基于属性邻接矩阵的攻击图表示方法研究

苏婷婷* 潘晓中 肖海燕 申军伟
(武警工程大学网络与信息安全武警部队重点实验室 西安 710086)

摘 要：为降低攻击图的复杂度，方便安全人员的理解分析，该文提出了属性邻接矩阵的表示方法，并设计了多步邻接矩阵的算法。利用邻接矩阵元素表示目标网络中各属性的连接关系，通过矩阵算法得到多步攻击路径，对邻接矩阵进行概率计算可得攻击成功的概率。实验环境验证了所提方法能提高攻击图的可视性，降低安全分析的难度。

关键词：网络安全；攻击图；邻接矩阵；脆弱性
中图分类号：TP309 **文献标识码**： A **文章编号**：1009-5896(2012)07-1744-04
DOI: 10.3724/SP.J.1146.2012.00261

Research on Attack Graph Based on Attributes Adjacncy Matrix

Su Ting-ting Pan Xiao-zhong Xiao Hai-yan Shen Jun-wei
(*Key Laboratory of Network & Information Security of Armed Police Force*,
Engineering University of Armed Police Force, *Xi'an* 710086, *China*)

Abstract: In order to extend visualization of attack graphs, a method of adjacency matrix based on attributes is proposed, and the arithmetic of multi-step adjacency matrix is designed. The elements of the matrix shows connections of the network. The probability of attack paths is obtained through numeration of probability of the adjacency matrix. Experiment results show that the proposed method can efficiently decrease the complexity of attack graphs, and make it easier to analyze the network vulnerability.

Key words: Network security; Attack graphs; Adjacency matrix; Vulnerability

1 引言

攻击图是用于网络安全分析的重要工具，它经历了从手工构建到自动构建，从面向小型网络到面向大规模网络的发展[1−5]。大规模目标网络包含的节点数目庞大，相互之间连接关系复杂，为攻击图的自动构建和分析带来巨大的困难。为增强攻击图的可视性，简洁直观地展示攻击者的攻击路径，方便安全人员进行安全分析，本文提出了攻击图的属性邻接矩阵表示方法，利用矩阵来表示网络中各属性节点之间的攻击行为，并给出了多步属性邻接矩阵的计算方法，表示属性节点之间的多步攻击行为。

研究者提出了多种攻击图的表示方法，主要可分为两种：一是用顶点和有向边来表示，二是用邻接矩阵来表示。文献[6]提出状态攻击图，图中节点代表目标网络和攻击者的全局状态，节点内容通常包括主机名、用户权限、攻击的影响等，有向边代表原子攻击，它被执行后将会引起全局状态的变迁。文献[7]提出了属性攻击图，图中包含两类节点：一类节点为攻击行为节点；另一类节点为属性节点，表示这些原子攻击的前提或后果。属性攻击图包含了攻击者执行各个原子攻击的前提属性和攻击行为发生后所拥有的属性，相对状态攻击图更简洁，但可能存在含圈路径。另外，文献[8]提出了渗透依赖攻击图，文献[9]提出了属性依赖攻击图。顶点和有向边的表示方法能够直观地表示攻击者的攻击路径，对小规模网络具有较强的表现力，但对于较大规模的网络，顶点和有向边数目繁多、结构复杂，为攻击图的理解和分析带来很大难度。

文献[10]提出了邻接矩阵表示方法，用 0 和 1 表示各节点之间的连接关系，0 表示两个节点之间不存在攻击行为，1 表示存在攻击行为，通过对矩阵进行乘法运算分析任意两个节点之间是否多步攻击行为。邻接矩阵增强了攻击图的可视性，并方便了基于攻击图的安全分析。文献[11]提出了风险邻接矩阵，使用非负数值来表示邻接矩阵中的元素，并给出了多步最大可能风险邻接矩阵和多步最大损失风险邻接矩阵的计算方法，用来描述成功可能性最大的攻击行为的概率以及该攻击行为造成的损失。采用 0 和 1 的表示方法能描述节点之间是否存在攻击行为，但不能显示具体的攻击行为。风险邻接矩阵

