基于转换的攻击图分析方法研究

闫 峰[1,2],刘淑芬[1],冷 煌[1]
(1.吉林大学计算机科学与技术学院,吉林长春 130012; 2.吉林省福利彩票发行管理中心,吉林长春 130061)

摘 要: 攻击图是一种分析计算机网络脆弱性的有效工具,它以图的方式描述了攻击者利用系统漏洞和单元间脆弱性信息综合入侵目标网络的行为过程.针对攻击图的最优弥补集问题,文章论证了最优弥补集问题与加权碰集问题之间的等价性,并提供了相应的形式化转换方法.在不增大问题规模的前提下,本文将最优弥补集问题形式化地转换为单一的加权碰集问题以进行求解.理论和实验均表明,在收敛于全局最优解方面,基于转换的分析方法较传统方法有更好的性能.

关键词: 攻击图; 最优弥补集; 转换; 全局最优解
中图分类号: TP393.08 **文献标识码:** A **文章编号:** 0372-2112 (2014)12-2477-04
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.12.20

Study on Analysis of Attack Graphs Based on Conversion

YAN Feng[1,2], LIU Shu-fen[1], LENG Huang[1]
(1. *College of Computer Science and Technology, Jilin University, Changchun, Jilin* 130012, *China*;
2. *Technology Department, Jilin Province Welfare Lottery Issue Center, Changchun, Jilin* 130061, *China*)

Abstract: Attack graph analysis is an effective tool for analyzing network vulnerability, representing the process that attackers penetrate networks using the complex interdependence between vulnerabilities and network configurations. In this paper, we prove the equivalence of the optimization security measure problem and the weighted hitting set problem, and present the method which converts the optimization security measure problem to the weighted hitting set problem on the premise of not increasing the problem scale. Theoretical analysis and experiments show that the method based on conversion has better performance than the method based on critical attack sets in converging to the global optimal solution.

Key words: attack graph; optimization security measure; conversion; global optimal solution

1 引言

随着现代网络技术的发展,网络系统涉及的节点规模,软件平台和软件包的数量,都在与日俱增.由于网络节点间的脆弱性之间、脆弱性和网络配置之间均存在着复杂的互相依赖关系,攻击者可以据此入侵有严密防护的网络.作为分析网络脆弱性的有效手段,攻击图利用对各主机节点扫描得到的弱点信息[1],能够对攻击者可能采用的攻击路线进行列举,从而将系统面临的安全威胁有效地展现给分析人员.

文献[2]等提出来攻击图的概念,基于包括目标网络和攻击者的全局状态进行建模,通常被称为状态攻击图.状态攻击图以图的方式显示地展示了攻击者利用系统漏洞和单元间脆弱性综合入侵目标网络的整个行为过程.随着目标网络的扩大,为了解决状态攻击图的"状态爆炸"问题,文献[3]基于攻击者的"单调性"假设进行模型分析,提出属性依赖攻击图.该假设认为攻击者在攻击的过程中不断获得新的权限的同时不会放弃以获得的权限.在对攻击图分析方面,文献[4]在状态攻击图中首次提出并研究了攻击图中的最优弥补集问题,即寻找最小代价的弥补措施集以保障目标网络中的关键资源.文献[5,6]则在属性依赖攻击图中论述了攻击图的最优弥补集问题的解决方案.文献[7]在属性依赖攻击图中提出了布尔代数的方法,将问题转换为布尔表达式,通过计算析取范式的方式求解问题.但是在最坏情况下,仍不可避免具有指数时间复杂度.文献[8]就属性依赖攻击图中存在的含圈攻击路径问题,提出了 n 有效攻击路径的假设.

本文着重研究了攻击图的最优弥补集问题,在不增大问题规模的前提下,将最优弥补集问题形式化地转换为单一的加权碰集问题进行求解.

