Near Optimal Protection Strategies Against Targeted Attacks on the Core Node of a Network

Frank Yeong-Sung Lin, Po-Hao Tsang[+], Yi-Luen Lin
Department of Information Management
National Taiwan University
Taipei, Taiwan, R.O.C.
{yslin, d91002, r93041}@im.ntu.edu.tw

Abstract

The issue of information security has attracted increasing attention in recent years. In network attack and defense scenarios, attackers and defenders constantly change their respective strategies. Given the importance of improving information security, a growing number of researchers are now focusing on how to combine the concepts of network survivability and protection against malicious attacks. As defense resources are limited, we propose effective resource allocation strategies that maximize an attacker's costs and minimize the probability that the "core node" of a network will be compromised, thereby improving its protection. The two problems are analyzed as a mixed, nonlinear, integer programming optimization problem. The solution approach is based on the Lagrangean Relaxation method, which solves this complicated problem effectively. We also evaluate the survivability of real networks, such as scale-free networks.

1. Introduction

It has been shown that the Internet's topology follows a power-law degree distribution [1] and is thus highly susceptible to malicious attacks [2]. As a result, the field of information security has attracted increasing attention in recent years, and a number of approaches have been proposed to protect networks against such attacks. 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.

Network survivability is another important research domain. Initially, researchers focused on the effect of random failures on networks and tested the robustness and dependability of networks. However, given the need to constantly improve information security, researchers are now paying more attention to protection against malicious attacks and to combining the concept with the field of network survivability.

Many definitions, techniques, and architectures for evaluating a network's survivability have been proposed. The most well-known definition is "the ability of a system to fulfill its mission in a timely manner, in the presence of attacks, failures, or accidents" [3]. Several of the definitions address the following key information security requirements: 1) the maintenance of service under attack; and 2) the provision of strategies to prevent attacks [4]. In this paper, we focus on the second requirement.

In addition to the above definitions of survivability, a number of models have been proposed to evaluate network survivability. For example, in [5], the authors describe several models that quantitatively evaluate survivability; and in [6], the state-based architecture proposed in [7] is adopted to quantitatively analyze survivability. The latter is implemented by a Markov chain. Meanwhile, because of the growing importance of information security, some researchers have started to focus on how to combine the concept of survivability with that of protection against malicious attacks. Thus in [8], the authors model attack-defense scenarios as mathematical programming problems in the context of survivability.

In this paper, we consider network survivability in terms of protection of the "core node" in which organizations store their most valuable knowledge. Because of the node's importance, attackers do their best to compromise it; thus, defenders must change their strategies to protect the node against compromise by the constantly evolving strategies of attackers. As defense resources are limited, network operators need guidelines about how to allocate security budgets

[+] Correspondence should be sent to d91002@im.ntu.edu.tw.

Second International Conference on Availability, Reliability and Security (ARES'07)
0-7695-2775-2/07 $20.00 © 2007 IEEE

effectively. To this end, we propose two mathematical models: the protection strategies for defenders (PSD) model and the probabilistic protection strategies for defenders (PPSD) model, to formulate attack-defense scenarios. Our objective is to provide defenders with effective defense resource allocation strategies to protect the core node, so that the cost of compromising the node would be unacceptable to an attacker.

The remainder of the paper is organized as follows. In Section 2, we propose the PSD model, and present a Lagrangean Relaxation-based solution approach for obtaining near optimal protection strategies. In Section 3, the second mathematical formulation, the PPSD model, is proposed. It is an extension of the PSD model and employs heuristics to calculate good primal feasible solutions. In Section 4, the results of computational experiments on the PSD and PPSD models are reported. Finally, in Section 5, we present our conclusions.

2. Problem formulation for the PSD model

2.1. Problem description and assumptions

To compromise a core node, an attacker must find a suitable path to it and compromise all the intermediate nodes on that path. However, compromising a node costs the attacker some resources, such as time, money, and man-power. From a defender's perspective, if more defense resources are allocated to a node, its security will be improved and the attacker's costs will be increased. However, since defense resources are limited, the defender must adopt an effective resource allocation strategy to maximize the attacker's costs.

