transactions on Dependable and Secure Computing*, Volume 2, Number 3, pp. 262-267, July-September 2006.

[4] D. W. Coit and A. Konak, "Multiple Weighted Objectives Heuristic for the Redundancy Allocation Problem," *IEEE Transactions on Reliability*, Volume 55, Issue 3, pp. 551-558, September 2006.

[5] C. Ha and W. Kuo, "Multi-Path Heuristic for Redundancy Allocation: The Tree Heuristic," *IEEE Transactions on Reliability*, Volume 55, Issue 1, pp. 37-43, March 2006.

[6] J. E. Ramirez-Marquez, D. W. Coit, and A. Konak, "Redundancy Allocation for Series-Parallel Systems Using a Max-Min Approach," *IIE Transactions*, Volume 36, Issue 9, pp. 891-898, September 2004.

[7] Z. Zeitlin, "Integer Allocation Problems of Min-Max Type with Quasiconvex Separable Functions," *Operations Research*, Volume 29, Number 1, pp. 207-211, January-February 1981.

[8] A. Stewart, "On Risk: Perception and Direction," *Computers and Security*, Volume 23, Issue 5, pp. 362-370, July 2004.

[9] P.-H. Tsang, F.Y.-S. Lin, and C.-W. Chen, "Maximization of Network Survival Time in the Event of Intelligence and Malicious Attacks," accepted by ICC2008.

[10] M. L. Fisher, "The Lagrangean Relaxation Method for Solving Integer Programming Problems," *Management Science*, Volume 27, Number 1, pp. 1-18, January 1981.