计算机科学
COMPUTER SCIENCE

基于贝叶斯攻击图的网络资产安全评估模型

曾昆仑, 张尼, 李维皓, 秦媛媛

引用本文

曾昆仑, 张尼, 李维皓, 秦媛媛. 基于贝叶斯攻击图的网络资产安全评估模型[J]. 计算机科学, 2023, 50(12): 349-358.

ZENG Kunlun, ZHANG Ni, LI Weihao, QIN Yuanyuan. Network Asset Security Assessment Model Based on Bayesian Attack Graph [J]. Computer Science, 2023, 50(12): 349-358.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.221000019

基于贝叶斯攻击图的网络资产安全评估模型

曾昆仑　张　尼　李维皓　秦媛媛
华北计算机系统工程研究所　北京 100083
(1184982609@qq.com)

摘　要　当前攻击图模型没有考虑漏洞的重复利用,并且风险概率计算不够全面、准确。为了准确评估网络资产环境安全,提出了一种基于贝叶斯攻击图的网络资产安全评估模型。首先根据漏洞可利用性、主机安防强度、漏洞时间可利用性和漏洞来源计算原子攻击成功概率,并结合贝叶斯网络量化攻击图。其次,根据漏洞的重复利用情况,对部分原子攻击成功概率和相应先验可达概率进行修正,作为对网络资产静态安全风险的评估。再次,根据实时发生的攻击事件,动态更新相关节点的可达概率,实现对网络资产安全风险的动态评估。最后,通过实验仿真和与现有工作的对比分析,对所提模型进行有效分析和验证。

关键词:贝叶斯攻击图;攻击事件;安全评估;后验概率;风险概率
中图法分类号　TP393

Network Asset Security Assessment Model Based on Bayesian Attack Graph

ZENG Kunlun,ZHANG Ni,LI Weihao and QIN Yuanyuan
National Computer System Engineering Research Institute of China,Beijing 100083,China

Abstract　Current attack graph models do not consider the reuse of vulnerabilities,and the calculation of risk probability is not comprehensive and accurate. In order to overcome these difficulties and evaluate security of network assets environment accurately,a network assets security assessment model based on Bayesian attack graph is proposed. Firstly,successful probabilities of atomic attacks are calculated according to vulnerability exploitability,host protection strength,vulnerability time exploitability and vulnerability source. Then attack graph is quantified by Bayesian network. Secondly,successful probabilities of partial atomic attacks and corresponding prior reachable probabilities are modified according to the reuse of vulnerabilities to evaluate static security risk of network assets. Thirdly,reachable probabilities of related nodes are updated dynamically according to real-time attack events to realize the dynamic assessment of network assets security risk. Finally,the proposed model is analyzed and verified effectively by experimental simulation and comparison with existing works.

Keywords　Bayesian attack graph,Attack event,Security assessment,Posterior probability,Risk probability

1　引言

信息技术的发展与普及极大地提高了生产生活效率,但也带来了大量的网络安全漏洞,攻击者可能利用网络系统中软硬件和安全策略上的缺陷,在未授权的情况下访问或破坏系统。理论上,为确保安全应扫描并修复网络中的全部漏洞,但实际上,由于安全与业务架构之间的矛盾、修复的代价、漏洞修复的滞后性等问题,通常无法修复全部漏洞[1]。为了经济、有效地消除漏洞,我们需要分析评估网络资产的风险概率,从而优先处理比较危险的漏洞和节点。

风险概率分为两种,一种是攻击成功概率,另一种是可达概率,即攻击者占有某个节点的概率。可达概率有两种形式:(1)根据已有经验和知识,在攻击事件发生前计算得到的先验可达概率;(2)根据发生的攻击事件,计算得到的后验可达概率。

现有研究工作中,评估攻击成功概率的指标过于单一,专注于漏洞可利用性,有的研究虽然考虑了多个指标,但缺少对它们的适当结合。而在评估漏洞可利用性时,现有研究没有考虑攻击图中的依赖关系和攻击路径,往往将攻击复杂度、用户交互、攻击向量和权限要求全部计算在内,导致评估结果不准确。此外,现有研究都没有考虑同一个漏洞在不同主机上被重复利用的情况。而在网络整体安全性的评估方面,部分现有研究没有考虑安全事件的影响。还有部分研究虽然考虑了这一点,但是计算方法不能保证父节点的概率更新在子节点之前,因此,其计算结果不准确,也没有将正向更新和反向更新相融合,故更新时会遗漏部分节点。

综上所述,针对现有研究工作中存在的问题,本文基于贝叶斯攻击图建立了一种网络资产安全评估模型,主要创新如下:

(1)综合分析漏洞可利用性、主机安防强度、漏洞时间可利用性和漏洞来源4个维度,并使用Fuzzy-AHP方法将四者结合,实现对攻击成功概率更加准确、全面的评估。

到稿日期:2022-10-07　返修日期:2023-03-16
通信作者:李维皓(weihaoli99@163.com)

(2)考虑到攻击图中的依赖关系和攻击路径,本文认为在评估漏洞可利用性时,不应采用现有研究中的方法将攻击向量和权限要求计算在内,并提出了一种针对漏洞重复利用情况的攻击成功概率修正方法。

(3)根据发生的攻击事件计算后验可达概率,综合考虑正向更新和反向更新,确保所有受影响节点的可达概率都能得到更新。并使用改进的广度优先搜索遍历算法,保证父节点的概率更新在子节点之前,提高了后验可达概率的准确性。

2 相关工作

攻击图由 Philips 等[2]于 20 世纪 90 年代提出,可以用于分析攻击者如何攻击目标,也可以用于分析网络管理员如何采取一系列措施来阻止攻击者实现目标[3]。根据类型不同,攻击图的节点可以表示主机、服务、漏洞和权限等网络安全要素,也可以表示账户被破解、权限被攻击者获取等网络安全状态,其有向边则用于表示攻击行为的先后顺序[4]。相较于对各个漏洞的孤立分析,攻击图可以将网络系统中的漏洞全部连接到一起[5],并且在图中枚举出全部入侵路径,直观地展示不同攻击步骤间的因果关系以及漏洞利用造成的潜在威胁,符合当今以多步攻击为主的现状[6]。

