Maximization of Network Survival Time in the Event of Intelligent and Malicious Attacks

Po-Hao Tsang[+], Frank Yeong-Sung Lin, Chun-Wei Chen
Department of Information Management
National Taiwan University
Taipei, Taiwan, R.O.C.
{d91002, yslin, r94021}@im.ntu.edu.tw

***Abstract*—It is not possible to ensure that a network is absolutely secure. Therefore, network operators must continually change their defense strategies to counter attackers who constantly seek new ways to compromise networks. However, as defense resources are limited, it is essential that network operators devise effective resource allocation strategies to maximize the survival time of critical/core nodes under attack. In this paper, the problem of effective resource allocation is analyzed as a mixed, nonlinear, integer programming optimization problem. To solve this complex problem, we propose an effective solution approach based on Lagrangean relaxation and the subgradient method. The efficiency and effectiveness of the proposed heuristic are evaluated by computational experiments.**

I. INTRODUCTION

Attackers who compromise computers or networks might actually crash a network or interrupt a system's normal services. In this situation, the time between the beginning of a service and the time that it is compromised is called the *survival time*. The survival time, shown in Fig. 1, can be calculated as the average time between reports for an average target IP address [1]. The figure illustrates the average survival time. In each month, the thick line indicates the range of the standard deviation, while the peak point and lowest point represent, the maximum and minimum survival times, respectively. The survival time reflects the compromise probability of a network i.e., the lower the compromise probability, the longer the network will survive.

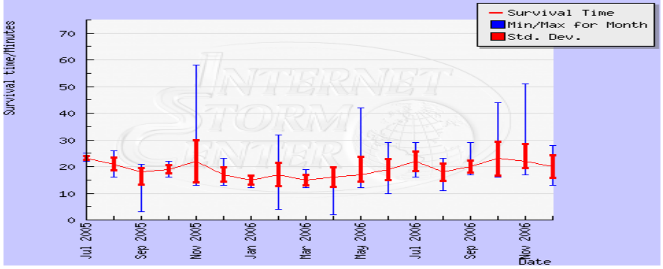

Fig. 1. Monthly Survival Time (2006/12/25 12:00PM)

F. Cohen described the main strategies of defenders and attackers [2]. In practice, both parties must adjust their respective strategies frequently. As defenders adjust their network security mechanisms, attackers try to find new network vulnerabilities to continue compromising the networks. In other words, defenders must change their strategies to protect the network against compromise by the constantly evolving strategies of attackers.

According to [3], the most important asset of an organization is its know-how or a mission critical system. Since it is the "core node" of a network, it is the target that attackers try to compromise. In this paper, we consider network survivability in terms of ensuring that the "core node" survives as long as possible given that defenders only have limited resources to ensure network survivability. To this end, we propose a mathematical model to formulate attack-defense scenarios. Our objective is to provide defenders with effective defense resource allocation strategies so that they can reduce the end-to-end compromise probability (i.e., increase the survival time of the core node) in different time slots. Previous research has shown that attempts to model attack-defense scenarios in an abstract, mathematical way are non-trivial. Moreover, the issues remain unsolved [3, 4].

The remainder of this paper is organized as follows. In Section 2, we formulate the budget allocation problem. Then, in Section 3, we propose a Lagrangean Relaxation-based solution approach to the problem. The results of computational experiments conducted to evaluate the proposed solution are reported in Section 4. Finally, in Section 5, we present our conclusions and indicate possible directions of future research.

II. PROBLEM FORMULATION

A. Problem Description and Assumptions

An attacker must find a suitable path from the source node *s* to the core node *t* and compromise all the intermediate nodes on that path to maximize the end-to-end compromise probability in a specific time slot (i.e., minimize the network survival time). Meanwhile, a defender must allocate limited resources, such as time, money, and man-power, effectively in order to minimize the maximized compromise probability (i.e., maximize the minimized network survival time).

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

We assume that the target network is at the Autonomous System (AS) level. There may be more than one attacker attempting to compromise the network, but we can model a group of attackers in different locations as an omnipresent attacker, and consider defenders similarly [5]. Although it is improbable that an attacker would know everything about a network in practice, the worst-case scenario must be considered. Therefore, we assume that an attacker can obtain complete information about the target network and use it intelligently.

