

doi: 10. 11830/ISSN. 1000-5013. 201604025



# 层次化分类淘汰法的网络 最优弥补模型

李远敏

(厦门理工学院 计算机与信息工程学院, 福建 厦门 361024)

**摘要:** 针对求解最优弥补的特点和需求,利用层次化分类淘汰,提出一种基于层次化分类淘汰法的最优弥补模型(HSE-ONHM),得到最优弥补的精确解.为了验证 HSE-ONHM 的可行性和有效性,分别采取穷举法和层次化淘汰算法求解同一目标网络环境的最优弥补.实验结果表明:无论是淘汰次数还是 CPU 消耗时间,层次化分类淘汰法比穷举法优越;层次化分类淘汰法的计算时间随着初始属性节点数量呈指数增加,该实验结果与算法性能分析结果一致.

**关键词:** 最优弥补模型;层次化淘汰算法;穷举法;网络安全

**中图分类号:** TP 393      **文献标志码:** A      **文章编号:** 1000-5013(2016)04-0515-04

## Optimal Network Hardening Model Based on Hierarchical Classification Elimination

LI Yuanmin

(College of Computer and Information Engineering, Xiamen University of Technology, Xiamen 361024, China)

**Abstract:** This paper considers the characteristics and requirement of solving the optimal hardening problem. A new optimal network hardening model based on hierarchical separatal elimination (HSE-ONHM) is proposed and accurate solution for optimal hardening is got. In order to verify the feasibility and effectiveness of the model, the optimal exhaustive method and hierarchical algorithm is taken for elimination of the same target for network environment. Experimental results show that either eliminated or the number of CPU time consuming, HSE-ONHM is superior. The computation time of HSE-ONHM with initial attribute node increases exponentially with the number. The experimental results are consistent with the performance analysis of the algorithm.

**Keywords:** optimal hardening model; hierarchical classification elimination algorithm; enumeration method; network security

网络脆弱性评估的目的之一是为网络管理者及用户提供最优弥补,提高目标网络系统的安全性<sup>[1-6]</sup>.由于采取不同的安全弥补措施需要花费不同的成本代价,最优弥补即在有限资源的前提下,以最小的成本代价保证目标网络系统正常、安全运行. Phillips 等<sup>[7]</sup>首次提出了最优弥补建议的分析方法,但该方法由于分析过于简单,其准确性有待进一步考察. Sheyner 等<sup>[8-9]</sup>提出了一种攻击图自动生成方法,并基于攻击图对最优弥补建议进行了理论分析. Homer 等<sup>[10]</sup>认为安全弥补措施提高目标网络系统的安全性的同时,会受到多种条件的约束,基于此,利用逻辑攻击图提出了一种自动化网络配置管理方法. 该

**收稿日期:** 2016-01-20

**通信作者:** 李远敏(1970-),男,副教授,主要从事信息融合、嵌入式系统的研究. E-mail: cxllymin@163. com.

**基金项目:** 福建省教育厅 A 类项目(JA09217); 厦门理工学院高层次人才科技项目(YKJ08013R)

方法通过多次迭代分析,最终会给出权衡了各种约束的网络配置方案.本文提出了一种基于层次化分类淘汰法的网络最优弥补模型(HSE-ONHM),能得到最优弥补的精确解.

# 1 网络最优弥补模型

求解最优弥补时,若只弥补一个初始属性节点能保证目标网络系统正常、安全运行,且需耗费的成本代价为  $a$ ,则其他所有的除弥补该初始属性节点外,仍弥补其他初始属性节点的弥补策略,需耗费的成本代价必须大于  $a$ .根据代价最小原则,应将这些策略淘汰.

基于此,为了得到目标网络系统最优弥补的精确解,对精确搜索方法进行了改进,提出一种基于层次化分类淘汰法的最优弥补模型(HSE-ONHM).该模型首先根据攻击图中的初始属性节点进行分类;然后,对弥补策略进行层次化淘汰,依据代价最小原则,淘汰成本代价相对比较大的弥补策略,直至分类中的所有弥补策略都被淘汰,与此同时,得到最优弥补.