收稿日期:2013-08-01;修回日期:2013-12-25;责任编辑:梅志强
基金项目:国家 863 高技术研究发展计划重点项目(No.2009AA010314863);国家自然科学基金(No.60973041)

2 攻击图及最优弥补集问题

虽然因构建模型的不同,产生的攻击图形式各异.但是对于攻击图分析中的最优弥补集问题,基本都采用文献[2]提出的计算关键攻击集的思想.因此,本文采用状态攻击图作为原型进行论述,形式化描述如下:

定义 1 以 P 为一组原子命题的集合,状态攻击图 G 是一个五元组关系 $G=(S,E,S_0,S_S,L)$.其中,S 是有限状态的集合.$E\subset S\times S$,$|E|\leqslant|S|^2$,即 E 表示集合 S 中状态间的转换关系,是集合 S 与其自身的笛卡尔乘积的子集.$S_0\subset S$,表示初始状态的集合.$S_S\subset S$,表示成功状态的集合.$L:S\to 2^P$,表示对状态的标记函数,S 中的每个状态对应一组原子命题的真值.

定义 2 给定有限全集 U 与集合 U 的部分子集构成的源集合簇 S 和目的集合簇 M.对于集合簇 C,若集合簇 C 为集合簇 M 的子集且集合簇 C 中所有元素的并集是集合簇 S 的碰集,则称集合簇 C 覆盖集合簇 S.为集合簇 M 中的每个元素设权值 $\omega:\mathbf{R}^+$.最优弥补集问题,即对于给定的输入有限全集 U、源集合簇 S 和目的集合簇 M,计算目的集合簇 M 的子集,使其覆盖源集合簇 S 且含最少权值.

3 基于转换的攻击图分析方法

3.1 最优弥补集问题的等价性

定义 3 对于二分图的两个互不相交的顶点集 A_1、A_2,若对于点集 A_1 中的任意一点 a,点集 A_2 中都存在至少一点 a' 与点 a 构成边,则称点集 A_2 覆盖点集 A_1.

引理 1 最优弥补集问题与加权集合覆盖问题等价.

证明 一个最优弥补集问题可以对应为一个二分图.其中,二分图的点集 A_1 的点分别表示源集合簇 S 中的不同元素,二分图的点集 A_2 的点分别表示目的集合簇 M 中的不同元素,二分图的边表示源集合与目的集合有交集.则,最优弥补集问题的目的是寻找点集 A_2 的最小权重子集使之覆盖点集 A_1.在二分图中,对于点集 A_1 中的任意点都至少存在上述问题解集中的一点与之构成边.所以该最优弥补集问题可等价二分图问题 Q_1:寻找二分图中的点集 A_2 的最小权值子集使之覆盖点集 A_1.

以点集 A_1 的点表示与目的集合簇的元素有非空交集的集合,将点集 A_2 的点表示为元素,则有加权集合覆盖问题 Q_2:寻找点集 A_2 的最小权值子集使之覆盖点集 A_1.显然,加权集合覆盖问题 Q_2 与二分图问题 Q_1 等价.因而,最优弥补集问题与加权集合覆盖问题等价.

引理证毕.

定理 1 最优弥补集问题与加权碰集问题等价.

证明 根据加权集合覆盖问题与加权碰集问题的等价性,引理 1 最优弥补集问题与加权集合覆盖问题等价,定理得证.

3.2 最优弥补集问题的形式化转换方法

根据上节的证明过程,可以得到将最优弥补集问题转化为加权碰集问题的方法:给定的输入有限全集 U、源集合簇 S 和目的集合簇 M,求解最优弥补集问题.

最优弥补集问题:

$$\min\Big(\sum_{c\in C'}\omega_c\Big)\text{ 满足}$$

$$\forall_{s'\in S}\Big(\bigcup_{c\in C'}c\Big)\cap s'\neq\varnothing,\ C'\subset M,$$

$$\forall_{s'\in S}s'\subset U,\ \forall_{m'\in M}m'\subset U.$$

转化为加权集合覆盖问题:

$$\min\Big(\sum_{c\in C'}\omega_c\Big)\text{ 满足}$$

$$\bigcup_{c\in C'}c=S,\ C'\subset S\_\text{cover},\ \forall_{s'\in S\_\text{cover}}s'\subset S,$$

$$S\_\text{cover}=\{\{s'\mid m'\cap s'\neq\varnothing,\ s'\in S\}\mid m'\in M\}.$$