Based on Fig. 1 and other information from the same source [1], we assume that both the survival time and the compromise probability follow normal distributions. From a defender's perspective, he could allocate extra budget to each node to increase the mean and the variance of the survival time, and thereby reduce the compromise probability. The end-to-end compromise probability distribution from the source node to the core node is calculated by convolution of the probability density functions of all the intermediate nodes on the path.

B. Problem Formulation

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

TABLE I
DECISION VARIABLES

Notation	Description
b_i	The budget allocated to protect a node i, where $i \in N$
μ	The mean of the normal distribution, which is the convolution of the probability density functions of all nodes on the attack path
σ^2	The variance of the normal distribution, which is the convolution of the probability density functions of all nodes on the attack path
m_p	The mean of the normal distribution, which is the convolution of the probability density functions of all nodes on the path p, where $p \in P_w$
$s_p{}^2$	The variance of the normal distribution, which is the convolution of the probability density functions of all nodes on the path p, where $p \in P_w$
$\mu_i(b_i)$	The mean of the normal distribution, which is the probability density function of a node i that is a function of the budget, where $i \in N$
$\sigma_i(b_i)^2$	The variance of the normal distribution, which is the probability density function of a node i that is a function of the budget, where $i \in N$
y_i	1 if the node i is chosen, and 0 otherwise (where $i \in N$)
y_t	1 if the core node t is chosen, and 0 otherwise
x_p	1 if the path p is selected as the attack path, and 0 otherwise (where $p \in P_w$)

TABLE II
GIVEN PARAMETERS

Notation	Description
N	The index set of all nodes in the network
w	The O-D pair (s , t)
P_w	The index set of all candidate paths for an O-D pair w
δ_{ip}	The indicator function, which is 1 if node i is on path p, and 0 otherwise (where $i \in N$, $p \in P_w$)
δ_{ip^*}	The indicator function, which is 1 if node i is on the shortest path p^* (where the cost associated with node i is $\mu_i(min\{B_i\})$), and 0 otherwise (where $i \in N$)
σ_{iq^*}	The indicator function, which is 1 if node i is on the shortest path q^* (where the cost associated with node i is $\mu_i(max\{B_i\})$), and 0 otherwise (where $i \in N$)
B	The total budget
B_i	All possible values of b_i allocated to node i, where $i \in N$
T	The time taken by the attacker
M	All possible values of μ on the attack path
Σ^2	All possible values of σ^2 on the attack path
M_p	All possible values of m_p on the path p, where $p \in P_w$
$S_p{}^2$	All possible values of $s_p{}^2$ on the path p, where $p \in P_w$
$P(t, \mu, \sigma^2)$	A polynomial approximation tail distribution of the normal distribution with mean μ and variance σ^2 at the time t [6]

Objective function:

$$Z_{IP1} = \min_{b_i} \max_{y_i} 1 - P(T, \mu, \sigma^2) \quad , \qquad \text{(IP 1)}$$

subject to:

$$\mu = \sum_{i \in N} \mu_i(b_i) y_i \qquad \text{(IP 1.1)}$$

$$\sigma^2 = \sum_{i \in N} \sigma_i(b_i)^2 y_i \qquad \text{(IP 1.2)}$$

$$\sum_{i \in N} \mu_i(\min\{B_i\}) \delta_{ip^*} \le \mu \le \sum_{i \in N} \mu_i(\max\{B_i\}) \sigma_{iq^*} \qquad \text{(IP 1.3)}$$

$$\sum_{i \in N} \sigma_i(\min\{B_i\})^2 \delta_{ip^*} \le \sigma^2 \le \sum_{i \in N} \sigma_i(\max\{B_i\})^2 \sigma_{iq^*} \qquad \text{(IP 1.4)}$$

$$\mu \in M \qquad \text{(IP 1.5)}$$

$$\sigma^2 \in \Sigma^2 \qquad \text{(IP 1.6)}$$

$$\sum_{p \in P_w} x_p \, \delta_{ip} = y_i \qquad \forall\, i \in N \qquad \text{(IP 1.7)}$$