贝叶斯网络由 Pearl[7]提出,其中初始节点被赋予概率值,有向边用于表示节点间的因果关系,可以推理计算各个节点的条件概率。结合两者而形成的贝叶斯攻击图,利用了贝叶斯网络量化处理不确定性信息和因果关联的优势,以及不确定性推理能力,度量结果比较准确[8]。其可以很好地量化网络系统中的风险概率,评估各个节点的风险水平。

Wang 等[9]利用通用漏洞评分系统(Common Vulnerability Scoring System,CVSS)[10]中基础度量组和时间度量组的分数作为漏洞利用的概率,根据攻击路径逐步计算每个节点的累计可达概率。Xie 等[11]将贝叶斯网络和攻击图相结合,第一次深入探讨了攻击图中的 3 种不确定性,即攻击行为成功概率、攻击者选择的不确定性和安全告警正确率。Wang 等[12]发现了攻击图中漏洞节点的依赖关系,他们根据依赖关系修改 CVSS 中漏洞的基础度量算法,从而评估网络受攻击的概率及影响。Hu 等[13]用边代表攻击者获得的权限,提出网络边权限攻击图,再将目标被攻击概率、主机价值和攻击者所获权限重要性结合,计算出网络的脆弱性指数。Yang 等[14]在构建主机攻击图的基础上,依据漏洞属性值计算原子攻击概率,从而得到主机攻击概率,再结合漏洞影响值、主机的资产重要性和拓扑结构重要性,计算得到主机安全值。Zhao 等[1]利用漏洞 CVSS 得分、攻击路径长度和目标节点重要性评估攻击路径风险系数,再利用蚁群算法搜索攻击路径最大风险系数,并结合网络规模、网络性质和实际需求设置危险阈值,搜索高于阈值的攻击路径,最后据此计算得出低代价的网络安全加固策略。

但是上述工作大多没有考虑实时的攻击事件,它们是对网络系统的一般情况进行风险分析和安全评估,从而得到静态评估结果。

Chen 等[15]针对内部攻击,给出了单步攻击检测结果不确定性的刻画和概率推导方法,再根据观测事件推断当前攻击的潜在意图,并给出了针对目标的最大概率攻击路径。Wang 等[16]根据攻击者执行原子攻击的收益和面临的风险量化攻击意图,并结合原子攻击成功概率来描述贝叶斯攻击图中节点的状态转移概率。Yang 等[17]构建系统动态威胁属性攻击图,对多告警信息进行融合分析,再利用告警信息对网络威胁态势进行推断和量化分析。Luo 等[18]利用漏洞价值、攻击成本和攻击收益计算出原子攻击概率,再结合贝叶斯信念网络量化攻击图,建立静态风险评估模型,并根据入侵意图调整模型风险程度。Gao 等[19]、Li 等[20]首先在贝叶斯攻击图中计算各个节点的先验可达概率,再根据发生的攻击事件计算后验可达概率来评估动态风险。

上述研究基于攻击图建立了多种网络安全风险评估模型,但原子攻击成功概率的评估指标比较单一,专注于漏洞可利用性,有的虽然考虑了多个指标,但缺少对它们的适当结合。而在评估漏洞可利用性时,上述研究也没有考虑攻击图中的依赖关系和攻击路径,往往将攻击复杂度、用户交互、攻击向量和权限要求全部计算在内,导致评估结果不准确。此外,上述研究都没有考虑漏洞重复利用的情况。而在利用攻击事件、攻击意图等信息计算后验可达概率时,上述研究不能保证父节点的概率更新在子节点之前,因此其计算结果不够准确,也没有将正向更新和反向更新相融合,故更新时会遗漏部分节点。

为了解决上述问题,本文基于贝叶斯攻击图建立一种网络资产安全评估模型。一方面可以更加准确地评估漏洞可利用性和原子攻击成功概率,另一方面可以根据发生的攻击事件对相应节点的可达概率进行更新,及时预测接下来路径中节点的风险程度,并修正之前凭借经验知识生成的先验可达概率,根据攻击情况及时调整节点的风险级别,为管理员的安全决策提供支持。

3 研究动机

由于现在的网络系统中存在多样化频繁攻击威胁,因此针对漏洞利用的分析已成为网络安全领域的重要研究方向,其对网络资产的安全性具有重要意义。目前,已有一些基于攻击图分析漏洞利用、评估网络系统安全性的研究,但还存在一些不足。

图 1 给出了文献[17]中的网络拓扑,包含隔离区(Demilitarized Zone,DMZ)和可信域。表 1 列出了这个网络系统中存在的漏洞,Host 列表示漏洞所在的主机,Vulnerability 列表示漏洞来自哪一软件,CVE ID 列表示漏洞的 CVE 编号。攻击者可以利用这些漏洞,首先攻击 DMZ 域,再以其为跳板攻击可信域。

图 2 展示了文献[17]给出的基于图 1 和表 1 生成的攻击图,有向边表示从某台主机出发,利用另一台主机的漏洞对其进行攻击;节点表示系统中的各个主机;节点旁的数字表示该节点的先验可达概率。先验可达概率是利用原子攻击成功概率和贝叶斯网络的概率推理计算得出的,可以作为对该系统静态安全风险的评估。但是现有研究工作中,原子攻击成功概率的计算指标过于单一,也没有考虑漏洞重复利用的情况,并且计算漏洞可利用性时没

有考虑攻击图中的依赖关系和攻击路径。

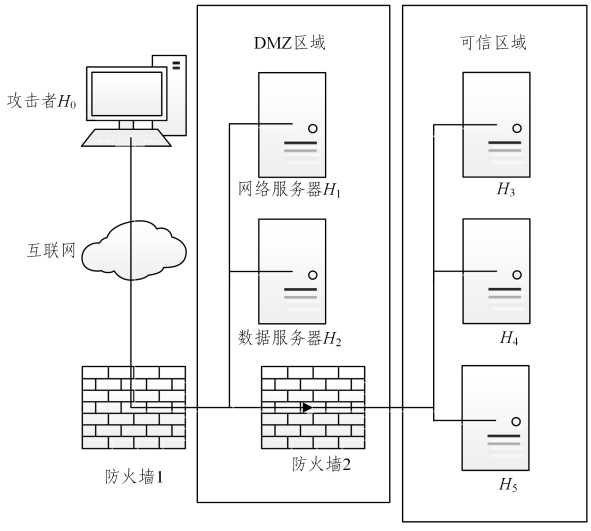


图 1 网络拓扑示例

Fig. 1 Network topology

表 1 漏洞信息

Table 1 Vulnerability information

Host	Vulnerability	CVE ID
H_1	IIS	CVE-2015-7597
H_2	Apache	CVE-2018-8015
H_3	HIDP	CVE-2018-8169
H_4	GUN Wget	CVE-2016-4971
H_5	NDproxy	CVE-2013-5065

