An Evaluation of Network Survivability When Defense Levels Are Discounted by the Accumulated Experience of Attackers

Frank Yeong-Sung Lin
National Tatiwan University, Taiwan
yslin@im.ntu.edu.tw

Pei-Yu Chen[+]
National Tatiwan University, Taiwan
d96006@im.ntu.edu.tw

Po-Hao Tsang
National Tatiwan University, Taiwan
d91002@im.ntu.edu.tw

Abstract

In this paper, we consider the allocation of resources for attack-defense problems when an attacker accumulates the experience gained by attacking nodes in a network. Mathematical programming and graph modeling are used to solve the problems optimally. To analyze the problems, we propose two models: the Accumulated Experience of an Attacker (AEA) model and the Advanced Accumulated Experience of an Attacker (AAEA) model. Both models are based on a concept called discount coupon, which is a specific application of the Traveling Salesman Problem (TSP). Under our approach, each node in the target network has a number of discount coupons that represent the experience an attacker could gain if he compromised that node. By accumulating the discount coupons (experience) obtained from compromised nodes, the attacker can minimize the total cost of a new attack. The proposed models can be used to design networks that are robust against intelligent and malicious attacks.

Keywords: *Internet Security, Network Attack and Defense, Survivability, Resource Allocation, Traveling Salesman Problem (TSP), Discount Coupon, Graph Modeling, Node Splitting, Generalized Shortest Path Problem, Optimization*

Introduction

The terrorist attacks on New York and Washington in September 2001 had an enormous influence on Internet security research. Since then, many researchers have focused on how to ensure the effective and efficient protection of infrastructures like the Internet. Although the Internet has many obvious benefits, it has also become an effective tool that can be used to compromise the security of nations and the business activities of organizations.

[+] Correspondence should be sent to d96006@im.ntu.edu.tw

In the past, the security of systems or infrastructures was analyzed in terms of two states: safe or compromised (*Ellison, R. J., 1997*). Nowadays, however, network security professionals are primarily concerned with ensuring the availability and continuity of services. Therefore, the binary concept is no longer sufficient to describe a system's state under malicious attack or random error conditions. Hence, in recent years, the concept of security has been increasingly generalized as an issue of survivability (*Knight, J. C., 2003 and Nicol, D. M., 2004*). Ellison et al. (*Ellison, R. J., 1997*) defined survivability as "the capability of a system to fulfill its mission, in a timely manner, in the presence of attack, failures, or accidents."

According to (*Lin, F.Y.-S., 2007*), the most important asset of an organization is its know-how or a mission critical system that keeps the business operating efficiently and profitably. 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 how to ensure that the "core node" survives given that attackers only have limited resources to target a network. Therefore, for an attacker, decisions about how to allocate attack resources effectively and how to devise an optimal attack strategy are key issues.

In (*Chen,C.H., 2006*), the authors propose two optimization-based mathematical models for evaluating the survivability of a network under two survivability metrics, and calculate the minimal attack cost incurred by an attacker. The metrics are 1) the connectivity of at least one given critical Origin-Destination pair (O-D pair), and 2) the connectivity of all given critical O-D pairs. Although the models of an attacker's behavior are well-formulated, the approach does not consider the experience that the attacker could accumulate after conducting a series of successful attacks. The concept of accumulated attack experience is proposed in (*Jonsson, E., 1997*). This approach divides an attacker's behavior into three phases: a learning phase, a standard attack phase, and an innovative attack phase.

There are two ways an attacker can obtain experience or information that could be used to reduce the effort involved in future attacks. The first way actually involves two kinds of experience: 1) Initial experience, which is based on valuable information the attacker gains before he launches an attack. For example, the attacker might learn about a newly discovered vulnerability in a program before the software developer can make a patch available. This is also known as a Zero-Day Attack (*Liu, Y., 2004*). 2) The attacker gains some useful attack experience after compromising a node. For instance, the attacker could learn about the trust relationship that exists between several computers, which simplifies the work of an administrator when managing several Microsoft network domains *(2007)*. Under this scenario, if the attacker could compromise one network domain, it would be easier for him to compromise other network domains.