In the worst-case scenario, if the attacker can obtain complete information about the target network and use it intelligently, he will find the path with the minimal attack cost to compromise the core node. Meanwhile, the defender will try to maximize the minimized attack cost through different budget allocation strategies. In response, the attacker will then search for another path with the minimal attack cost to compromise the core node.

Next, we define the notations used in this paper and formulate the problem.

Table 1. Given parameters

Notation	Description
B	The defender's total budget
N	The index set of all nodes in the network
W	The Origin-Destination pair (OD pair) (s, t), where s is the source node, and t is the core node
P_w	The index set of all candidate paths for the OD 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 $i \in N$, $p \in P_w$)

Table 2. Decision variables

Notation	Description
y_i	1 if node i is compromised, and 0 otherwise (where $i \in N$)
x_p	1 if path p is chosen as the attack path, and 0 otherwise (where $p \in P_w$)
b_i	The budget allocated to protect node i, where $i \in N$
$\hat{a}_i(b_i)$	The threshold of the attack power required to compromise node i, i.e., the defense capability of node i, where $i \in N$
$P_i(b_i)$	The probability of node i being compromised, where $i \in N$

Objective function:

$$\max_{b_i} \min_{x_p} \sum_{i \in N} \hat{a}_i(b_i) \sum_{p \in P_w} x_p \delta_{pi}, \qquad \text{(IP 1)}$$

subject to:

$$\sum_{i \in N} b_i \le B \qquad (1\text{-}1)$$

$$0 \le b_i \le B \qquad i \in N \qquad (1\text{-}2)$$

$$\sum_{p \in P_w} x_p = 1 \qquad (1\text{-}3)$$

$$x_p = 0 \text{ or } 1 \qquad p \in P_w. \qquad (1\text{-}4)$$

The objective function is to maximize the minimized total attack cost, where the defender manipulates the budget to maximize the total attack cost, while the attacker tries to minimize that cost by choosing a suitable attack path. To simplify the original problem, we reformulate it as follows:

Objective function:

$$\min_{b_i} -\sum_{i \in N} y_i \hat{a}_i(b_i), \qquad \text{(IP 2)}$$

subject to:

$$\sum_{i \in N} y_i \hat{a}_i(b_i) \le \sum_{i \in N} \delta_{pi} \hat{a}_i(b_i) \qquad p \in P_w \qquad (2\text{-}1)$$

$$\sum_{p \in P_w} x_p \delta_{pi} \le y_i \qquad i \in N \qquad (2\text{-}2)$$

$$\sum_{p \in P_w} x_p = 1 \qquad (2\text{-}3)$$

$$x_p = 0 \text{ or } 1 \qquad p \in P_w \qquad (2\text{-}4)$$

$$y_i = 0 \text{ or } 1 \qquad i \in N \qquad (2\text{-}5)$$

$$\sum_{i \in N} b_i \le B \qquad (2\text{-}6)$$

$$0 \le b_i \le B \qquad i \in N. \qquad (2\text{-}7)$$

We reformulate the objective function (IP 1) as one of minimizing the attacker's negative attack cost, i.e., (IP 2). Constraint (2-1) requires that the selected path for the OD pair should be the minimum attack cost path. Constraint (2-2) is the relation between y_i, x_p and δ_{pi}. We use the auxiliary set of decision variables, y_i, to replace the product of x_p and δ_{pi}, which further simplifies the problem-solving procedures. Other constraints are straightforward.

2.2. Solution for the PSD model

By applying the Lagrangean Relaxation method [9] with a vector of Lagrangean multipliers u^1 and u^2, we can transform the reformulation of the PSD model into the following Lagrangean Relaxation problem (LR 1). In this case, Constraints (2-1) and (2-2) are relaxed. Furthermore, we assume that $\hat{a}_i(b_i)$ is equal to the concave function $\ln(b_i+1)$, which indicates that the marginal defense capability of node i can be reduced by allocating additional budget.