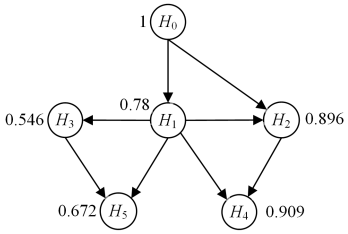


图 2 攻击图示例

Fig. 2 Attack graph

静态安全风险只能代表网络的一般风险情况，没有体现出攻击事件的影响，不能代表网络系统的动态风险情况。文献[20]根据发生的攻击事件，会对先验可达概率进行正向和反向更新，但是它不能保证父节点的概率更新在子节点之前，因此其计算结果不准确；并且它没有将正向更新和反向更新相融合，故在更新中会遗漏部分节点。以图 2 为例，如果其中 H_4 处发生了攻击事件，则文献[20]会将 H_1，H_2，H_4 的可达概率分别更新为 0.84，0.953，1，表明随着攻击事件的发生，网络的风险情况发生了改变，但它不会更新其他节点的可达概率。

基于上述问题，本文将攻击图中的依赖关系和攻击路径纳入对漏洞可利用性的评估，然后从多个维度计算原子攻击成功概率。再计算先验可达概率，并根据漏洞的重复利用情况，对部分原子攻击成功概率和相应先验可达概率进行修正。最后根据发生的攻击事件，利用提出的 Dynamic_BAG 算法，更新所有相关节点的可达概率，作为对网络资产动态安全风险的评估。

4 模型架构

基于贝叶斯攻击图的网络资产安全评估模型架构如图 3 所示，包括 6 个阶段：

(1)对网络系统中的节点配置和链路关系等信息进行识别。

(2)利用漏洞扫描器对网络系统进行扫描，发现其中的系统漏洞和服务漏洞。

(3)基于上述信息，利用攻击图生成算法生成不包含风险概率的基本攻击图。

(4)计算攻击图中各个原子攻击的成功概率，再结合贝叶斯网络和多步原子攻击因果关系，推理计算条件概率与条件节点先验可达概率，得到静态贝叶斯攻击图(Static Bayesian Attack Graph，SBAG)。

(5)如果静态贝叶斯攻击图中存在漏洞重复利用的情况，可以对相应原子攻击成功概率和先验可达概率进行修正，得到改进静态贝叶斯攻击图(Improve Static Bayesian Attack Graph，ISBAG)，用于评估静态安全风险。

(6)根据发生的网络安全事件，对改进静态贝叶斯攻击图中所有受影响节点的可达概率进行动态更新，计算其后验可达概率，得到动态贝叶斯攻击图(Dynamic Bayesian Attack Graph，DBAG)，用于评估动态安全风险。

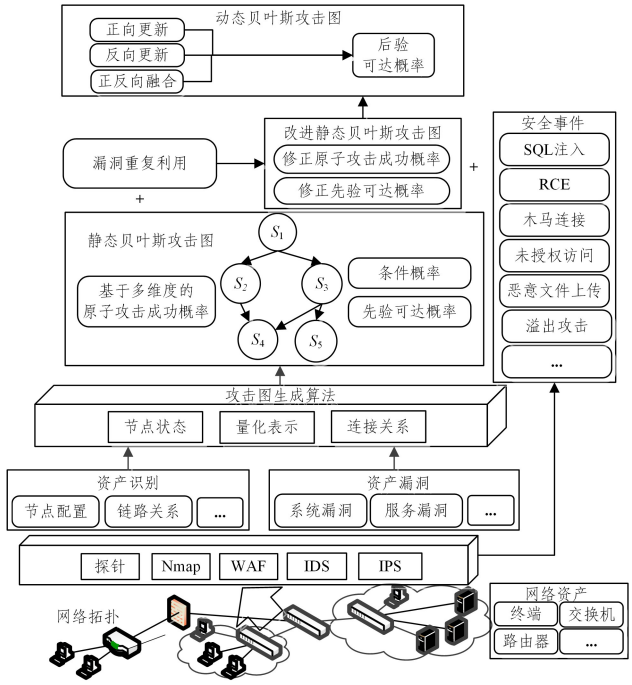


图 3 网络资产安全评估模型架构

Fig. 3 Architecture of network asset security assessment model

5 基于贝叶斯攻击图的网络资产安全评估模型

5.1 贝叶斯攻击图建立

攻击图一般可分为状态攻击图和属性攻击图两类。状态攻击图中节点表示主机名、服务等网络状态信息，有向边表示状态之间的迁移。但是状态攻击图在视觉上不够直观，并且在大规模网络中，随着状态的迁移，其状态增长速度过快。

属性攻击图将网络中的安全要素作为独立的属性节点，解决了状态攻击图的状态爆炸问题，对大规模网络有更好的适应性[4]。为了计算攻击图中各个节点的可达概率和可能的攻击路径，本文利用贝叶斯网络描述节点间的因果关系，结合属性攻击图的图形化结构，生成贝叶斯攻击图，对目标网络进行安全风险评估。

贝叶斯攻击图(Bayesian Attack Graph，BAG)是一个有向无环图，可以表示为 $BAG=(S,E,R,P)$，具体定义如下：

(1)S 是条件节点集合，表示攻击者占有的攻击资源和访问权限，其中 S_0 通常代表攻击者，其余节点则代表被攻击网络系统中的主机和相应访问权限。$S_i=\{0,1\}$，其中 1 表示攻击者已经占有该节点，0 表示攻击者未占有该节点。