2012-03-15 收到，2012-05-11 改回
国家自然科学基金项目(61103230, 61103231)资助课题
*通信作者：苏婷婷 suting0518@163.com

能够表示可能性最大的攻击行为，但不能展示攻击者所有可能的攻击路径。

本文提出的属性邻接矩阵，保留了邻接矩阵可视性优势。利用攻击行为表示矩阵中元素表示相对应的属性之间的攻击行为，对属性邻接矩阵进行运算可得到任意两个属性之间的所有多步攻击路径。

2　属性邻接矩阵

2.1 属性邻接矩阵的提出

定义 1　对于存在 n 个属性节点的目标网络，$\boldsymbol{V}$ 是一个 $n\times n$ 的矩阵，v_{ij} 表示从属性 i 到 j 的攻击行为，若 v_{ij} 为非零值则存在 i 到 j 的攻击路径，若为零则不存在。称这种攻击图表示方法为属性邻接矩阵。

图 1 是一个简单的属性攻击图，图中文字节点表示属性，椭圆节点表示攻击行为，节点之间通过有向边连接。图中 $V1$ 到 2 的有向边是攻击行为 2 的前提边，$V1$ 是攻击行为 2 发生的前提属性；从 2 到 $V3$ 的有向边是攻击行为 2 的后果边，$V3$ 是攻击行为 2 发生后所拥有的后果属性。图 2 与图 1 是同一个目标网络，用属性邻接矩阵表示。用 $i\xrightarrow{1}j:i(v_{ij})j$ 表示从 i 到 j 的单步攻击路径，其中( )内的元素表示攻击行为。矩阵中 $v_{13}=2$ 表示从 $V1$ 出发，利用攻击行为 2 可以获得 $V3$，攻击路径为 $V1\xrightarrow{1}V3:V1(2)V3$；$v_{14}=0$ 表示从 $V1$ 到 $V4$ 不存在单步攻击路径。

2.2 多步属性邻接矩阵

与属性攻击图相比，邻接矩阵的表示方法在表示单步攻击行为的时候较为直观，但是无法表示多步攻击行为。因此，本文提出基于属性攻击图的多步邻接矩阵表示方法。

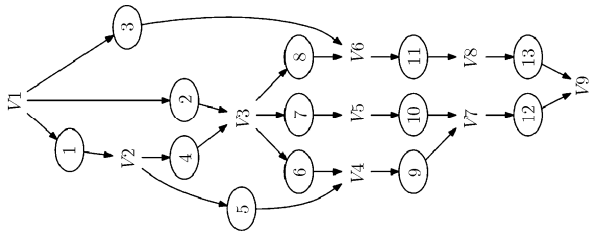

图 1 属性攻击图

$$\boldsymbol{V}=\begin{pmatrix}0&1&2&0&0&3&0&0&0\\0&0&4&5&0&0&0&0&0\\0&0&0&6&7&8&0&0&0\\0&0&0&0&0&0&9&0&0\\0&0&0&0&0&0&10&0&0\\0&0&0&0&0&0&0&11&0\\0&0&0&0&0&0&0&0&12\\0&0&0&0&0&0&0&0&13\\0&0&0&0&0&0&0&0&0\end{pmatrix}$$

图 2 属性邻接矩阵

定义 2　$\overset{n}{\underset{i=1}{\curlyvee}}a_i=a_1\oplus a_2\oplus\cdots\oplus a_n(i=1,2,3,\cdots,n)$。

定义 3　$v_{ik}\circ v_{kj}$ 为从属性 i 到 j 的两个相邻的攻击行为，k 为中间结点。表示从 i 到 j 的两步攻击路径为 $i\xrightarrow{2}j:i(v_{ik})k(v_{kj})j$。