$$Z_{D1}(u^1,u^2) = \min -\sum_{i\in N} y_i \ln(b_i+1) + \sum_{p\in p_w} u_p^1 \sum_{i\in N}(y_i-\delta_{pi})\ln(b_i+1) + \sum_{i\in N} u_i^2 (\sum_{p\in P_w} x_p\delta_{pi} - y_i) \qquad (\text{LR } 1),$$

subject to:

$$\sum_{p\in P_w} x_p = 1 \qquad (3\text{-}1)$$

$$x_p = 0 \text{ or } 1 \qquad p \in P_w \qquad (3\text{-}2)$$

$$y_i = 0 \text{ or } 1 \qquad i \in N \qquad (3\text{-}3)$$

$$\sum_{i\in N} b_i \le B \qquad (3\text{-}4)$$

$$0 \le b_i \le B \qquad i \in N. \qquad (3\text{-}5)$$

To solve (LR 1) optimally, we decompose it into the following two independent and easily solvable optimization subproblems.

Subproblem 1-1 (related to decision variable x_p)

$$\min \sum_{i\in N}\sum_{p\in P_w} u_i^2 x_p \delta_{pi}, \qquad (\text{SUB } 1\text{-}1)$$

subject to (3-1) and (3-2).

(SUB 1-1) can be viewed as a minimum cost path problem with node weight $u_i^2\delta_{pi}$. Because u_i^2 is non-negative, we can apply Dijkstra's shortest path algorithm to solve it optimally. The time complexity is $O(|N|^2)$.

Subproblem 1-2 (related to decision variables y_i, b_i)

$$\min \ (\sum_{p\in p_w} u_p^1 - 1)\sum_{i\in N} y_i \ln(b_i+1) - \sum_{p\in p_w}\sum_{i\in N} u_p^1 \delta_{pi} \ln(b_i+1) - \sum_{i\in N} u_i^2 y_i, \qquad (\text{SUB } 1\text{-}2)$$

subject to (3-3), (3-4), and (3-5).

To solve (SUB 1-2) optimally, we adopt some mathematical techniques to carefully choose proper values for the random variables b_i and y_i. The time complexity is $O(|N|^2)$.

Based on the weak Lagrangean duality theorem [9], the optimal value of problem (LR 1) is, by its nature, the lower bound (for minimization problems) of the objective function value in the primal problem. We try to obtain the tightest lower bound of (LR 1) by applying the subgradient optimization technique proposed in [10] to tune the Lagrangean multipliers.

Getting primal feasible solutions

Information provided by the multipliers is very helpful in deriving a heuristic that can solve the problem (IP 2). In this case, the multiplier vector u_i^2 is adjusted by the function $\sum_{i\in N}(y_i - \delta_{pi})\hat{a}_i(b_i)$, which indicates the relative importance of each node i. This gives us a hint about how to allocate the budget. Our proposed heuristic is described in Table 3.

Table 3. Algorithm for getting a primal feasible solution for the PSD model

Step 1	Construct a minimal defense region by applying the labeling and the removal processes. The labeling process is based on a breadth-first search, and the removal process tests whether each outer layer node is necessary.
Step 2	Allocate b_i to each node, where $b_i \sim r_i = \frac{u_i^2}{\text{total } u_i^2}$, $i \in N$. If a node has $r_i > 0$, and it is not in the minimal defense region, allocate its budget to the source and destination nodes.
Step 3	Tune the epsilon budget from the source and core nodes to the other nodes in the minimal defense region. If the value of the objective function is less than that of the previous state, we continue the tuning process recursively.

The time complexity of the heuristic is $O(|N|^2)$.

3. Problem formulation for the PPSD model

3.1 Problem description and assumptions

Based on the PSD model, we assume there is a probability that each node can be compromised, and that attacks on nodes are independent. Therefore, from an attacker's perspective, the probability that a core node can be compromised successfully is the aggregate of the compromise probability of all nodes on the attack path between the source node and the core node. A defender can reduce a node's compromise probability by allocating more defense resources to it. However, because such resources are limited, the defender needs to adopt a strategy that allocates the defense budget effectively in order to minimize the possibility of the core node being compromised.

In the worst-case scenario, if the attacker can obtain complete information about the target network and can use it intelligently, he will try to find the least secure path to compromise the core node, i.e., the path on which the aggregate of the compromise probability of all nodes is maximal. Meanwhile, the defender will try to improve the network's security by allocating a different budget to each node.