(2)E 是攻击图中的有向边集合，它既表示节点间的因果关系，即每一条有向边的起点是其终点的前置条件；也表示利用漏洞进行攻击，这是条件节点的迁移方式。

(3)R 表示条件节点与其入边之间的关系，其根据各个漏洞之间的依赖关系，以及漏洞利用所需的实际情况来确定，可用 $\langle S_j,d_j\rangle$ 表示。$d_j\in\{\text{AND},\text{OR}\}$，AND 表示 S_j 的所有入边代表的攻击都成功了，攻击者才能占有 S_j 节点；OR 表示 S_j 的入边代表的攻击中有一个成功了，攻击者就能占有 S_j 节点。

(4)P 为攻击图中条件节点可达概率的集合，P_i 表示攻击者占有 S_i 的概率，即 S_i 的可达概率。

图 4 是一个贝叶斯攻击图的示例，其中 S_0,S_1,S_2,S_3,S_4 是条件节点且 S_0 是攻击的发起节点；E_1,E_2,E_3,E_4,E_5,E_6 是有向边；AND 表示 E_3 和 E_4 两个攻击都成功时攻击者才能占有 S_3；OR 表示 E_5 和 E_6 两个攻击任意一个成功时攻击者即可占有 S_4；P_0,P_1,P_2,P_3,P_4 分别表示攻击者占有 S_0,S_1,S_2,S_3,S_4 的概率，其中 P_0 通常为 1。

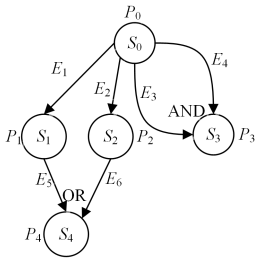


图 4 贝叶斯攻击图示例

Fig. 4 Bayesian attack graph

5.2 贝叶斯攻击图量化

攻击图构建完成后，需要量化网络系统的不确定性，从而评估各节点的安全风险。

网络系统的不确定性主要体现在两方面，一是原子攻击成功概率，即利用系统中主机上存在的某个漏洞，对该主机进行攻击的成功概率，主要受漏洞可利用性、主机安防强度、漏洞时间可利用性和漏洞来源以及漏洞重复利用情况的影响；二是各个节点的可达概率，代表攻击者占有该节点的可能性，可以借助贝叶斯概率推理得到。

5.2.1 漏洞可利用性

漏洞可利用性(Vulnerability Exploition，VE)表示漏洞利用的难度，可以利用 CVSS 进行量化计算，数值越大表示漏洞可利用性越高，数值越小表示漏洞可利用性越低。其中 CVSS 中文名为通用漏洞评分系统，用于评测漏洞的严重程度，并帮助确定所需反应的紧急度和重要性，通常与 CVE 漏洞一同公布。VE 的计算方法如下：

$$VE_i=AC_i*UI_i \tag{1}$$

其中，AC_i 表示攻击复杂度，分为高、低两个等级，取值分别为 0.44 和 0.77；UI_i 表示用户交互，分为不需要和需要两个等级，取值分别为 0.85 和 0.62。

现有研究利用 CVSS 对漏洞可利用性或攻击概率等进行量化计算时，通常会将 CVSS 中可利用性度量组(Exploitability Metrics，EM)包含的攻击向量(Attack Vector，AV)、攻击复杂度(Attack Complexity，AC)、权限要求(Privilege Required，PR)和用户交互(User Interaction，UI)全部连乘。但 CVSS 对漏洞的处理是孤立的，没有考虑目标网络中多步攻击之间的依赖关系[9]，漏洞是静态的概念，而利用漏洞进行攻击是动态的过程。

AV 指漏洞利用需要的环境，其分数体现了攻击者获取相应环境的难度，从而影响漏洞的严重性。但在动态的攻击过程中，攻击者必然已经通过前置操作获得了相应的环境，然后才会利用该漏洞进行攻击。即获取所需环境的难度体现在前置的攻击过程中，所以计算攻击者利用该漏洞进行攻击的成功概率时不应将 AV 的分数计算在内。

PR 表示攻击者在成功利用该漏洞之前必须具有的权限级别。与 AV 同理，在动态的攻击过程中，攻击者必然已经通过前置操作获得了相应的权限，然后才会利用该漏洞进行攻击，所以计算攻击成功概率时不应将 PR 的分数计算在内。

综上所述，AV 和 PR 都属于静态、孤立情况下对漏洞危险性的衡量，作为原子攻击成功概率的一部分，漏洞可利用性的计算不应包含它们，否则会降低原子攻击成功概率。如果两个原子攻击所用漏洞的 AV 和 PR 分值不同，更会造成相应原子攻击成功概率之间出现不合理的差异。

5.2.2 主机安防强度

从主机自身防御能力的角度分析，主机的安防措施完备程度越高，原子攻击成功实施的难度就越大。并且根据网络安全实践经验可知，原子攻击成功概率对安防措施的变化有较高的敏感度。参考文献[21]，本文将主机安防强度(Protection Strength，PS)划分为 5 个等级，如表 2 所列。主机的安防措施越完备，则安防等级越高；量化评分的分数越高，表示主机越安全，被攻击成功的概率越低。

表 2 安防强度量化分级

Table 2 Quantitative classification of protection strength

安防等级	量化值	安防措施描述
1	0.1	几乎不具备有效的安防措施
2	0.3	具备有效的检测类安防措施
3	0.5	具备有效的检测、防护类安防措施
4	0.7	具备有效的检测、防护和响应类安防措施
5	0.9	具备有效的检测、防护、响应和恢复类安防措施

5.2.3 漏洞时间可利用性

从时间的角度分析，漏洞被公布的时间越长，攻击者对它的研究就越深入，获得攻击代码和工具的可能性也越大。参考文献[22]，随着漏洞被公布时间的增加，漏洞利用代码和

工具产生的概率即漏洞时间可利用性(Time Exploitability，TE)也会增加。TE 符合 Pareto 分布，计算公式如下：

$$TE_i=1-\left(\frac{k}{t_i}\right)^{\alpha} \tag{2}$$

其中，k 和 α 是 Pareto 分布的参数，根据文献[22]的统计分析，其取值为 $\alpha=0.552$，$k=0.05029$；t_i 表示漏洞从公布之日到计算时的天数。