在具体的实现过程中,该方法主要分为两个步骤.

**步骤 1** 将弥补策略进行分类.

**步骤 2** 将淘汰成本代价大的弥补策略.

若弥补初始属性节点  $c_1$  能保证目标网络系统正常、安全运行,即  $g(\{10\cdots 0\})=0$ ,根据代价最小原则,则除弥补  $c_1$  外,仍弥补其他初始属性节点的弥补策略都应被淘汰.设 1-弥补  $\{c_N=1\}$ ,使  $g(x)=0$ ,其中,  $N$  为初始属性节点的编号.具体的淘汰规则为

淘汰 2-弥补中的弥补策略:  $2^i+2^j, 0\leq i\leq n-1, i\neq N, j=N$ ;

淘汰 3-弥补中的弥补策略:  $2^i+2^j+2^k, 0\leq i\leq j\leq n-1, i, j\neq N, k=N$ ;

淘汰  $n$ -弥补中的弥补策略:  $2^i+2^j+\cdots+2^m, 0\leq i<j<\cdots<s\leq n-1, i, j, \cdots, s\neq N, m=N$ .

具体有以下 4 个淘汰步骤.

**步骤 1** 依次判断 1-弥补  $\{c_i=1\}$  中的弥补策略.

**步骤 2** 若  $g(x)\neq 0$ ,将该策略从 1-弥补中淘汰.

**步骤 3** 若  $g(x)=0$ ,令  $N=i$ ,并将弥补代价与  $\cos t$  比较.若弥补代价  $\geq \cos t$ ,按照淘汰规则逐层淘汰弥补策略;若弥补代价  $\cos t$ ,则  $\cos t=\text{弥补代价}$ ,然后,按照淘汰规则逐层淘汰弥补策略.

**步骤 4** 依次类推,直至所有的弥补策略都被淘汰.即 1-弥补, 2-弥补,  $\cdots$ ,  $n$ -弥补都为空,与此同时,得到最优弥补.

# 2 算法复杂度分析

目标网络系统中主机数量为  $H$ ,初始属性节点数量为  $C$ .在具体的实现过程中,首先,分析 1-弥补中的弥补策略;然后,分析 2-弥补中的弥补策略;依次类推,1-弥补算法的复杂度比其他弥补算法的复杂度要高.因此,该算法的时间复杂度即 1-弥补算法的时间复杂度.

在 1-弥补算法中,主要有两个子函数:弥补策略淘汰子函数和弥补策略判断子函数.其中,前者的目标是依据淘汰规则逐层淘汰  $xn$  的弥补策略,后者的目标是判断该弥补策略是否已被淘汰.

弥补策略判断子函数的时间复杂度为  $O(C)$ ,在弥补策略淘汰子函数中,首先,将十进制弥补策略转换为二进制形式,时间复杂度为  $O(C)$ ;然后,遍历  $[xa,xb)$  中的所有弥补策略,依次判断该策略是否被淘汰,时间复杂度为  $O(|xb-xa|)\cdot O(C)$ .  $[xa,xb)$  为弥补策略中包含未被淘汰弥补策略的最小敬意,  $|xb-xa|\leq 2^C$ .因此,弥补策略淘汰子函数的时间复杂度为

$$O(C)+O(2^C)\cdot O(C)=O(2^C)\cdot O(C).$$

在 1-弥补算法中,依次判断 1-弥补中的弥补策略,时间复杂度为  $O(C)$ .若该弥补策略的  $g(x)=0$ ,调用弥补策略淘汰子函数,按照淘汰规则逐层淘汰弥补策略,时间复杂度为  $O(2^C)\cdot O(C)$ ;然后,计算该弥补策略的弥补代价,时间复杂度为  $O(C)$ ;将弥补代价与  $\cos t$  比较,若弥补代价小于  $\cos t$ ,则  $\cos t$  等于弥补代价,按照淘汰规则逐层淘汰弥补策略,时间复杂度为  $O(2^C)\cdot O(C)$ .因此,1-弥补算法的时间复杂度为

$$O(C) + O(2^C) \cdot O(C) + O(C) + O(C) + O(2^C) \cdot O(C) + O(2^C) \cdot O(C) = O(C^2 \cdot 2^C).$$