定义 4　设矩阵 $\boldsymbol{A}=(a_{ij})_{m\times s}$，$\boldsymbol{B}=(b_{ij})_{s\times n}$，$\boldsymbol{A}*\boldsymbol{B}$ 是指一个 $m\times n$ 矩阵 $\boldsymbol{C}=(c_{ij})_{m\times n}$，其中矩阵元素 $c_{ij}=[a_{i1}\circ b_{1j}]\oplus[a_{i2}\circ b_{2j}]\oplus\cdots\oplus[a_{is}\circ b_{sj}]=\overset{s}{\underset{k=1}{\curlyvee}}[a_{ik}\circ b_{kj}]$，记 $\boldsymbol{C}=\boldsymbol{A}*\boldsymbol{B}$。

对于单步属性邻接矩阵 $\boldsymbol{V}$，称 $\boldsymbol{V}^2=\boldsymbol{V}*\boldsymbol{V}$ 为 2 步属性邻接矩阵，其中 $v_{ij}^2=\overset{n}{\underset{k=1}{\curlyvee}}\left[v_{ik}\circ v_{kj}\right]$。对图 2 进行计算得到 2 步属性邻接矩阵，其中 $v_{14}^2=[v_{12}\circ v_{24}]\oplus[v_{13}\circ v_{34}]$，表示从 $V1$ 可以通过 $v_{12}\circ v_{24}$ 和 $v_{13}\circ v_{34}$ 两种连续的攻击行为获得 $V4$，攻击路径表示为 $V1\xrightarrow{2}V4:[V1(1)V2(5)V4]\oplus[V1(2)V3(6)V4]$。

定理 1　m 步邻接矩阵 $\boldsymbol{V}^m$ 中元素 $v_{ij}^m=\overset{n}{\underset{k=1}{\curlyvee}}[v_{ik}^{m-1}\circ v_{kj}]$ 表示属性 i 到 j 的 m 步攻击行为。

证明　$m=1$ 时，$\boldsymbol{V}$ 中元素 v_{ij} 表示从属性 i 到 j 的单步攻击行为，$m=2$ 时，$\boldsymbol{V}^2=\boldsymbol{V}*\boldsymbol{V}$ 中矩阵元素 $v_{ij}^2=\overset{n}{\underset{k=1}{\curlyvee}}\left[v_{ik}\circ v_{kj}\right]$ 表示从属性 i 到 j 的 2 步攻击行为，定理显然成立；假设 $m=t$ 时，$\boldsymbol{V}^t=\boldsymbol{V}^{t-1}*\boldsymbol{V}$ 中元素 $v_{ij}^t=\overset{n}{\underset{l=1}{\curlyvee}}\left[v_{il}^{t-1}\circ v_{lj}\right]$ 表示属性 i 到 j 的 t 步攻击行为，$m=t+1$，$v_{ij}^{t+1}=\overset{n}{\underset{k=1}{\curlyvee}}\left[v_{ik}^t\circ v_{kj}\right]$，其中 v_{ik}^t 是 i 到 k 的 t 步攻击行为，v_{kj} 是 k 到 j 的单步攻击行为。攻击者在经过 t 步攻击取得属性 k 后，再实施从 k 到 j 的单步攻击，所以 $v_{ij}^{t+1}=\overset{n}{\underset{k=1}{\curlyvee}}\left[v_{ik}^t\circ v_{kj}\right]$ 是 i 到 j 的 $t+1$ 步攻击行为。　证毕

2.3 属性邻接矩阵的分析

属性邻接矩阵 $\boldsymbol{V}$ 对应的概率用 $\boldsymbol{P}$ 表示。$\boldsymbol{P}$ 是一个 $n\times n$ 的矩阵，其中 p_{ij} 表示属性邻接矩阵中攻击行为 v_{ij} 成功的概率，即攻击者采用 v_{ij} 从属性 i 出发获得属性 j 成功的概率。多步攻击路径成功的概率是路径中包含的所有单步攻击行为成功概率的乘积。