5.2.4 漏洞来源

从漏洞来源的角度分析，每个漏洞都有所属的软件，包括操作系统和应用软件，不同软件的市场占有率和用户数量是不同的。常见的软件因为用户数量多、市场占有率高，其漏洞对于攻击者而言潜在攻击收益就高。所以攻击者会更愿意研究这些漏洞，制作漏洞利用的代码和工具，可能获得的相关资料也较多，从而使攻击能力得到提升。与之相反，攻击者对于那些用户数量较少的软件的漏洞的重视程度就会下降，可能获得的资料也较少。

根据漏洞所属软件的常见程度，本文将漏洞来源(Vulnerability Source，VS)划分为 3 个等级，如表 3 所列。取值越大表示漏洞所属软件的用户人数越多、市场占有率越高，范围区间内的具体取值可由评估人员根据系统中漏洞的实际情况来赋值。

表 3 漏洞来源量化分级

Table 3 Quantitative classification of vulnerability sources

漏洞来源	取值	漏洞所属软件描述
常见	0.7～1	市场占有率很高，用户数量很多，如 linux 和 MS Office
较常见	0.3～0.7	有较高的市场占有率，有一定规模的用户，如 nginx 和 mysql
不常见	0.1～-0.3	市场占有率很低，用户规模有限

5.2.5 Fuzzy-AHP

模糊层次分析法(Fuzzy Analytical Hierarchy Process，Fuzzy-AHP)是一种常用的赋权方法，它将性质分析和数量分析相结合，将性质判断转化为数量结果[23]，具体步骤如下[24]。

步骤 1 建立模糊互补判断矩阵

将需要赋权的同一层次中的各个要素进行两两比较判断，评分标度为 0.1～0.9，分数越高表示前者相较于后者越重要，评分为 0.5 时表示两者一样重要。在本文中，漏洞可利用性、主机安防强度、漏洞时间可利用性和漏洞来源都是原子攻击成功概率的影响因素，所以对它们进行两两比较，从而构造模糊互补判断矩阵 $\boldsymbol{A}=(\tilde{a}_{ij})_{n\times n}$。其中 $\tilde{a}_{ij}=(a_{lij},a_{mij},a_{uij})$ 是三角模糊数，表示针对上层准则，元素 x_i 较元素 x_j 的重要程度。a_{lij}，a_{mij}，a_{uij} 分别表示专家认为的最低、最可能和最高的判断，如果 $a_{mij}>0.5$，说明专家认为最可能的情况下元素 x_i 比 x_j 更重要。并且 $\boldsymbol{A}$ 中元素满足 $a_{lij}+a_{uji}=a_{mij}+a_{mji}=a_{uij}+a_{lji}=1$。

步骤 2 模糊权重计算

设当前层次中要素个数为 n，则第 i 个要素相对于上层准则的模糊权重 $\tilde{w}_i$ 为：

$$\tilde{w}_i=\frac{\sum_{j=1}^{n}\tilde{a}_{ij}}{\sum_{x=1}^{n}\sum_{y=1}^{n}\tilde{a}_{xy}}=\left(\frac{\sum_{j=1}^{n}a_{lij}}{\sum_{x=1}^{n}\sum_{y=1}^{n}a_{uxy}},\frac{\sum_{j=1}^{n}a_{mij}}{\sum_{x=1}^{n}\sum_{y=1}^{n}a_{mxy}},\frac{\sum_{j=1}^{n}a_{uij}}{\sum_{x=1}^{n}\sum_{y=1}^{n}a_{lxy}}\right),i=1,2,\cdots,n \tag{3}$$

步骤 3 建立可能度矩阵

设 $\tilde{a}=(a_l,a_m,a_u)$，$\tilde{b}=(b_l,b_m,b_u)$，则 $\tilde{a}\geqslant\tilde{b}$ 的可能度为：

$$p(\tilde{a}\geqslant\tilde{b})=\lambda\times\max\left\{1-\max\left\{\frac{b_m-a_l}{a_m-a_l+b_m-b_l},0\right\},0\right\}+(1-\lambda)\max\left\{1-\max\left\{\frac{b_u-a_m}{a_u-a_m+b_u-b_m},0\right\},0\right\} \tag{4}$$

其中，$a_i,b_i\in[0,1]$，$i=l,m,u$。通常 λ 取 0.5，表示决策者是风险中立的。计算 $p(\tilde{w}_i\geqslant\tilde{w}_j)$，$i,j=1,2,\cdots n$，记为 p_{ij}，并建立可能度矩阵 $\boldsymbol{P}=(p_{ij})_{n\times n}$。

步骤 4 各要素相对权重计算

先将可能度矩阵转化为模糊一致性矩阵，方法如下：

设 $r_i=\sum_{j=1}^{n}p_{ij}$，$i=1,2,\cdots n$，并计算 $r_{ij}=\frac{r_i-r_j}{2(n-1)}+0.5$，从而得到模糊一致判断矩阵 $\boldsymbol{R}=(r_{ij})_{n\times n}$，再计算

$$w_i=\frac{\sum_{j=1}^{n}r_{ij}+\frac{n}{2}-1}{n(n-1)},i=1,2,\cdots,n \tag{5}$$

w_i 就是我们需要的第 i 个要素在当前层次中的相对权重[25]。

5.2.6 原子攻击成功概率

由于漏洞可利用性、主机安防强度、漏洞时间可利用性和漏洞来源对原子攻击成功概率的重要程度不一致，因此要确定它们之间的相对权重。使用 Fuzzy-AHP 方法计算出漏洞可利用性、主机安防强度、漏洞时间可利用性和漏洞来源分别对应的相对权重 w_1，w_2，w_3，w_4。

对于 E_i 代表的原子攻击，其攻击成功概率计算公式为：

$$P(E_i)=VE_i^{\,1-w_1}\times(1-PS_i)^{1-w_2}\times TE_i^{\,1-w_3}\times VS_i^{\,1-w_4} \tag{6}$$