$$\sum_{p \in P_w} x_p = 1 \qquad \text{(IP 1.8)}$$

$$x_p = 0 \; or \; 1 \qquad \forall\, p \in P_w \qquad \text{(IP 1.9)}$$

$$y_i = 0 \; or \; 1 \qquad \forall\, i \in N - \{t\} \qquad \text{(IP 1.10)}$$

$$y_t = 1 \qquad \text{(IP 1.11)}$$

$$\min\{B_i\} \le b_i \le \max\{B_i\} \qquad \forall\, i \in N \qquad \text{(IP 1.12)}$$

$$\sum_{i \in N} b_i \le B \qquad \text{(IP 1.13)}$$

$$b_i \in B_i \qquad \forall\, i \in N \cdot \qquad \text{(IP 1.14)}$$

The objective is to minimize the maximized end-to-end compromise probability *1-P (T, μ, σ²)*. In the inner problem, an attacker tries to maximize the compromise probability by selecting the most vulnerable nodes to attack. In the outer problem, the defender attempts to minimize the compromise probability by allocating a defense budget to each node. As function *P* is a tail distribution of the probability from time T to infinity and we want to cumulate the functions from time zero to T, we take one minus function *P* as the objective function. To simplify the original problem, we reformulate it as follows:

Objective function:

$$Z_{IP2} = \min_{b_i, y_i} - P(T, \mu, \sigma^2) \quad , \qquad \text{(IP 2)}$$

subject to:

$$\forall\, p \in P_w \qquad \text{(IP 2.1)}$$

$$\overset{\times}{\mu} = \sum_{i\in N} \mu_i(b_i)y_i \qquad \text{(IP 2.2)}$$

$$\sigma^2 = \sum_{i\in N} \sigma_i(b_i)^2 y_i \qquad \text{(IP 2.3)}$$

$$\sum_{i\in N} \mu_i(\min\{B_i\})\delta_{ip*} \le \mu \le \sum_{i\in N} \mu_i(\max\{B_i\})\sigma_{iq*} \qquad \text{(IP 2.4)}$$

$$\sum_{i\in N} \sigma_i(\min\{B_i\})^2\delta_{ip*} \le \sigma^2 \le \sum_{i\in N} \sigma_i(\max\{B_i\})^2\sigma_{iq*} \qquad \text{(IP 2.5)}$$

$$\mu \in M \qquad \text{(IP 2.6)}$$

$$\sigma^2 \in \Sigma^2 \qquad \text{(IP 2.7)}$$

$$m_p = \sum_{i\in N} \mu_i(b_i)\delta_{ip} \qquad \forall\, p \in P_w \qquad \text{(IP 2.8)}$$

$$s_p^2 = \sum_{i\in N} \sigma_i(b_i)^2\delta_{ip} \qquad \forall\, p \in P_w \qquad \text{(IP 2.9)}$$

$$\sum_{i\in N} \mu_i(\min\{B_i\})\delta_{ip} \le m_p \le \sum_{i\in N} \mu_i(\max\{B_i\})\delta_{ip} \qquad \forall\, p \in P_w \qquad \text{(IP 2.10)}$$

$$\sum_{i\in N} \sigma_i(\min\{B_i\})^2\delta_{ip} \le s_p^2 \le \sum_{i\in N} \sigma_i(\max\{B_i\})^2\delta_{ip} \qquad \forall\, p \in P_w \qquad \text{(IP 2.11)}$$

$$m_p \in M_p \qquad \forall\, p \in P_w \qquad \text{(IP 2.12)}$$

$$s_p^2 \in S_p^2 \qquad \forall\, p \in P_w \qquad \text{(IP 2.13)}$$

$$\sum_{p\in P_w} x_p\, \delta_{ip} \le y_i \qquad \forall\, i \in N \qquad \text{(IP 2.14)}$$

$$\sum_{p\in P_w} x_p = 1 \qquad \text{(IP 2.15)}$$

$$x_p = 0 \text{ or } 1 \qquad \forall\, p \in P_w \qquad \text{(IP 2.16)}$$

$$y_i = 0 \text{ or } 1 \qquad \forall\, i \in N - \{t\} \qquad \text{(IP 2.17)}$$

$$y_t = 1 \qquad \text{(IP 2.18)}$$

$$\min\{B_i\} \le b_i \le \max\{B_i\} \qquad \forall\, i \in N \qquad \text{(IP 2.19)}$$

$$\sum_{i\in N} b_i \le B \qquad \text{(IP 2.20)}$$

$$b_i \in B_i \qquad \forall\, i \in N\,. \qquad \text{(IP 2.21)}$$

Constraint (IP 2.1) represents the original inner problem, where the end-to-end compromise probability of the attack path should always be less than or equal to the compromise probability of every other path so that the objective function can be maximized.