Objective function:

$$\min_{b_i} \sum_{i \in N} \ln P_i(b_i) y_i \,, \qquad \text{(IP 4)}$$

subject to:

$$\sum_{i \in N} -\ln P_i(b_i) y_i \le \sum_{i \in N} -\ln P_i(b_i) \delta_{pi} \qquad p \in P_w \qquad \text{(4-1)}$$

$$\sum_{p \in P_w} x_p \delta_{pi} \le y_i \qquad i \in N \qquad \text{(4-2)}$$

$$\sum_{p \in P_w} x_p = 1 \qquad \text{(4-3)}$$

$$x_p = 0 \; or \; 1 \qquad p \in P_w \qquad \text{(4-4)}$$

$$y_i = 0 \; or \; 1 \qquad i \in N \qquad \text{(4-5)}$$

$$\sum_{i \in N} b_i \le B \qquad \text{(4-6)}$$

$$0 \le b_i \le B \qquad i \in N. \qquad \text{(4-7)}$$

To simplify this problem, we transform the compromise probability $P_i(b_i)$ of each node i into a weight, $\ln P_i(b_i)$. Therefore, for the defender, the objective function (IP 4) is to minimize the weight of compromising the core node. Constraint (4-1) requires that the selected path for the OD pair should be the path with the minimal weight.

3.2. Solution to the PPSD model

By applying the Lagrangean relaxation method with a vector of Lagrangean multipliers u^1 and u^2, we can transform the PPSD model into the following Lagrangean relaxation problem (LR 2). In this case, Constraints (4-1) and (4-2) are relaxed.

$$Z_{D2}(u^1, u^2) = \min \sum_{i \in N} \ln \lambda e^{-\lambda b i} y_i + \sum_{p \in p_w} u_p^1 \sum_{i \in N} \ln \lambda e^{-\lambda b i} (\delta_{pi} - y_i) + \sum_{i \in N} u_i^2 (\sum_{p \in P_w} x_p \delta_{pi} - y_i) \,, \qquad \text{(LR 2)}$$

subject to:

$$\sum_{p \in P_w} x_p = 1 \qquad \text{(5-1)}$$

$$x_p = 0 \; or \; 1 \qquad p \in P_w \qquad \text{(5-2)}$$

$$y_i = 0 \; or \; 1 \qquad i \in N \qquad \text{(5-3)}$$

$$\sum_{i \in N} b_i \le B \qquad \text{(5-4)}$$

$$0 \le b_i \le B \qquad i \in N. \qquad \text{(5-5)}$$

Furthermore, we assume that $P_i(b_i)$ follows an exponential distribution with λ, which indicates that the compromise probability will be rapidly reduced by the additional budget allocated to a node. We can decompose the optimization problem (LR 2) into the following two independent subproblems and solve them optimally.

Subproblem 2-1 (related to decision variable x_p)

$$\min \sum_{i \in N} \sum_{p \in P_w} u_i^2 x_p \delta_{pi} \,, \qquad \text{(SUB 2-1)}$$

subject to (5-1) and (5-2).

Because u_i^2 is non-negative, we can apply Dijkstra's shortest path algorithm to solve (SUB 2-1) optimally. The time complexity is $O(|N|^2)$.

Subproblem 2-2 (related to decision variables y_i, b_i)

$$\min \; (1 - \sum_{p \in p_w} u_p^1) \sum_{i \in N} \ln \lambda e^{-\lambda b i} y_i + \sum_{p \in p_w} u_p^1 \sum_{i \in N} \ln \lambda e^{-\lambda b i} \delta - \sum_{i \in N} u_i^2 y_i \,, \qquad \text{(SUB 2-2)}$$

subject to (5-3), (5-4), and (5-5).

To solve (SUB 2-2) optimally, we use mathematical techniques to determine the proper values of the random variables b_i and y_i. The time complexity is $O(|N|)$.

Getting primal feasible solutions

Using the method for getting primal feasible solutions for the PSD model, we derive a heuristic for the PPSD model, as shown in Table 4.