### 3 实验结果与分析

为了验证 HSE-ONHM 的可行性和有效性,分别采取穷举法(算法 1)和层次化淘汰算法<sup>[12]</sup>(算法 2)求解同一目标网络环境的最优弥补.实验环境如下:服务器为 PowerEDGE R710;操作系统为 Re-tHAT V5.4;内存为 32 GB;CPU 为 2.26 GHz.无论是淘汰次数还是 CPU 消耗时间,层次化淘汰算法比穷举法要优越很多;层次化淘汰算法的计算时间会随着初始属性节点数量呈指数增加,该实验结果与算法性能分析结果一致.

**步骤 1** 求约束条件  $g(x)$ .假设攻击者的攻击目标是属性节点  $c_{15}$ , $g(x)$  为

$$g(x) = c_{15} = e_{13} = c_{13} = e_{11} = c_{11} = e_{10} = c_{10} \wedge c_7 \wedge c_{12} = e_4 \wedge e_5 \wedge 0 = 0.$$

由于  $g(x)=0$ ,因此,属性节点  $c_{15}$  不能被满足,即  $e_{11},c_{11},e_{10},c_{12}$  构成的循环路径在实际的应用中是不存在的,而且该循环路径涉及的节点  $c_{15},e_{13},c_{13},e_{11},c_{11},e_{10},c_{12}$  应被删除.

简单的攻击图,如图 1 所示.简化的攻击图,如图 2 所示.

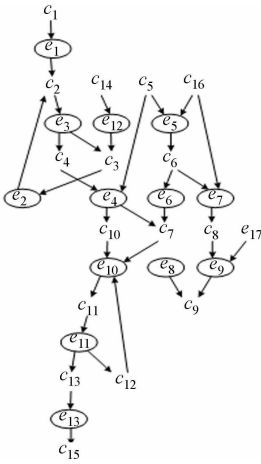


图 1 简单攻击图示例

Fig. 1 Simple attack graph example

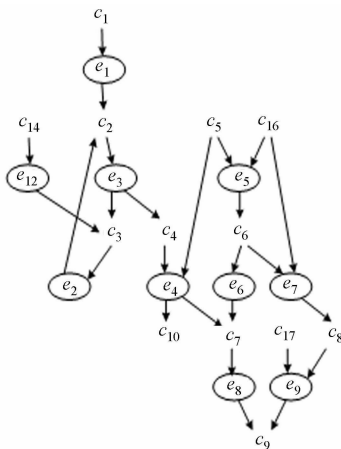


图 2 简化攻击图

Fig. 2 Simplified attack graph

**步骤 2** 利用 HSE-ONHM 求最优弥补.在步骤 1 获得  $g(x)$  的基础上,求攻击目标  $c_9$  的最优弥补,令弥补初始属性节点的成本代价为  $\{\cos t(c_1),\cos t(c_5),\cos t(c_{14}),\cos t(c_{16}),\cos t(c_{17})\} = \{2,4,3,5,6\}$ .求解过程,如表 1 所示.表 1 中:淘汰策略列中  $\{c_{17}=1\}$  表示逐层淘汰  $\{c_{17}=1\}$  的弥补策略.