III. SOLUTION APPROACH

A. *Lagrangean Relaxation*

By applying the Lagrangean relaxation method [7] with a vector of Lagrangean multipliers, we can transform the reformulated problem (IP 2) into the following Lagrangean relaxation problem (LR 1), where constraints (IP 2.1), (IP 2.2), (IP 2.3), (IP 2.8), (IP 2.9), (IP 2.14), and (IP 2.20) are relaxed.

$$\begin{aligned} Z_D(u^1,u^2,u^3,u^4,u^5,u^6,u^7) = \min_{b_i, y_i} & - P(T,\mu,\sigma^2) \\ & + \sum_{p\in P_w} u_p^1 \left(P(T,\mu,\sigma^2) - P(T,m_p,s_p^2) \right) + u^2\left(\mu - \sum_{i\in N} \mu_i(b_i)y_i \right) \\ & + u^3\left(\sigma^2 - \sum_{i\in N} \sigma_i(b_i)^2 y_i \right) + \sum_{p\in P_w} u_p^4 \left(m_p - \sum_{i\in N} \mu_i(b_i)\delta_{pi} \right) \\ & + \sum_{p\in P_w} u_p^5 \left(s_p^2 - \sum_{i\in N} \sigma_i(b_i)^2\delta_{pi} \right) + \sum_{i\in N} u_i^6 \left(\sum_{p\in P_w} x_p\delta_{pi} - y_i \right) \\ & + u^7\left(\sum_{i\in N} b_i - B \right) \quad , \end{aligned} \qquad \text{(LR 1)}$$

subject to:

$$\sum_{i\in N} \mu_i(\min\{B_i\})\delta_{ip*} \le \mu \le \sum_{i\in N} \mu_i(\max\{B_i\})\sigma_{iq*} \qquad \text{(LR 1.1)}$$

$$\sum_{i\in N} \sigma_i(\min\{B_i\})^2\delta_{ip*} \le \sigma^2 \le \sum_{i\in N} \sigma_i(\max\{B_i\})^2\sigma_{iq*} \qquad \text{(LR 1.2)}$$

$$\mu \in M \qquad \text{(LR 1.3)}$$

$$\sigma^2 \in \Sigma^2 \qquad \text{(LR 1.4)}$$

$$\sum_{i\in N} \mu_i(\min\{B_i\})\delta_{ip} \le m_p \le \sum_{i\in N} \mu_i(\max\{B_i\})\delta_{ip} \qquad \forall\, p \in P_w \qquad \text{(LR 1.5)}$$

$$\sum_{i\in N} \sigma_i(\min\{B_i\})^2\delta_{ip} \le s_p^2 \le \sum_{i\in N} \sigma_i(\max\{B_i\})^2\delta_{ip} \qquad \forall\, p \in P_w \qquad \text{(LR 1.6)}$$

$$m_p \in M_p \qquad \forall\, p \in P_w \qquad \text{(LR 1.7)}$$

$$s_p^2 \in S_p^2 \qquad \forall\, p \in P_w \qquad \text{(LR 1.8)}$$

$$\sum_{p\in P_w} x_p = 1 \qquad \text{(LR 1.9)}$$

$$x_p = 0 \text{ or } 1 \qquad \forall\, p \in P_w \qquad \text{(LR 1.10)}$$

$$y_i = 0 \text{ or } 1 \qquad \forall\, i \in N - \{t\} \qquad \text{(LR 1.11)}$$

$$y_t = 1 \qquad \text{(LR 1.12)}$$

$$\min\{B_i\} \le b_i \le \max\{B_i\} \qquad \forall\, i \in N \qquad \text{(LR 1.13)}$$

$$b_i \in B_i \qquad \forall\, i \in N\,. \qquad \text{(LR 1.14)}$$

By definition, u^1, u^2, u^3, u^4, u^5, u^6, and u^7 are the vectors of $\{u_p^1\}$, $\{u^2\}$, $\{u^3\}$, $\{u_p^4\}$, $\{u_p^5\}$, $\{u_i^6\}$, and $\{u^7\}$ respectively, where u^1, u^6, and u^7 are non-negative and u^2, u^3, u^4, and u^5 are unrestricted. To solve (LR 1) optimally, we decompose it into four independent and easily solvable subproblems as follows.