The second way an attacker can gain experience is that, after compromising a node and gaining some experience, he might allocate extra resources to further probe the node, which has different levels of valuable information. The more resources he allocates, the greater the benefit he will derive. Since the attacker has only limited resources to probe the compromised node, he must decide which levels of information he wants to obtain.

The concept of the Traveling Salesman Problem (TSPs) has been applied in the areas of planning and scheduling for a long time. Some researchers have found that a specific application of the TSP can be used to describe how a salesman can reduce his total traveling costs by buying a discount coupon in each city (*Choi, J., 2004*). The

salesman may decide to visit certain cities early in his trip because he will be able to purchase discount coupons, which he can then use to reduce his total traveling costs. In each city, the salesman can only buy one discount coupon and use it to reduce the costs of traveling to the next city on his itinerary. The concept provides us with a special insight into reducing the total resources required in network attack and defense scenarios. Specifically, we liken discount coupons to the experience an attacker can gain by compromising nodes in a network. The concept of discount coupon can be viewed as the experience gained from compromising a node. By extension, an attacker can discount his total costs by accumulating the experience gained from compromising a series of nodes.

To the best of our knowledge, very little research has been devoted to modeling attack and defense problems by considering an attacker's accumulated experience in the context of network survivability. In this paper, we model an attacker's behavior via mathematical programming. The attacker's objective is to minimize the total attack cost and compromise the core node such that the network cannot survive. We propose two models, both of which adopt the concept of a discount coupon to represent the experience an attacker has accumulated from previously compromised nodes. The experience is then used to reduce the costs of future attacks. The models are called the Accumulated Experience of an Attacker (AEA) model and the Advanced Accumulated Experience of an Attacker (AAEA) model. The former considers the experience obtained by compromising a node without allocating extra resources to probe it further; while the latter considers the scenario where an attacker allocates extra resources to obtain information for use in further probing which is similar to purchasing a discount coupon in the TSP. We use the Generalized-Reverse-Dijkstra algorithm (*Ahuja, R.K., 1993*) to solve the two models.

The remainder of this paper is organized as follows. In Sections 2 and 3, we describe the AEA and AAEA problem scenarios, respectively, and use graph modeling to simplify and solve the two models. Then, in Section 4, we present our conclusions and indicate possible directions for future research.

Accumulated Experience of an Attacker (AEA) Model

Problem Description and Assumptions

Under the AEA model, an attacker gains some experience from a compromised node, which he then uses to reduce the cost of attacks on new nodes. The objective is to minimize the total attack cost such that the core node is compromised and the network cannot survive. From the defender's perspective, the attack cost could be viewed as an evaluation of the network's robustness against intentional or malicious attacks.

Under this model, it is assumed that the attacker has complete information about the targeted network's topology and defense strategy. Although it is not possible for an attacker to know everything about a network, we assume the worst case scenario from the defender's perspective; hence, we overestimate the attack power for the purposes of this study.

An attacker launches an attack on the network by first selecting an entry node. For example, in Figure 1, node *i* is the entry node. The attacker then compromises a series of nodes along the attack path from the entry node to the core node. The minimum total attack cost is the optimal solution for the attacker. To solve this traditional attack scenario,

we apply node splitting transformation to the problem, which can be viewed as a shortest path problem that can be optimally solved by Dijkstra's algorithm. We extend the scenario in Figure 1 with the concept of discount coupons, which are used to reduce the total attack costs. We use a similar transformation process, which is described below.

As shown in Figure 2, each node is split into two dummy nodes, *i'* and *i''*, which correspond to the input and output of node *i*, respectively. An artificial link is then introduced between node *i'* and node *i''*. We assume that the set L_2 represents all artificial links, which replace the attributes of the original nodes (e.g., the attack costs and discount factors). An original link connects the output dummy node of one original node to the input dummy node of another original node. All the original links form the set L_1. We also introduce a dummy entry node and a dummy destination node. The dummy entry node connects with the input dummy nodes of all the original nodes via artificial links, which form the set L_3. In this model, the dummy entry node and the dummy destination node represent the entry node and the core node respectively. The discount factors of all artificial links in L_1 and L_3 should be 1 because they have no effect on the attacker's accumulated experience.