图 3 是图 2 对应的概率矩阵，$V1$ 到 $V2$ 的单步攻击路径 $V1\xrightarrow{1}V2:V1(v_{12})V2$ 成功的概率 $p_{12}=0.6$；从 $V1$ 到 $V4$ 2 步攻击路径 $V1\xrightarrow{2}V4:[V1(v_{12})V2(v_{24})V4]\oplus[V1(v_{13})V3(v_{34})V4]$ 成功的概率为 $p_{14}^2=p_{12}\times p_{24}\oplus p_{13}\times p_{34}=0.42\oplus 0.25$，表示攻击者从 $V1$ 到 $V4$ 两种 2 步攻击路径成功的可能性分别为 0.42 和 0.25。

$$\boldsymbol{P}=\begin{pmatrix}0&0.6&0.5&0&0&0.4&0&0&0\\0&0&0.6&0.7&0&0&0&0&0\\0&0&0&0.5&0.6&0.3&0&0&0\\0&0&0&0&0&0&0.3&0&0\\0&0&0&0&0&0&0.7&0&0\\0&0&0&0&0&0&0&0.3&0\\0&0&0&0&0&0&0&0&0.4\\0&0&0&0&0&0&0&0&0.6\\0&0&0&0&0&0&0&0&0\end{pmatrix}$$

图 3 概率邻接矩阵

属性邻接矩阵中包含了所有的属性及各属性之间的连接关系，通过矩阵运算可以求得任意属性之间的攻击路径。多步属性邻接矩阵的时间复杂度不超过$O(n^3)$，其中n为目标网络中包含的属性节点。属性邻接矩阵中对角线元素表示对应属性到其自身的攻击路径，形成了回路增加了计算的复杂度，为安全人员的分析带来困难。采用文献[11]提出的方法，通过将对角线元素置0，可以避免出现含圈路径。

3 实验

本文模拟类似文献[9]的网络环境，包含 3 台主机ip_0，ip_1，ip_2。主机之间的连接关系如表 1 所示，表中的每个元素都表示相对应的两台主机(h_1,h_2)的连接关系，分别由 3 个布尔值表示。第 1 个值为y表示h_1和h_2存在物理连接，为n则不存在；第 2 个值为y表示h_1和h_2能通过 ftp 端口连接，为n则不能；第 3 个值为y表示h_1和h_2能通过 sshd 端口连接，为n则不能。在攻击者实施攻击行为之前，任意两台主机之间不存在信任关系，攻击者拥有ip_0的 user 权限，任意两台主机之间不存在信任关系，攻击目标是获取ip_2的 root 权限。

表 1 主机连接关系

	ip_0	ip_1	ip_2
ip_0	y,y,n	y,y,y	y,y,n
ip_1	y,y,n	y,y,y	y,y,n
ip_2	y,y,n	y,y,y	y,y,n

实验中包含 4 种原子攻击行为：

0: sshd buffer overflow，攻击者可以直接获得目标主机的 root 权限；

1: ftp_rhosts，攻击者可以获得目标主机的信任；

2: rsh login，攻击者可以获得目标主机的 user 权限；

3: local buffer overflow，攻击者可以获得本地主机的 root 权限。

采用文献[9]提出的算法，分别采用属性攻击图(如图 4)和属性邻接矩阵(如图 5)表示生成的攻击图。属性攻击图中包含 15 个属性，12 个原子攻击行为，36 条有向边，结构较复杂不便理解。属性邻接矩阵是一个15×15的矩阵，矩阵中包含的非零值表示网络中的对应属性之间的连接关系。