在 HSE-ONHM 中,虽然对初始属性节点采取了二进制编码,将弥补策略转化成了二进制序列,但在具体的实现过程中,为了提高算法的性能和效率,将二进制序列转化成了十进制数.由表 1 可知:最优

表 1 HSE-ONHM 的求解过程

Tab. 1 Solving process of the HSE-ONHM

弥补策略	$g(x)$	淘汰策略	被淘汰的弥补策略	弥补代价	$\cos t$	被淘汰的弥补策略
00001	0	$\{c_{17}=1\}$	3,5,7,9,11,13,15,17	—	—	1,2,4,6,8,10,12,14,16
			—	6	6	—
			19,21,23,25,27,29,31	—	—	18,20,22,24,26,28,30
00010	0	$\{c_{16}=1\}$	6,10,14,18,22,26,30	5	6	1,2,4,8,12,16,20,24,28
		弥补代价比较	1	—	5	2,4,8,12,16,20,24,28
		$\{c_{14}=1\}$	12,20,28	3	5	2,4,8,16,24
00100	0	弥补代价比较	2	—	3	4,8,16,24
		$\{c_5=1\}$	24	4	3	4,8,16
		弥补代价比较	8	—	3	4,16
01000	0	—	—	2	3	4,16
		$\{c_1=1\}$	—	—	—	—
10000	0	弥补代价比较	4	—	2	16

弥补为 $\{c_1, c_5, c_{14}, c_{16}, c_{17}\} = \{1, 0, 0, 0, 0\}$ , 即只弥补初始属性  $c_1$ , 并且弥补成本代价为 2.

## 4 结 束 语

网络脆弱性评估方法的最终目标之一, 针对实际的目标网络系统, 得到该网络的最优弥补, 从而指导网络安全管理者有针对性地进行保护. 运用基于层次化分类淘汰法的最有弥补模型求解最优弥补, 对弥补策略进行层次化淘汰, 依据代价最小原则, 淘汰成本代价相对比较大的弥补策略, 直至分类中的所有弥补策略都被淘汰, 从而得到最优弥补.

### 参考文献:

- [1] YEH W C. A Revised layered-network algorithm to search for all d-minpaths of a limited-flow acyclic network[J]. IEEE Transactions on Reliability, 1998, 47(4): 436-442.
- [2] IN Yongkun. A Simple algorithm for reliability evaluation of a stochastic-flow network with node failure[J]. Computers and Operations Research, 2001, 28(13): 1277-1285.
- [3] 骆剑锋, 陈俞强. 采用环加星型网络结构负载均衡集群技术的云平台设计[J]. 华侨大学学报(自然科学版), 2016, 37(2): 164-167.
- [4] CHEN Run, MO Yong, PAN Zhan. Performance improvement of edge expansion technique for BDD-based network reliability analysis[J]. Journal of Computers 2013, 8(9): 2190-2196.
- [5] JHA S, SHEYNER O, WING J M. Two formal analyses of attack graphs[C]// Proceedings of 15th IEEE Computer Security Foundations Workshop. Ottawa: IEEE Press, 2002: 234-238.
- [6] NOEL S, JAJODIA S, OBERRY B, et al. Efficient minimum-cost network hardening via exploit dependency graphs [C]// Proceedings of 19th Annual Computer Security Applications Conference. Hangzhou: IEEE Press, 2003: 86-95.
- [7] PHILLIPS C, SWILER L. A graph-based system for network vulnerability analysis[C]// Proc of the New Security Paradigms Workshop. Charlottesville: User Evaluation, 1998: 71-79.
- [8] SHEYNER O, HAINES J, JHA S, et al. Automated generation and analysis of attack graphs[C]// Proc of the IEEE Symposm on Security and Privacy. Oakland: IEEE Computer Society Press, 2002: 254-265.
- [9] SHEYNER O. Scenario graphs and attack graphs[D]. Pittsburgh: Carnegie Mellon University, 2004: 256-257.
- [10] HOMER J. A comprehensive approach to enterprise network security management[D]. Manhattan: Kansas State University, 2008: 148-150.
- [11] WANG Lingyu, NOEL S, JAJODIA S. Minimum-cost network hardening using attack graphs[J]. Computer Communications, 2006, 29(18): 3812-3824.
- [12] CHEN Feng, WANG Lingyu, SU Junshang. An efficient approach to minimum-cost network hardening using attack graphs[C]// Proc of the Fourth International Conference on Information Assurance and Security. Tokyo: User Evaluation, 2008: 209-212.

(责任编辑: 陈志贤      英文审校: 吴逢铁)