Using the above technique, the AEA model can be transformed into a generalized shortest path problem completely.

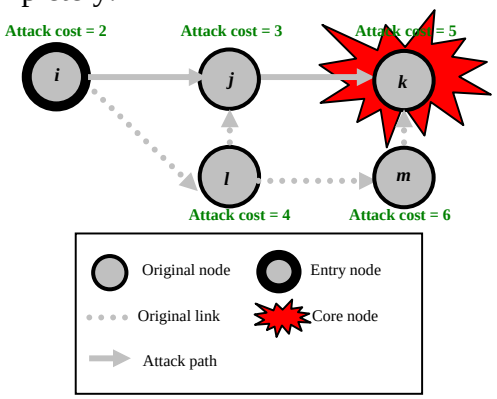

Figure 1 An Attack Scenario

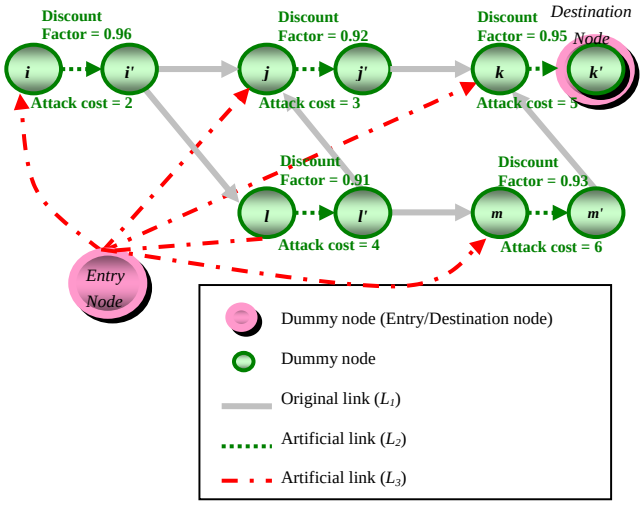

Figure 2 An Attack Scenario with Node Splitting

Solution Approach
Generalized Shortest Path Problem

The shortest path problem has been used to solve several important network issues. The link weight in this kind of problem is static and set to one. However, in the generalized version of the shortest path problem, the link weight is non-static (*Ahuja, R.K., 1993*). We use the weight to represent a discount factor, as mentioned in Subsection 2.2. The accumulation of discount factors on a path might be additive or multiplicative (*Batagelj, V., 2000*). In this paper, we assume the accumulation of discount factors is multiplicative when considering the worst case scenario.

The generalized shortest path problem is a special case of the shortest path problem; hence, it can be solved in polynomial time using the Generalized-Reverse-Dijkstra algorithm (*Batagelj, V., 2000*). More precisely, in this problem, each link has a weight that might discount the future link costs in a multiplicative fashion.

AEA Model: Solution Approach

In Section 2.2, we transformed the AEA model into a shortest path problem via the node splitting technique, without considering the progressive discount effects. Next, Lemma 1 states that that the AEA model can be optimally solved by the Generalized-Reverse-Dijkstra algorithm.

Lemma 1 *Given a budget allocation strategy, a topology, G= (V, L), and critical O-D pairs, W, the formulation of the AEA model can be optimally solved by the Generalized-Reverse-Dijkstra algorithm* (*Batagelj, V., 2000*) *with the node splitting method. The time complexity is* $O(|V^2|)$.

Proof. By adopting the node splitting method, a node can be divided into two independent sub-nodes connected by an artificial link. The attributes of an artificial link inherit the attributes of the original node, i.e., the attack cost and the discount factor. The discount factors and attack costs of the other links' are 1 and 0, respectively. We then transform *G(V, L)* into *G'(V', L')*. Using the Generalized-Reverse-Dijkstra algorithm, we can then find the shortest path with the minimal cost in *G'*.