Table 4. Algorithm for getting a primal feasible solution for PPSD model

Step 1.	Construct a minimal defense region by applying the labeling and the removal processes. The labeling process is based on a breadth-first search, and the removal process tests whether each outer layer node is necessary.
Step 2.	Allocate b_i to each node, where $b_i \sim r_i = \frac{u_i^2}{\text{total } u_i^2}$, $i \in N$. If a node has $r_i > 0$, and it is not in the minimal defense region, allocate its budget to the source or destination nodes, depending on which one has the larger λ value.
Step 3.	Tune the epsilon budget from the source and core nodes to the other nodes that have the highest negative value of the objective function in the minimal defense region. If the value of the objective function is less than that of the previous state, we continue the tuning process recursively.
Step 4.	Compare with the primal-based heuristic, which allocates the budget to each node according to the value of the primal variable b_i. Then, we determine the minimal objective value of the heuristics.

The time complexity of the heuristic is $O(|N|^3)$.

4. Computational experiments

4.1 Experiment environments

In the PSD model, we assume that $\hat{a}_i(b_i)$ is the same for each node in a homogenous network.

To evaluate the PPSD model, we consider two scenarios. In scenario 1, following the 20/80 rule, we assume that 20% of the nodes in the network are more important than the other 80%. Therefore, we assume that the $P_i(b_i)$ for 20% of the nodes follows an exponential distribution with a smaller $\lambda(\lambda_1)$ value; and for the other 80%, the $P_i(b_i)$ follows an exponential distribution with a larger $\lambda(\lambda_2)$ value. Note that λ represents the initial compromise probability of each node.

In scenario 2, we assume that the $P_i(b_i)$ for an OD pair follows an exponential distribution with a randomly selected λ value between [0, 0.5]. Because the source node and the core node are important, we assume that the OD pair has a certain level of protection initially. For the other nodes, we assume that $P_i(b_i)$ follows an exponential distribution with a randomly selected λ value between [0, 1].

We use two simple algorithms and one primal-based heuristic to compare the attack costs of different defense resource allocation strategies with those of our proposed algorithms. Simple algorithm 1 (SA1) allocates b_i uniformly. In simple algorithm 2 (SA2), however, the allocation of b_i is proportionate to the ratio $\frac{\text{Links of a node}}{\text{Total \# of Links}}$. In the primal-based heuristic (HE3), the budget allocation for each node is based on the value of the primal variable b_i, which is derived by solving (SUB 1-2).

We discuss the experiment results in the next two subsections and present them in tabulated form in the Appendix. The LR value represents the primal feasible solution derived by the LR process; and LB represents the lower bound gained from the LR process. The duality gap is calculated by $\frac{\text{LB-LR}}{\text{LR}} * 100\%$, and the survivability factor is calculated by $\frac{\text{LR}}{\text{LB}}$. Finally, we transform the objective value into a positive to simplify the explanation