转化为加权碰集问题:

$$\min\Big(\sum_{c\in C'}\omega_c\Big)\text{ 满足}$$

$$\forall_{s'\in S\_\text{hit}}C'\cap s'\neq\varnothing,\ C'\subset M,\ \forall_{s'\in S\_\text{hit}}s'\subset M,$$

$$S\_\text{hit}=\{\{m'\mid m'\cap s'\neq\varnothing,\ m'\in M\}\mid s'\in S\}.$$

下面是对转换方法的举例说明.对于有限全集{1,2,3,4,5,6},与集合 U 的部分子集构成的集合簇{A={1,2,3},B={3,4},C={5,6},D={1,2,6}}与集合簇{Z={1,3},Y={2,6},X={1,4},W={3,5}},标示如图 1,则以下两个问题等价:

最优弥补集问题:对于给定的输入有限全集{1,2,3,4,5,6}、源集合簇{A,B,C,D}和目的集合簇{Z,Y,X,W},计算目的集合簇的子集,使其覆盖源集合簇且含最小权值.

加权碰集问题:对于给定的输入有限全集{Z,Y,X,W}和集合簇{A'={Z,Y,X,W},B'={Z,X,W},C'={Y,W},D'={Z,Y,X}},计算最小权值的碰集.

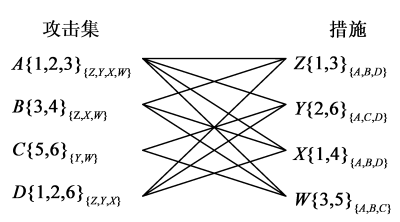

图1 最优弥补集问题与加权碰集问题的二分图实例

3.3 基于转换的分析方法

对攻击图进行分析,求解最优弥补集问题的一般

方法是通过计算最小关键攻击集.所谓关键攻击集,是一个原子攻击集,通过对该原子攻击集的防御,可以保证整个网络的安全.而最小关键攻击集指包含元素数目最少的关键攻击集.该方法包括两步:第一步寻找最小关键攻击集;第二步寻找最小代价的措施集使之能防御该最小关键攻击集.

将最优弥补集问题分成两部分求解,实际是一个贪心算法的思想,但是最优弥补集问题并不符合最优子结构性质.在寻找最小关键攻击集时,仅考虑对于当前看来最好的选择,即最小关键攻击集,而没有考虑整体最优的情况.而以最小关键攻击集作为输入的最优措施集问题的解通常并不是最优弥补集问题的全局最优解,反而很容易陷入局部最优.

如上,对于最优弥补集问题,两步求解的方法容易导致局部最优情况的发生.而为了修正结果,需要扩大方法第二部分的输入规模,又增大了问题的规模.根据定理 1,在不增大问题规模的前提下,最优弥补集问题可以在多项式时间内转换为加权碰集问题.这样,本文将最优弥补集问题转换为一个单一加权碰集问题以减小问题陷入局部最优的可能性.

下面就基于关键攻击集的分析方法与基于转换的分析方法进行对比分析.基于关键攻击集的分析方法若要计算最优解,需要遍历所有的极小关键攻击集,对每个极小关键攻击集遍历对应的所有极小弥补集,最后比较得出最优弥补集.而基于转换的分析方法,将最优弥补集问题转换为加权碰集问题,然后进行一次对极小碰集的遍历.因此,基于转换的分析方法在效率上有较大提高.

每个弥补集中元素的并集都包含了一个或多个极小关键攻击集.对于转换后的加权碰集问题,需要计算所有极小碰集,即原弥补集问题中的弥补集.这样,相较基于关键攻击集的分析方法需要对所有的极小关键攻击集计算弥补集,转换后的加权碰集问题只涉及极小碰集所对应的极小关键攻击集,从而缩小了候选极小关键攻击集的规模.由于碰集问题是 *NP* 完全问题,一般对其进行近似算法或者优化算法处理.也由于弥补集与极小关键攻击集的一对多关系,在相同时间内,基于转换的分析方法拥有更好的搜索能力.

4　实验分析

贪心算法是攻击图分析中比较常见和有效的一种近似算法,本文沿用文献[4]提供的贪心算法在吉林省福利彩票销售系统中对基于关键攻击集的分析方法和基于转换的分析方法进行了对比分析.实验环境如下:Red Flag DC Server 5.0, IBM 机架式服务器 xSeries 3650M4.实验采用了 5 种不同规模的攻击图,具体特征如下表 1.由于贪心算法具有随机性,对每种规模的攻击图分别计算 200 次取统计平均值.实验通过近似度来衡量方法的优劣.所谓近似度,取目标解与全局最优解的权值之比.