Advanced Accumulated Experience of an Attacker (AAEA) Model
Problem Description and Assumptions

In the AAEA model, the attacker's behavior is more realistic than in the AEA model. From a practical point of view, the attacker can gain some free experience by compromising a node. He can also allocate extra resources, which is similar to paying a fee, to probe the compromised node and gain further valuable information or experience from the node. The cost, in terms of resources, depends on the degree of probing; thus, the more an attacker probes, the greater the amount of resources he must allocate to the task. From the attacker's perspective, the objective is to minimize the total attack cost such that the core node can be compromised and the network will not survive.

Graph Modeling

Unlike the AEA model, in the AAEA model, the attacker has to make decisions about which level to probe in order to obtain more experience and thereby discount the total attack costs. Because of this characteristic, node splitting is also used to transform the problem as follows.

Dummy level nodes are introduced to represent the different levels, i.e. level 1, level 2, level 3…etc., between dummy nodes *i'* and *i''*, as shown in Fig. 3. We assume that the set L_4 represents the artificial links that connect the conjunction node *c'* to all dummy level nodes and replace all the attributes of the *j*-th level, (d_{ij}, m_{ij}); m_{ij} is the extra cost, i.e., the cost of probing, and d_{ij} is the discount factor. We also assume that all the artificial links from the dummy nodes *i'* to conjunction node *c'* belong to the set L_2. The set L_3 represents all artificial links from the dummy level nodes to the conjunction node *c''* and from the conjunction node *c''* to the dummy node *i''*. The attack cost and discount factor of sets L_2 are set to nodes *i*'s attack cost and 1 while those of sets L_3 are 0 and 1, respectively. By this transformation, the AAEA model becomes a generalized shortest path problem.

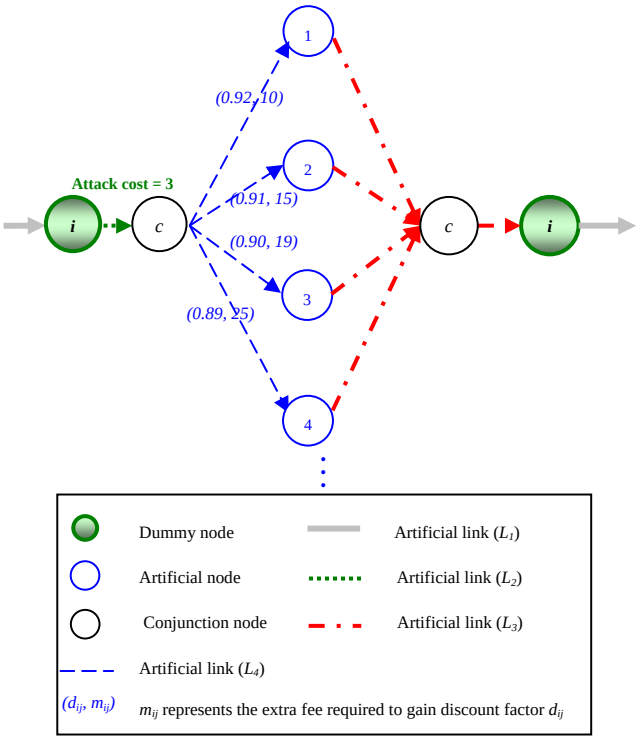

Figure 3 An Attack Scenario with Node Splitting in Different Levels

Solution Approach

In Section 3.2, we transformed the AAEA model into the AEA model by the node splitting technique, so that it becomes a generalized shortest path problem. Next, Lemma 2 states that the AAEA model can be solved by the Generalized-Reverse-Dijkstra algorithm

Lemma 2 *Given a budget allocation strategy, a topology, G= (V, L), and all levels of each node i is L_4, the formulation of the AAEA model can be transformed into the AEA*

model and optimally solved by the Generalized-Reverse-Dijkstra algorithm (*Batagelj, V., 2000*) *with the node splitting technique. The time complexity is* $O(|V^2 \cup L_4|)$.

Proof. A node *i* is converted into two sub-nodes *i' and i''*. Using the node splitting technique, all levels of a node can be converted into artificial nodes, which are then connected to node *c'* and node *c''*. The links from node *c'* to the artificial nodes inherit the attributes of the levels (i.e., the discount factor and attack cost). Moreover, the discount factor and attack cost of the link from node *i'* to node *c'* are set to 1 and node *i*'s attack cost, respectively. The discount factor of every other link is 1 and the attack cost is 0. Hence, the AAEA model is transformed into the AEA model, and can be optimally solved by the Generalized-Reverse-Dijkstra algorithm.