其中，VE_i，TE_i，VS_i 分别表示 E_i 所利用漏洞在漏洞可利用性、漏洞时间可利用性和漏洞来源 3 个维度的分值，PS_i 则表示 E_i 的目的节点所代表主机的安防强度。

5.2.7 条件概率

定义 1 $Par(S_j)$ 表示节点 S_j 的父节点集合，连接 S_j 和 $Par(S_j)$ 的有向边组成的集合为 $\{E_{i+1},E_{i+2},\cdots,E_{i+n}\}$。设 $T_k=\begin{cases}0, & Src(E_k)=0\\1, & Src(E_k)=1\end{cases}$，其中 $Src(E_k)$ 表示有向边 E_k 的源节点。$P(S_j=1|Par(S_j))$ 表示节点 S_j 的条件概率，是其在父节点影响下被攻击者占有的概率。根据 d_j 的不同，$P(S_j=1|Par(S_j))$ 有两种计算方式：

当 $d_j=$AND 时

$$P(S_j=1|Par(S_j))=\prod_{k=1}^{n}T_{i+k}P(E_{i+k}) \tag{7}$$

当 $d_j=$OR 时

$$P(S_j=1|Par(S_j))=1-\prod_{k=1}^{n}[1-T_{i+k}P(E_{i+k})] \tag{8}$$

5.2.8 先验可达概率

利用贝叶斯攻击图中各个节点的条件概率和原子攻击成功概率，可以计算出每个节点的可达概率，即先验可达概率，

用于评估网络资产的静态安全风险。

定义 2 设节点 S_j 共有 n 个祖先节点，记为 $\{S_{k+1}, S_{k+2}, \cdots, S_{k+n}\}$，则 S_j 的先验可达概率为：

$$P(S_j=1)=P(S_j=1|Par(S_j))\prod_{i=1}^{n}P(S_{k+i}|Par(S_{k+i})) \tag{9}$$

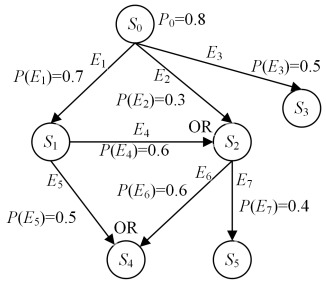


图 5 贝叶斯攻击图概率计算示例

Fig. 5 Probability calculation of Bayesian attack graph

以图 5 所示的贝叶斯攻击图为例，S_1，S_2，S_4 的先验可达概率计算过程如下：

$$P_1=P(S_1|S_0)P_0=0.7\times0.8=0.56$$

$$P_2=P(S_2|S_1,S_0)P(S_1|S_0)P_0+P(S_2|S_1=0,S_0)P(S_1=0|S_0)P_0$$
$$=(1-0.4\times0.7)\times0.7\times0.8+0.3\times0.3\times0.8$$
$$=0.4752$$

$$P_4=P(S_4|S_1=0,S_2)P(S_2|S_1=0,S_0)P(S_1=0|S_0)P_0+P(S_4|S_1,S_2=0)P(S_2=0|S_1,S_0)P(S_1|S_0)P_0+P(S_4|S_1,S_2)P(S_2|S_1,S_0)P(S_1|S_0)P_0$$
$$=0.6\times0.3\times0.3\times0.8+0.5\times0.7\times0.4\times0.7\times0.8+(1-0.5\times0.4)\times(1-0.7\times0.4)\times0.7\times0.8$$
$$=0.44416$$

5.2.9 后验可达概率

网络是一个动态的系统，攻击事件会影响条件节点的可达概率，为了体现网络资产的动态安全风险，需要根据发生的攻击事件来更新相关条件节点的可达概率。

定义 3 设节点 S_j 共有 n 个祖先节点，记为 $\{S_{k+1}, S_{k+2}, \cdots, S_{k+m}, \cdots, S_{k+n}\}$，则 S_j 被攻击者占有，即 $S_j=1$ 时 S_{k+m} 的后验可达概率为：

$$P(S_{k+m}=1|S_j=1)=\frac{P(S_j=1|S_{k+m}=1)P(S_{k+m}=1)}{P(S_j=1)}$$
$$=\frac{P(S_j=1|Par(S_j,S_{k+m}=1))P(S_{k+m}=1|Par(S_{k+m}))\cdot\prod_{i\in[1,n],i\neq m}P(S_{k+i}|Par(S_{k+i},S_{k+m}=1))}{P(S_j=1)} \tag{10}$$

其中，如果 S_{k+m} 是 S_j 的父节点之一，则 $Par(S_j,S_{k+m}=1)$ 表示将 S_{k+m} 的值确定为 1 时 S_j 的父节点集合；如果 S_{k+m} 不是 S_j 的父节点，则 $Par(S_j,S_{k+m}=1)=Par(S_j)$。

以图 5 所示的贝叶斯攻击图概率计算为例，S_4 被攻击者占有，即 $S_4=1$ 时，S_1 和 S_2 的后验可达概率的计算过程如下：

$$P(S_1|S_4)=\frac{P(S_4|S_1,S_2=0)P(S_2=0|S_1,S_0)P(S_1|S_0)P_0+P(S_4|S_1,S_2)P(S_2|S_1,S_0)P(S_1|S_0)P_0}{P(S_4)}$$
$$=\frac{0.5\times0.4\times0.7\times0.7\times0.8+(1-0.5\times0.4)\times(1-0.7\times0.4)\times0.7\times0.8}{0.44416}$$
$$\approx0.9027$$

$$P(S_2|S_4)=\frac{P(S_4|S_1=0,S_2)P(S_2|S_1=0,S_0)P(S_1=0|S_0)P_0+P(S_4|S_1,S_2)P(S_2|S_1,S_0)P(S_1|S_0)P_0}{P(S_4)}$$
$$=\frac{0.6\times0.3\times0.3\times0.8+(1-0.5\times0.4)\times(1-0.7\times0.4)\times0.7\times0.8}{0.44416}$$
$$\approx0.8235$$