4.2 Experiment results for the PSD model

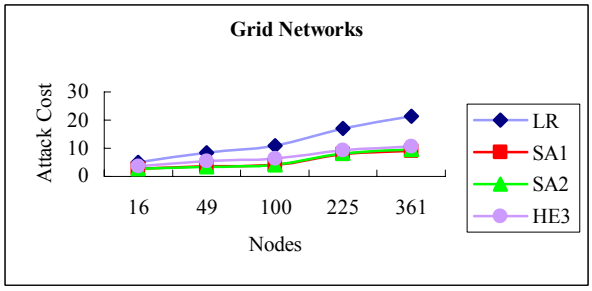

Figure 1. Attack costs in grid networks

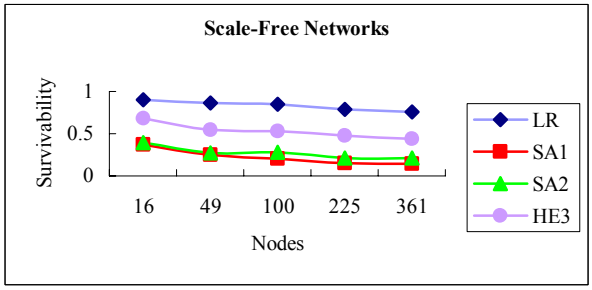

Figure 2. Survivability of scale-free networks

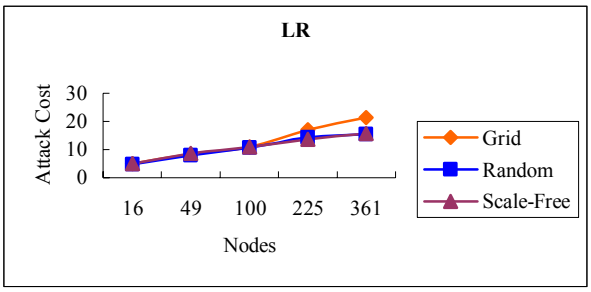

Figure 3. Effect of different network topologies

In Figure 1, the attack costs incurred by our proposed algorithm (Table 3) are always higher than those of the other algorithms used for comparison. The efficacy of the LR-based algorithm's solution is clearly demonstrated as the size of the network increases. Figure 2 shows that the survivability factor of the proposed algorithm is consistently higher than that of the other algorithms. Thus, by applying the algorithm, the core node will be more robust and secure. Meanwhile, Figure 3 demonstrates that a network's topological structure strongly influences its robustness against attack. The attack costs in large grid networks are higher than those in large random and scale-free networks [2]. The reason is that the average number of nodes that must be compromised in a grid network is higher than in a random or scale-free network. This is due to the small-world phenomenon [2]. Therefore, we can conclude that the defense-in-depth strategy [11] is an important factor in network survivability.

4.3 Experiment results for the PPSD model

The experiment results for scenario 1 of the PPSD model are similar to the results of the PSD model in Figures 1, 2, and 3. The proposed algorithm (Table 4) incurs higher attack costs than the two simple algorithms, and maintains a higher level of survivability in different-sized network topologies. We observe that, if the values of λ_1 and λ_2 are similar, the network is homogeneous.

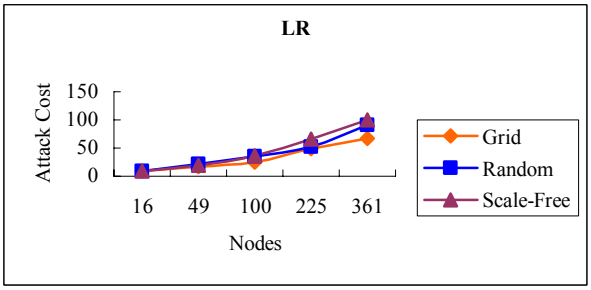

Figure 4. Attack costs of scenario 1 of the PPSD model: different network topologies (λ_1=0.2, λ_2=0.8)

However, if λ_1 is different to λ_2, we must consider the specific characteristics of each node, such as its importance on the path and its $P_i(b_i)$ function. For example, a node with a substantial number of links that provide short cuts from the source node to the core node is very important in a scale-free network. If this kind of node is vulnerable (especially if its λ value is high), more defense resources should be allocated to it in order to reduce the risk of it being compromised. Because the effect of a node's characteristics is greater than that of the defense-in-depth strategy, the attack costs in scale-free networks are higher than those in the other two network topologies, especially if the network is large, as shown in Figure 4.