Conclusion and Future Work

In the attack-defense scenario described in this paper, intelligent and malicious attacks occur constantly, and the attacker tries to compromise the target network by all available means. By modeling the attacker's behavior we can evaluate the robustness of a network. We consider the above scenario in terms of the following two issues.

First, we consider the robustness of a network and evaluate the minimal attack cost of an attacker based on two models, namely, the Accumulated Experience of Attacker (AEA) model and the Advanced Accumulated Experience of Attackers (AAEA) Model. Under these models, an attacker chooses a node to start the attack on the target network and finds a minimal cost attack path. These problems could also be modeled as mixed integer programming problems, but we adopt some straightforward heuristics to solve them.

Second, by using graph modeling and the node splitting technique, the AEA and AAEA models are successfully transformed into generalized shortest path problems, which can be optimally solved by the Generalized-Reverse-Dijkstra algorithm in pseudo-polynomial time.

The main contribution of our research is that it provides a special insight into an attacker's experience and how it could help him launch further attacks more easily. This concept is more practical than previous approaches and is useful in evaluating the robustness of a network. Another contribution is that we transform both models into well-known geometric problems by using two elegant mathematical techniques, namely, graph modeling and node splitting.

Our proposed modeling techniques can be extended to different attack and defense scenarios (e.g., disconnecting one or all critical OD-pairs and compromising multiple core nodes) by considering an attacker's experience. The main issue to be addressed in our future work concerns the behavior of a defender when an attacker uses his accumulated experience to compromise a network. More precisely, since an attacker does his best to compromise a core node, the defender must change his strategy accordingly to protect the node from being compromised by the constantly evolving strategy of the attacker.

References

(2007). Report spells out global attack patterns: More zero-days and phishing, but less critical flaws, Computer Fraud & Security,4, 3-4.

Ahuja, R.K., MAgnagti, T.L., and Orlin, J.B. (1993). Network Flows, Prentice Hall, Englewood Cliffs, ISBN 978-0136175490,.

Batagelj, V., Brandenburg, F.J., Mendez, P.O.D., and Sen A. (2000). The Generalized Shortest Path Problem, The Pennsylvania State University CiteSeer Archives.

Chen,C.H., Lin, Y.L., Lin, F.Y.S., Tsang, P.H., Tseng C.L., and Yen H.H. (2006). Evaluation of Network Robustness for Given Defense Resource Allocation Strategies, Proceedings of the 1st International Conference on Availability, Reliability and Security.

Choi, J., Realff, M.J., and Lee, J.H. (2004). An Algorithmic Framework for Improving Heuristic Solutions Part I: A Deterministic Discount Coupon Traveling Salesman Problem, Computers & Chemical Engineering, 28, 8,1285-1296.

Ellison, R.J., Fisher, D.A., Linger, R.C., Lipson, H.F., Longstaff, T. A. and Mead N. R. (1997). Survivable Network Systems: An Emerging Discipline, Technical Report CMU/SEI-97-TR-013, Software Engineering Institute, Carnegie Mellon University.

Jonsson, E. and Olovsson, T. (1997). A Quantitative Model of the Security Intrusion Process Based on Attacker Behavior, IEEE Transactions of Software Engineering, 23, 4, 235-245.

Knight, J.C., Strunk, E.A., and Sullivan, K.J. (2003). Towards a Rigorous Definition of Information System Survivability, Proceedings of the DARPA Information Survivability Conference and Exposition, 1,78-89.

Lin, F.Y.-S., Tsang, P.-H., and Lin, Y.-L. (*2007*). 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.

Liu, Y., Mendiratta, V.B., and Trivedi, K.S. (2004). Survivability Analysis of Telephone Access Network, Proceedings of the 15th IEEE International Symposium for Software Reliability Engineering, 367-378.

Nicol, D.M., W.H., Sanders, Trivedi, K.S. (2004). Model-Based Evaluation: From Dependability to Security, IEEE Transactions on Dependable and Secure Computing.