经过对大量真实攻击事件的统计，研究人员发现攻击者实施的有效攻击路径长度一般不大于 3 步，因此在本实验中只研究 3 步以内的攻击路径。图 5 显示了全局攻击图中所有的单步攻击行为，进行 2 步邻接矩阵计算可得 user(0) 到 root(2) 的 2 步攻击路径：$\text{user(0)}\xrightarrow{2}\text{root(2)}:\text{user(0)(rsh(0,2))user(2)(local\_bof(2))root(2)}$。经 3 步邻接矩阵计算可得 user(0) 到 root(2) 的所有 3 步攻击路径：$\text{user(0)}\xrightarrow{3}\text{root(2)}:\text{user(0)(sshd\_bof(0,1))user(1)(rsh(1,2))user(2)(local\_bof(2))root(2)}\oplus\text{user(0)(ftp\_rhost(0,2))trust(2,0)((rsh(0,2))user(2)(local\_bof(2))root(2)}$。

求 user(0) 到 root(2) 最短路径时，需要对邻接矩阵进行迭代运算直到 user(0) 到 root(2) 对应的矩阵元素值不为 0，即为最短路径中包含的攻击行为。实验中的最短路径为$\text{user(0)}\xrightarrow{2}\text{root(2)}:\text{user(0)(rsh(0,2))user(2)(local_bof(2))root(2)}$，只进行了一次矩阵运算。对于大规模网络，求最短路径只需要对特定的属性进行矩阵运算，时间复杂度最坏情况下不超过$O(n^2)$，而在属性攻击图中寻找最短路径的复杂度随着攻击行为数目的增加呈指数增加[9]。

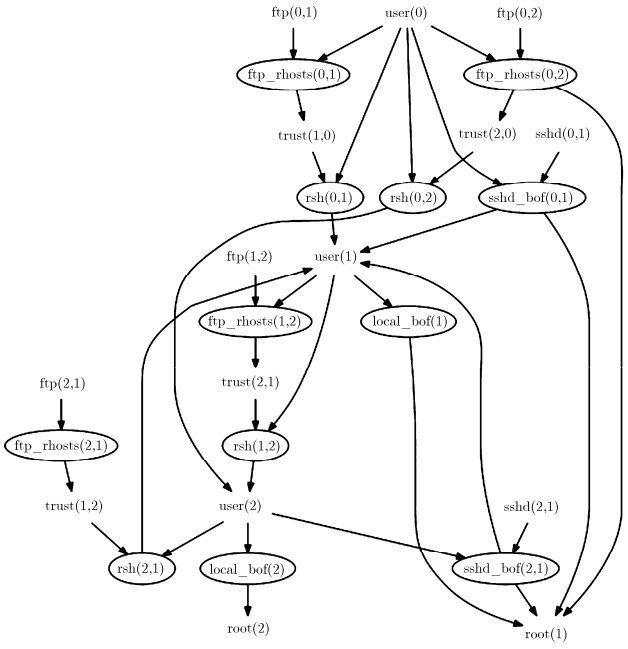

图 4 属性攻击图表示法

	user(0)	ftp(0,1)	trust(1,0)	user(1)	ftp(0,2)	trust(2,0)	user(2)	ftp(2,1)	trust(1,2)	ftp(1,2)	trust(2,1)	sshd(0,1)	sshd(2,1)	root(1)	root(2)
user(0)	0	0	ftp_rhosts(0,1)	sshd_bof(0,1)	0	ftp_rhosts(0,2)	rsh(0,2)	0	0	0	0	0	0	sshd_bof(0,1)	0
ftp(0,1)	0	0	ftp_rhosts(0,1)	0	0	0	0	0	0	0	0	0	0	0	0
trust(1,0)	0	0	0	rsh(0,1)	0	0	0	0	0	0	0	0	0	0	0
user(1)	0	0	0	0	0	0	rsh(1,2)	0	0	0	ftp_rhosts(1,2)	0	0	local_bof(1)	0
ftp(0,2)	0	0	0	0	0	ftp_rhosts(0,2)	0	0	0	0	0	0	0	0	0
trust(2,0)	0	0	0	0	0	0	rsh(0,2)	0	0	0	0	0	0	0	0
user(2)	0	0	0	rsh(2,1)	0	0	0	0	ftp_rhosts(2,1)	0	0	0	0	sshd_bof(2,1)	local_bof(2)
ftp(2,1)	0	0	0	0	0	0	0	0	ftp_rhosts(2,1)	0	0	0	0	0	0
trust(1,2)	0	0	0	rsh(2,1)	0	0	0	0	0	0	0	0	0	0	0
ftp(1,2)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
trust(2,1)	0	0	0	0	0	0	0	0	0	0	ftp_rhosts(1,2)	0	0	0	0
sshd(0,1)	0	0	0	sshd_bof(0,1)	0	0	0	0	0	0	0	0	0	sshd_bof(0,1)	0
sshd(2,1)	0	0	0	sshd_bof(2,1)	0	0	0	0	0	0	0	0	0	sshd_bof(2,1)	0
root(1)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
root(2)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