Subproblem 1 (related to decision variable x_p)

$$z_{sub1}(u^6) = \min_{x_p} \sum_{i\in N} \sum_{p\in P_w} u_i^6 x_p \delta_{pi} \quad , \qquad \text{(SUB 1)}$$

subject to (LR 1.9) and (LR 1.10).

(SUB 1) can be considered a minimum cost path problem with node costs $u_i^6\delta_{pi}$. Because of the non-negative costs, we can apply Dijkstra's shortest path algorithm to optimally solve this subproblem. The time complexity is $O(|N|^2)$.

Subproblem 2 (related to decision variable y_i , b_i)

$$z_{sub2}(u^2,u^3,u^4,u^5,u^6,u^7)=\min_{b_i,y_i}-\left(\sum_{i\in N}u^2\mu_i(b_i)y_i\right.$$
$$+\sum_{i\in N}u^3\sigma_i(b_i)^2y_i+\sum_{p\in P_w}\sum_{i\in N}u_p^4\mu_i(b_i)\delta_{pi}+\sum_{p\in P_w}\sum_{i\in N}u_p^5\sigma_i(b_i)^2\delta_{pi}$$
$$\left.+\sum_{i\in N}u_i^6y_i-\sum_{i\in N}u^7b_i+u^7B\right)\quad, \qquad \text{(SUB 2)}$$

subject to (LR 1.11) – (LR 1.14).

We assume that $\mu_i(b_i)$ and $\sigma_i\ (b_i)^2$ are equal to the concave functions $\mu_0+\lambda_A ln(\lambda_B\ b_i\ +1)$ and $\sigma_0{}^2+\lambda_C ln(\lambda_D\ b_i\ +1)$ respectively. This suggests that the marginal effect of the defense capability of node i could be reduced by allocating additional budget. If the constant value u^7B is ignored, (SUB 2) can be decomposed into a series of |N| subproblems that can be solved optimally by an exhaustive search. The time complexity is $O(|N|\times|B_i|)$.

Subproblem 3 (related to decision variable μ, σ^2)

$$z_{sub3}(u^1,u^2,u^3)=\min_{\mu,\sigma^2}\left(\sum_{p\in P_w}u_p^1-1\right)P(T,\mu,\sigma^2)+u^2\mu+u^3\sigma^2\quad, \qquad \text{(SUB 3)}$$

subject to (LR 1.1) – (LR 1.4).

The mean and variance, μ and σ^2, are discrete. Therefore, (SUB 3) can be solved optimally by an exhaustive search. The time complexity is $O(|\mathrm{M}|\times|\sum^2|)$.

Subproblem 4 (related to decision variable m_p , s_p^2)

$$z_{sub4}(u^1,u^4,u^5)=\min_{m_p,s_p^2}-\sum_{p\in P_w}u_p^1P(T,m_p,s_p^2)+\sum_{p\in P_w}u_p^4m_p+\sum_{p\in P_w}u_p^5s_p^2\quad, \qquad \text{(SUB 4)}$$

subject to (LR 1.5) – (LR 1.8).

We are concerned with paths on which one of the multipliers $u_p{}^1$, $u_p{}^4$, or $u_p{}^5$ is at least non-zero. Such paths can be considered as possible active paths and added to a list. After marking all possible active paths, the next step in solving (SUB 4) is to check the list and obtain the value of the smallest objective function. The time complexity is $O(|P_w|\times|M_p|\times|S_p{}^2|)$.

According to the weak Lagrangean duality theorem [7], 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 methods for solving this problem, the subgradient optimization technique [7] is the most popular.