表 1　5 种规模的攻击图的统计特征

攻击图	节点	边	有效路径	措施
A	54	65	5	29
B	95	118	85	36
C	148	187	825	43
D	213	272	8580	50
E	290	373	82660	57

图 2 是对 5 种规模的攻击图分别采用基于关键攻击集的分析方法和基于转换的分析方法得到的实验结果.随着攻击图问题规模的增大,虽然两种方法以贪心算法实现后,结果的近似度均呈现上升趋势.但是两者相较,基于转换的分析方法的计算结果普遍优于基于关键攻击集的分析方法.并且,随问题规模增大,基于转换的分析方法较基于关键攻击集的分析方法上升趋势较为平缓.

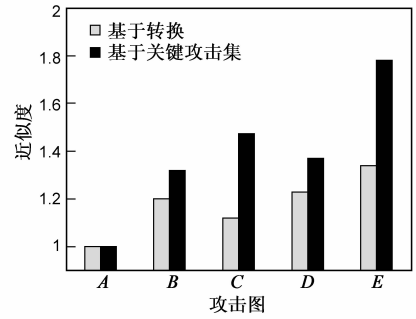

图2　两种分析方法的近似度对比图

5　结论

本文分析了基于关键攻击集的最优弥补集问题分析方法在逼近全局最优解方面的不足,在此基础上提出将最优弥补集问题作为单一问题进行处理的方法.通过理论证明,最优弥补集问题可以等价转换为加权碰集问题.因此在不增加问题规模的前提下,本文将最优弥补集问题转换为单一的加权碰集问题进行求解,并推导出相应转换方法.最后通过实验表明,在收敛于全局最优解方面,基于转换的分析方法较传统基于关键攻击集的分析方法有更好的性能.然而,加权碰集问题是 NP 完全问题.虽然目前较为可行的解决方案是使用优化算法,但如何在有限时间内获得满意的结果,仍是一个尚待继续研究的问题也是下一步研究的部分.

参考文献

[1] QIAN Yaguan, WU Chunming, YANG Qiang, et al. Network traffic anomaly detection based on maximum entropy model

[J]. Chinese Journal of Electronics, 2012, 21(CJE-3): 579 – 582.

[2] Phillips C, Swiler L. A graph-based system for network-Vulnerability analysis[A]. Proceedings of the 1998 Workshop on New Security Paradigms[C]. New York: ACM, 1998. 71 – 79.

[3] Ammann P, Wijesekera D, Kaushik S. Scalable, graph-based network vulnerability analysis[A]. Proceedings of the 9th ACM Conference on Computer and Communications Security[C]. New York: ACM, 2002. 217 – 224.

[4] Jha S, Sheyner O, Wing J. Two formal analyses of attack graphs[A]. Proceedings of the 15th IEEE Computer Security Foundations Workshop[C]. Los Alamitos: IEEE Computer Society, 2002. 49 – 63.

[5] Novel S, Jajodia S, O'Berry B, Jacobs M. Efficient minimum-cost network hardening via exploit dependency graphs[A]. Proceedings of the 19th Annual Computer Security Applications Conference[C]. Los Alamitos: IEEE Computer Society, 2003. 86 – 95.

[6] AlbaneseM, Jajodia S, Noel S. Time efficient and cost-effective network hardening using attack graphs[A]. Proceedings of the 42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks[C]. Boston: IEEE Computer Society, 2012. 1 – 12.

[7] Wang L, Novel S, Jajodia S. Minimum-Cost network hardening using attack graphs[J]. Computer Communications, 2006, 29(18): 3812 – 3824.

[8] 陈峰,张怡,苏金树,韩文报. 攻击图的两种形式化分析[J]. 软件学报, 2010, 21(4): 838 – 848.
Chen Feng, Zhang Yi, Su Jinshu, Han Wenbao. Two formal analyses of attack graphs[J]. Journal of Software, 2010, 21(4): 838 – 848. (in Chinese)

作者简介

闫 峰 男, 1973 年出生于吉林长岭, 博士生, 高级工程师, 研究方向: 计算机网络、网络安全.
E-mail: tt@vip.sina.com

刘淑芬 女, 1950 年出生于吉林榆树, 教授, 博士生导师, 研究方向: 计算机支持协同工作、软件体系结构、基于模型驱动的软件编程方法、网络管理技术.
E-mail: liusf@mail.jlu.edu.cn