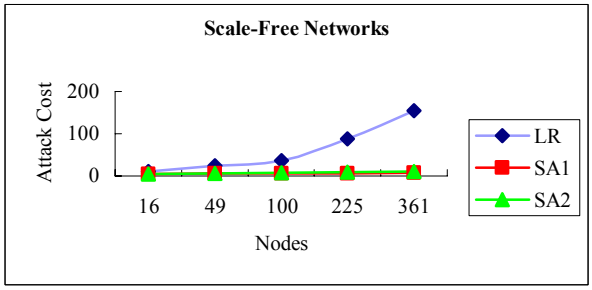

Figure 5. Attack costs in scenario 2: scale-free networks

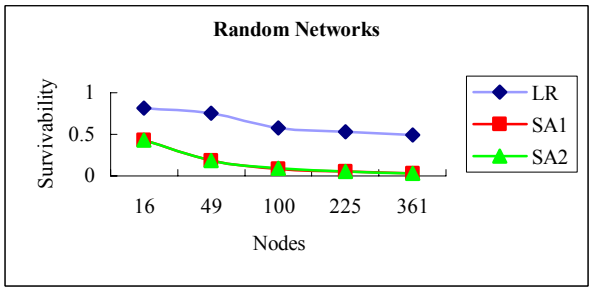

Figure 6. Survivability of random networks in scenario 2

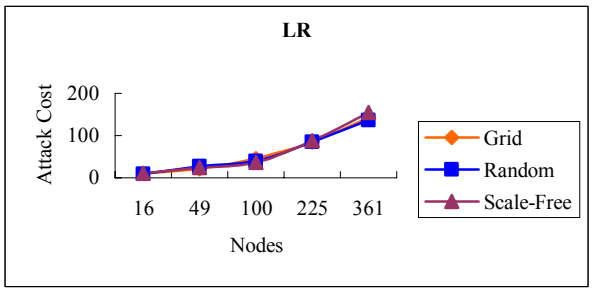

Figure 7. Attack costs of different network topologies in scenario 2

In scenario 2 of the PPSD model, the curves of the

LR-based algorithms are all above those of SA1 and SA2. Thus, the solution quality of LR is better than that of SA1 or SA2, as shown in Figures 5 and 6, respectively. Considering both the defense-in-depth concept and the nodes' characteristics, the attack costs incurred by the proposed algorithm are approximately equal in different-sized network topologies, as shown in Figure 7. This implies that the proposed protection strategy is very adaptive such that we can obtain almost the same result in networks of different size and topology.

5. Conclusion

We have focused on two issues. First, to improve the security of the core node in a network, we have proposed two mathematical models to formulate attack-defense scenarios and provide defenders with useful defense resource allocation strategies. Second, we have considered network survivability and evaluated the maximal minimized attack costs in different scenarios.

The mathematical models represent the major contribution of this work. We have carefully researched the security problem's characteristics, identified its objectives and associated constraints, and proposed well-formulated mathematical models to solve it. To the best of our knowledge, the proposed approach is one of the few that model attack-defense scenarios as mathematical programming problems in the context of survivability. In addition, we have provided solution approaches to determine the attack costs for both models.

Finally, our evaluation of different topologies revealed the following phenomenon. In a homogeneous network, the defense-in-depth strategy is the most important issue to be considered when allocating a defense budget. Because a grid network does not contain short cuts, the attacker must compromise more nodes than in random or scale-free networks. Therefore, a defender can employ nodes with more levels when allocating defense resources in a grid network, which means that an attacker must expend further resources to compromise the core node. However, if a network is heterogeneous, the defender must pay more attention to each node's characteristics. In random and scale-free networks, the nodes that provide short cuts are the most vulnerable. Therefore, we allocate more budget resources to them to improve the protection of the core node. The greater the differences between the nodes, the stronger will be the impact of each node's characteristics. The proposed solution approach is not only very effective, it is also adaptable to different attack/defense scenarios.

We believe that the proposed models can be extended to different attack-defense scenarios in the context of survivability, where the survivability metrics include "the percentage of critical OD pairs disconnected," "the number of core nodes that are survivable in a multiple core node environment," or "the percentage of valuable information not stolen." 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] M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On Power-Law Relationships of the Internet Topology", *ACM SIGCOIMM Computer Communications Review,* Volume 29, Number 4, pp. 251-263, September 1999.

[2] R. Albert, H. Jeong, and A.-L. Barabási, "Error and Attack Tolerance of Complex Networks", *Nature,* Volume 406, pp. 378-382, July 2000.

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

[4] V. R. Westmark, "A Definition for Information System Survivability", *Proceedings of the 37th IEEE Hawaii International Conference on System Sciences (HICSS'04)*, Volume 9, p. 90303.1, January 2004.

[5] D. M. Nicol, W.H. Sanders, and K.S. Trivedi, "Model-Based Evaluation: from Dependability to Security", *IEEE Transactions on Dependable and Secure Computing*, Volume 1, Issue 1, pp. 48-65, January 2004.

[6] D.-Y. Chen, S. Garg, and K.S. Trivedi, "Network Survivability Performance Evaluation: A Quantitative Approach with Applications in Wireless Ad-hoc Networks", *Proceedings of the 5th ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM'02),* pp. 61-68, September 2002.

[7] J. C. Knight and K. J. Sullivan, "On the Definition of Survivability", Technical Report CS-TR-33-00, Department of Computer Science, University of Virginia, December 2000.