B. *Getting Primal Feasible Solutions*

According to the solutions to (LR 1) and the multipliers, we can obtain some hints about deriving a heuristic to improve the solution quality of (IP 2). We observe that the multiplier $u_i{}^6$ represents the importance of each node; therefore, the more important a node i is, the bigger the multiplier $u_i{}^6$ it will have. Our proposed heuristic is described below.

TABLE III
HEURISTIC FOR THE MODEL

Step	Description
1	Allocate the budget b_i derived from (SUB 2) to each node, where $i \in N$.
2	Check if the budget allocated to the network fulfills the constraints.
3	Choose the path x_p derived from (SUB 1) as the attack path.
4	Move budget $\left(\max(u_i^6)-u_i^6\Big/\sum_{i\in N}u_i^6\right)\times B$ from a node not on the attack path to a node on the attack path, where $i\in N$ and node i was allocated budget $b_i > 0$ in step 1

IV. COMPUTATIONAL EXPERIMENTS

A. *Experiment Environments*

We choose two popular network topologies for our experiments. One is a grid network [8]; the other is a random network [8]. Clearly, a network with many nodes that are not allocated any budget has a lower defense capability than a network with fewer nodes that are allocated some budget. Hence, we assume that $\mu_i(b_i)$ = 1.3 ln (1.3 b_i + 1) + 0.11 and $\sigma_i(b_i)^2$ = 1.3 ln (1.3 b_i + 1) + 0.01.

We compare the compromise probability of two simple algorithms with that of our proposed heuristic. Simple algorithm 1 (SA$_1$) is a popularity-based budget allocation strategy that dispenses the budget according to the accumulated compromised frequency of each node on the candidate path. Simple algorithm 2 (SA$_2$) is a greed-based budget allocation strategy that first allocates a budget to the node with the smallest compromise probability between the source node and the core node.

The LR value represents the compromise probability of the primal feasible solution derived by our proposed heuristic, while the LB indicates the lower bound determined by the LR process. The duality gap is calculated by $\frac{LB-LR}{LR}\times 100\%$.

B. *Experiment Results*

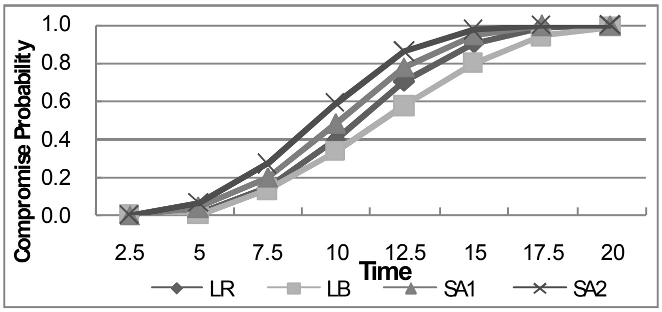

Fig. 2. Compromise Probability of a Grid Network with a 25-Unit Budget (|N|=9)

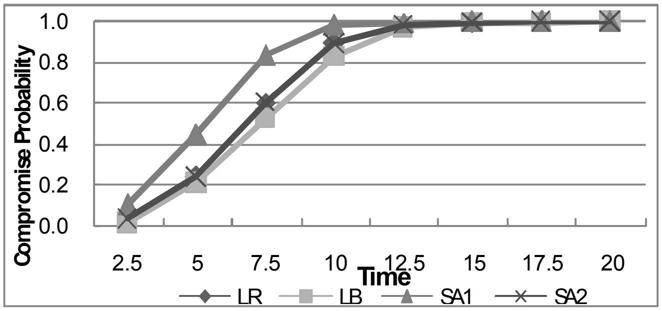

Fig. 3. Compromise Probability of a Random Network with a 10-Unit Budget (|*N*|=9)

From Figures 2 and 3, we observe that the compromise probability of the nodes between the source node and the core node increases continually over time; hence, the core node will be compromised eventually. We also observe that the proposed heuristic outperforms SA_1 and SA_2, and yields a smaller duality gap for the value of the optimal objective function.