5.3 贝叶斯攻击图风险分析方法

5.3.1 静态风险分析方法

根据上文所述计算原子攻击成功概率、条件概率和先验可达概率，可以在基本攻击图的基础上构建静态贝叶斯攻击图，构建算法如算法 1 所示。

算法 1 Static_BAG

输入：攻击图 AG=(S,E,R)，S_0 的先验可达概率 p 可以根据专家经验赋值

输出：静态贝叶斯攻击图 SBAG=(S,E,R,P)

1. 初始化 SBAG 的参数，将 AG 中的 S,E,R 复制到 SBAG 中
2. for SBAG 中任意有向边 E_i do
3. 计算 P(E_i)/ * 利用式(6) * /
4. SBAG.P_0←p
5. for i←1 to n do / * SBAG 中包含条件节点 S_i(i∈[0,n]) * /
6. 计算 P(S_i=1|Par(S_i))/ * 利用式(7)和式(8) * /
7. SBAG.Pi←P(S_i=1)/ * 利用式(9) * /
8. return SBAG=(S,E,R,P)

因为网络系统中的不同主机可能拥有相同的漏洞，所以攻击者在综合利用多个漏洞对目标网络进行逐步攻击的过程中，可能会重复利用不同主机上的相同漏洞。而一旦攻击者成功利用某个漏洞实现了攻击，那在接下来对其他主机进行攻击的过程中，如果该主机也有该漏洞，则攻击者再次成功利用该漏洞实现攻击的可能性将大大提高。并且此时的原子攻击成功概率将不再受漏洞可利用性、漏洞时间可利用性和漏洞来源这 3 个维度的影响，但会受到前后两台主机间安防强度差别的影响。

因此，如果某个原子攻击需要利用的漏洞在其所在攻击路径中已经被利用过，那么其成功的概率需要修正，计算方法如下：

定义 4 设 E_i 是 S_j 的出边，E_k，E_{k+1}，…，E_{k+n} 是 S_l 的入边，其中 E_k，E_{k+1}，…，E_{k+m} 和 E_i 利用的是同一个漏洞，并且 S_l 是 S_j 的祖先节点，则

$$P(E_i)=P(S_i=1|S_j=1)\cdot\frac{\sum_{x=k}^{k+m}P(E_x)P(Src(E_x)=1)}{\sum_{y=k}^{k+n}P(E_y)P(Src(E_y)=1)}\cdot \min\left(\frac{PS_k}{PS_i},1\right) \tag{11}$$

其中，$P(S_i=1|S_j=1)$的计算方法见式(10)。

所以，得到静态贝叶斯攻击图后，可以根据式(11)对所有需要的原子攻击成功概率进行修正，然后利用式(9)再次计算相应节点的先验可达概率，这样就得到了改进静态贝叶斯攻击图。它的原子攻击成功概率和条件节点先验可达概率更加准确，可以用来评估网络资产的静态安全风险。

5.3.2 *动态风险分析方法*

攻击事件发生时，我们可以根据实际情况，利用算法 2，更新基于经验知识的先验可达概率，得到后验可达概率，从而将改进静态贝叶斯攻击图转化为动态贝叶斯攻击图，用于对网络资产动态安全风险的评估。

算法 2 中包括 3 种对先验可达概率的更新方法。

第一种是正向更新，即更新被攻击节点的后续节点的可达概率。因为在一条攻击路径中，如果某一节点已被攻击者占有，那么后续节点被攻击的可能性将显著增加，因此正向更新有助于防范和阻止攻击者的进一步行动。

第二种是反向更新，即更新被攻击节点的前驱节点的可达概率。因为它们是根据经验知识生成的，依据攻击事件对其进行更新有助于网络管理员重新审视和评估各个节点的安全风险，及时调整安防措施和优先级。

第三种是正反向融合更新，即在反向更新时，如果前驱节点存在其他子节点，则该子节点的可达概率也会按照式(9)进行更新。并且，算法 2 可以保证在更新被攻击节点的后续节点 S_i 的可达概率时，S_i 祖先节点的可达概率都已更新完毕。以图 5 为例，如果检测到 S_1 节点被攻击，算法 2 会按照 S_2，S_3，S_4，S_5 的顺序执行语句(23)，而文献[20]中的方法则是依次对 S_4，S_2，S_5 执行相应操作。

算法 2 Dynamic_BAG

输入：ISBAG=(S,E,R,P)；被攻击节点 S_j

输出：动态贝叶斯攻击图 DBAG=(S,E,R,P)

```
1. 初始化 DBAG 的参数，将 ISBAG 中的 S,E,R,P 复制到 DBAG 中
2. 创建 3 个空数组 Φ,Ω,ζ
3. DBAG.P_j←1
4. Φ.append(S_j)/*将 S_j 加入 Φ 末尾*/
5. for k←0 to length(Φ) do
6.     for Φ[k]的每个父节点 S_i do
7.         if S_i∉Φ
8.             Φ.append(S_i)
9.             DBAG.P_i←P(S_i=1|S_j=1)/*式(10)*/
10.    for Φ[k]的每个子节点 S_i do
11.        if S_i∉Φ
12.            Ω.append(S_i)
13. for k←0 to length(Ω) do
14.    for Ω[k]的每个子节点 S_i do
15.        Ω.append(S_i)
16. for k←length(Ω)−1 to 0 do
17.    if Ω[k]∉ζ
18.        ζ.append(Ω[k])
19. for k←length(ζ)−1 to 0 do
20.    n←ζ[k].index/*若 Ω[k]是 S_i 则 n=i*/
21.    DBAG.P_n←P(S_n=1)/*利用式(9)*/
22. return DBAG=(S,E,R,P)
```