[8] Y.-S. Lin, P.-H. Tsang, C.-H. Chen, C.-L. Tseng, and Y.-L. Lin, "Evaluation of Network Robustness for Given Defense Resource Allocation Strategies", *Proceedings of the 1st International Conference on Availability,*

Reliability and Security (ARES'06), pp. 182-189, April 2006.

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

[10] M. Held, P. Wolfe, and H. P. Crowder, "Validation of Subgradient Optimization", *Mathematical Programming*, Volume 6, pp. 62-88, 1974.

[11] "Information Assurance Technical Framework (IATF) Release 3.1:2002", National Security Agency.

Appendix

Experiment Results for the PSD Model

Topology	No. of Nodes	LB	LR	Gap (%)	Surv.	SA1	Imp. Ratio to SA1 (%)	SA2	Imp. Ratio to SA2 (%)	HE3	Imp. Ratio to HE3 (%)
Grid Networks	16	6.23	4.89	27.37	0.79	2.63	85.84	2.67	83.12	3.62	35.37
	49	12.18	8.40	45.05	0.69	3.60	132.92	3.46	142.54	5.43	54.65
	100	16.80	10.96	53.26	0.65	4.02	172.70	3.99	174.73	6.37	72.13
	225	36.08	17.14	110.51	0.48	7.90	116.92	8.22	108.55	9.38	82.77
	361	46.51	21.29	118.51	0.46	9.15	132.65	9.48	124.45	10.79	97.26
Random Networks	16	5.74	4.87	17.99	0.85	2.22	119.45	2.40	102.49	3.97	22.53
	49	9.36	7.84	19.34	0.84	2.36	232.78	2.52	211.70	5.53	41.90
	100	15.50	10.71	44.70	0.69	3.33	221.96	3.53	203.68	6.76	58.37
	225	21.30	14.22	49.82	0.67	3.47	310.31	3.84	270.24	8.40	69.21
	361	25.65	15.43	66.22	0.60	3.60	328.21	4.29	260.06	8.52	81.19
Scale-Free Networks	16	5.56	5.00	11.31	0.90	2.08	140.36	2.20	127.00	3.79	31.83
	49	9.90	8.56	15.65	0.86	2.50	242.94	2.66	221.13	5.42	57.82
	100	12.74	10.85	17.41	0.85	2.63	311.93	3.58	203.13	6.79	59.81
	225	17.32	13.65	26.86	0.79	2.63	418.34	3.74	265.27	8.30	64.57
	361	20.77	15.66	32.62	0.75	3.05	413.47	4.47	250.35	9.11	71.97

Experiment Results for the PPSD Model Scenario 1 (λ_1=0.2, λ_2=0.8)

Topology	No. of Nodes	LB	LR	Gap (%)	Surv.	SA1	Imp. Ratio to SA1 (%)	SA2	Imp. Ratio to SA2 (%)
Grid Networks	16	16.48	8.62	91.22	0.52	5.67	52.15	5.68	51.79
	49	44.04	17.47	152.14	0.40	7.21	142.32	7.21	142.37
	100	75.69	24.64	207.13	0.33	10.28	139.80	10.71	130.06
	225	189.37	48.32	291.91	0.26	14.78	226.96	14.62	230.41
	361	301.64	67.45	347.24	0.22	18.57	263.16	19.13	252.63
Random Networks	16	14.71	9.17	60.45	0.62	5.16	77.61	5.22	75.57
	49	37.48	21.77	72.18	0.58	5.16	321.72	5.64	285.84
	100	84.84	34.78	143.89	0.41	6.07	472.64	6.79	411.96
	225	159.92	52.45	204.88	0.33	6.69	684.25	7.63	587.20
	361	296.79	90.91	226.45	0.31	7.27	1150.55	8.16	1014.15
Scale-Free Networks	16	14.29	8.86	61.33	0.62	4.44	99.64	4.72	87.63
	49	43.15	18.90	128.28	0.44	5.62	236.46	7.22	161.82
	100	84.78	36.34	133.26	0.43	6.03	503.03	7.83	364.14
	225	187.12	65.97	183.64	0.35	7.00	842.05	9.93	564.53
	361	297.63	100.19	197.07	0.34	7.32	1269.19	9.54	950.73