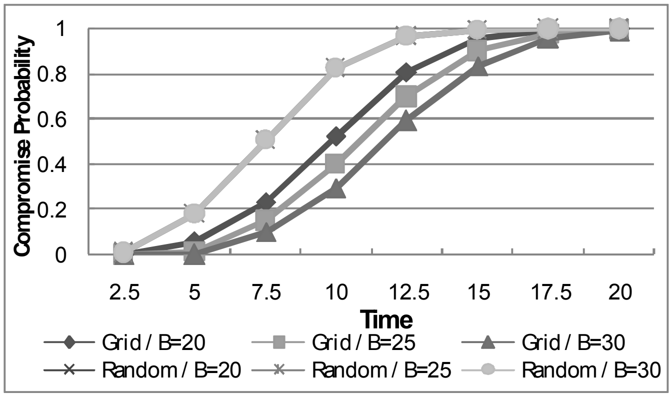

Fig. 4. Comparison of Different Budgets and Topologies (|*N*|=9)

The graph in Fig. 4 shows that the more budget we allocate to a grid network, the lower will be the compromise probability of nodes. Unlike grid networks, the compromise probability of random networks cannot be reduced by allocating more budgets. The reason is that, in random networks, there exists a shortest path from the source node to the core node. Even if nodes on this critical path are allocated the maximum budget, an attacker will still choose it as an attack path because the compromise probability of random networks cannot be reduced by simply allocating extra budget. Furthermore, comparing grid networks with random networks under different total budget scenarios, we observe that the compromise probability of grid networks is lower than that of random networks. This is because grid networks have larger diameters than random networks, so attackers need to go through more hub sites to compromise grid networks.

V. CONCLUSION

In this paper, we use attack-defense scenarios to describe one kind of targeted attack. An attacker tries to maximize the end-to-end compromise probability of a path between the source node and the core node, while a defender tries to minimize that probability. Although it is impossible to prevent attackers from penetrating networks, by implementing proper defense resource allocation strategies, defenders can establish solid defense mechanisms to reduce the compromise probability in the event of intelligent and malicious attacks. In other words, the survival time of the core node can be increased.

From our experiments, we conclude that, although increasing the total budget is a good way to defend grid networks, the compromise probability can also be reduced by adopting a defense-in-depth strategy (i.e., increase the depth of a network) when allocating the defense budget. We also note that providing extra budget does not increase the survival time of some networks (e.g., random networks); moreover, the survival time of such networks is less than that of grid networks.

The key contribution of this work is that we successfully model the security problem, including concepts like the core node, compromise probability, and survival time, as a well-formulated mathematical problem, which is then solved by the proposed heuristic. This is a major step in the analysis of network attacks, since previous research seldom modeled real-world attack behavior in this way. We believe that the proposed model can be extended to different attack-defense scenarios in the context of survivability. In our future work, we will consider the situation where attackers can devise new attack methods based on previous attack experience so that they can compromise other nodes more easily. Specifically, it is assumed that, for each node compromised, the attacker would obtain a discount coupon, which could be used to increase the compromise probability of nodes subsequently targeted for attack.

REFERENCES

[1] SANS-ISC (SysAdmin, Audit, Network, Security Institute - Internet Storm Center), *http://isc.sans.org/survivalhistory.php*.

[2] Fred Cohen, “Managing Network Security - Attack and Defense Strategies,” *Network Security*, Vol. 1999, No. 7, pp. 7-11, July. 1999.

[3] F.Y.-S. Lin, P.-H. Tsang, and Y.-L. Lin, "Near Optimal Protection Strategies against Targeted Attacks on the Core Node of a Network,", *Proceedings of the 2nd International Conference on Availability, Reliability and Security (ARES’07),* pp. 213-22, April 2007.

[4] C.-L. Tseng, F.Y.-S. Lin, and P.H. Tsang, "Near Optimal Attack Strategies for the Maximization of Information Theft," *Proceedings of the 11th World Multiconference on Systemics, Cybernetics and Informatics (WMSCI’07),* July 2007.

[5] Kong-wei Lye and Jeannette M. Wing, “Game strategies in network security,” *International Journal of Information Security* , Vol. 4, No. 1-2, pp. 71-86, February. 2005.

[6] Milton Abramowitz. and Irene A. Stegun, “Normal or Gaussian Probability Function,” *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, p.931, 1964.

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

[8] A.-L. Barabasi and R. Albert, “Emergence of Scaling in Random Networks,” *Science*, Volume 286, pp. 509-512, October 1999.