图 5 属性邻接矩阵表示法

4 结束语

本文讨论了大规模网络中攻击图的可视化问题，提出了攻击图属性邻接矩阵表示方法，在表示多步攻击路径时，提出了多步邻接矩阵，并给出了攻击成功概率的计算方法以及复杂度分析。属性邻接矩阵能够表示目标网络内的所有连接关系，与顶点和有向边的表示方法相比，增强了攻击图的可视性，降低了理解分析的难度，并能同时展示全局攻击图和部分攻击图。在模拟环境中与传统的属性攻击图进行了对比分析，表明了所提概念和方法的简洁性、合理性、有效性。

参 考 文 献

[1] 陈锋, 毛捍东, 张维明, 等. 攻击图技术研究进展[J]. 计算机科学, 2011, 38(11): 12–18.
Chen Feng, Mao Han-dong, Zhang Wei-ming, *et al.*. Survey of attack graph technique [J]. *Computer Science*, 2011, 38(11): 12–18.

[2] Supriya Khaitan and Supripa Raheja. Finding optimal attack path using attack graphs: a survey[J]. *International Journal of Soft Computing and Engineering*, 2011, 1(3): 2231–2307.

[3] Swiler L P, Phillips C, Gaylor T, *et al.*. A graph-based network vulnerability analysis system[R]. California: National Laboratories, 1998: 71–79.

[4] Shaojun Zhang and Shanshan Song. A novel attack graph posterior inference model based on Bayesian network[J]. *Journal of Information Security*, 2011, 2: 8–27.

[5] Ritchey R W and Ammann P. Using model checking to analyze network vulnerabilities[C]. Security and Privacy, IEEE, NJ, 2000: 156–165.

[6] Sheyner O, Jha S, Wing J M, *et al.*. Automated generation and analysis of attack graphs[C]. Security and Privacy, IEEE, NJ, 2002: 273–284.

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

[8] Ritchey R, O'Berry B, Noel S, *et al.*. Representing TCP/IP Connectivity for topological analysis of network security[C]. Proceedings of the 18th Annual Computer Security Applications Conference, IEEE, NJ, 2002: 25–31.

[9] Ammann P, Wijesekera D, Kaushik S, *et al.*. Scalable graph-based network vulnerability analysis[C]. Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington D.C., USA, 2002: 217–224.

[10] Noel S and Jajodia S. Understanding complex network attack graphs through clustered adjacency matrices[C]. Proceedings of the 21st Annual Computer Security Applications Conference, Tucson, USA, 2005: 160–169.

[11] 叶云, 徐锡山, 贾焰, 等. 基于攻击图的风险邻接矩阵研究[J]. 通信学报, 2011, 32(5): 112–120.
Ye Yun, Xu Xi-shan, Jia Yan, *et al.*. Research on the risk adjacency matrix based on attack graphs[J]. *Journal on Communications*, 2011, 32(5): 112–120.

苏婷婷：　女，1989 年生，硕士生，研究方向为网络安全.
潘晓中：　男，1964 年生，教授，主要研究方向为网络安全.
肖海燕：　女，1985 年生，讲师，主要研究方向为信息安全.