6 实验分析

6.1 实验建立

为了验证本文方法的有效性，本文基于网络靶场系统搭建了基础网络拓扑结构，如图 6 所示。

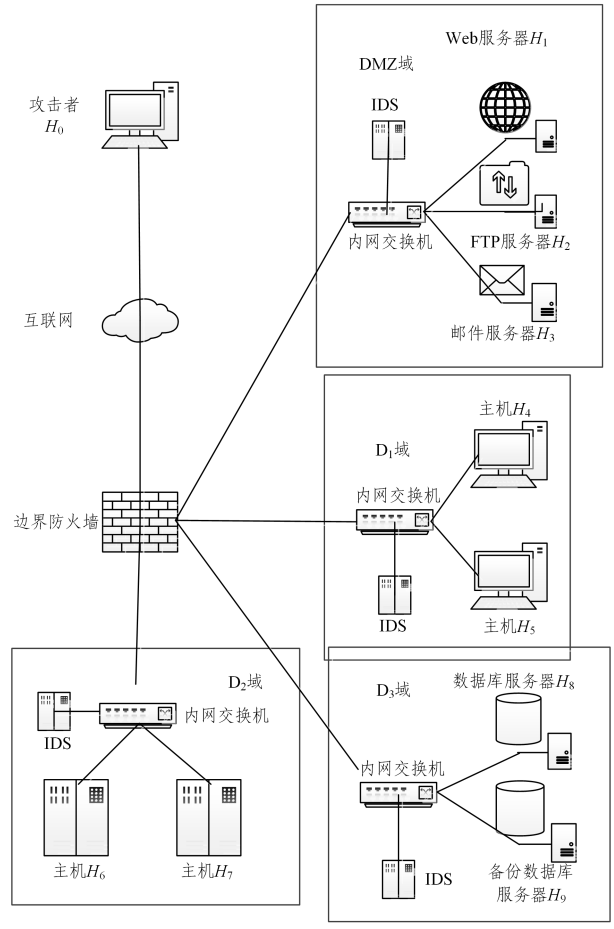


图 6 实验网络拓扑图

Fig. 6 Network topology

该靶场系统的硬件承载环境配置为 Intel Xeon Gold 5218(16 核 2.3 GHz)处理器 * 2 和 32GB 3200 MHz DDR4 内存 * 6 等。参照图 6，其中主机 H_4，H_5 使用 Win10 操作系统，其余主机使用 CentOS7 操作系统；DMZ 域用于对外提供 Web 服务(Nginx)、FTP 服务(zFTPServer)和邮件服务(Apache Commons Mail)；D_1 域是企业的内部办公网络，D_2 域是企业的系统业务区，D_3 域是数据存储区(PostgreSQL)。本文通过安装防火墙划分网络区域，并制定子网间通信规则，从而保证外部访问无法到达内网区域即 D_1，D_2，D_3 域。具体访问规则如下：

(1)允许 H_4 访问 H_8，从而管理数据库。

(2)允许 H_6 访问 H_8，从而对系统业务数据增删改查。

(3)允许 H_4 和 DMZ 域中的主机相互访问，从而管理 DMZ 域中的服务。

(4)允许 H_6 和 DMZ 域中的主机相互访问，因为 DMZ 域中的服务和系统业务有关。

(5)允许 H_4 访问 H_6，从而管理系统业务。

(6)域内主机可以相互访问,禁止除了上述规则外的跨域访问。

网络中各主机间的连通关系如表4所列,—表示未连通。

表4 各主机间网络连通关系

Table 4 Network connectivity between hosts

主机	H_0	H_1	H_2	H_3	H_4	H_5	H_6	H_7	H_8	H_9
H_0	—	连通	连通	连通	—	—	—	—	—	—
H_1	—	—	连通	连通	连通	—	连通	—	—	—
H_2	—	连通	—	连通	连通	—	连通	—	—	—
H_3	—	连通	连通	—	连通	—	连通	—	—	—
H_4	—	连通	连通	连通	—	连通	连通	—	连通	—
H_5	—	—	—	—	连通	—	—	—	—	—
H_6	—	连通	连通	连通	—	—	—	连通	连通	—
H_7	—	—	—	—	—	—	连通	—	—	—
H_8	—	—	—	—	—	—	—	—	—	连通
H_9	—	—	—	—	—	—	—	—	连通	—

6.2 攻击图生成

利用Nessus对实验网络进行漏洞扫描,获取到各主机上的漏洞信息,并结合美国国家漏洞数据库(National Vulnerability Database,NVD)[26]提供的信息,得到主机漏洞信息,如表5所列。其中AC和UI分别表示该漏洞的CVSS评分中攻击复杂度和用户交互两个维度的得分。

表5 主机漏洞信息

Table 5 Hosts vulnerability information

主机	CVE ID	漏洞所属软件	漏洞编号	AC	UI
H_1	CVE-2020-5864	Nginx	V1	H	N
H_1	CVE-2018-8059	Nginx	V2	L	N
H_2	CVE-2020-11706	zFTPServer	V3	L	R
H_3	CVE-2021-44549	Apache Commons Mail	V4	H	N
H_4	CVE-2016-0019	Win10 RDP Service	V5	H	N
H_5	CVE-2020-16898	Win TCP/IP stack	V6	L	N
H_6	CVE-2019-11815	Linux kernel	V7	H	N
H_7	CVE-2017-1000080	Linux kernel	V8	L	N
H_7	CVE-2022-23222	Linux kernel	V9	L	N
H_8	CVE-2016-2193	PostgreSQL	V10	L	N
H_8	CVE-2017-7547	PostgreSQL	V11	L	N
H_9	CVE-2016-2193	PostgreSQL	V12	L	N
H_9	CVE-2017-7547	PostgreSQL	V13	L	N

利用主机间连通关系、漏洞信息、漏洞间关系和网络配置等数据生成攻击图,如图7所示。其中节点代表实验网络中主机的权限;有向边既表示节点间的因果关系,也表示原子攻击。对于拥有多条入边的任意节点S_j,d_j=OR。

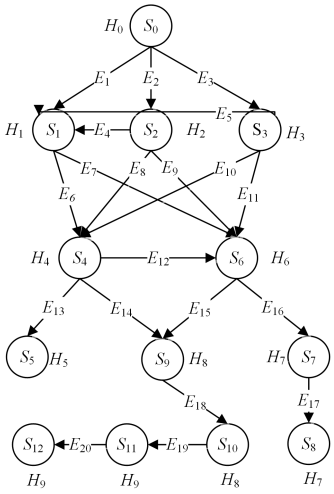


图7 实验网络的攻击图

Fig. 7 Attack graph of experimental network

6.3 静态风险分析

首先,利用Fuzzy-AHP方法对漏洞可利用性、主机安防强度、漏洞时间可利用性和漏洞来源关于原子攻击成功概率的相对重要性进行赋权。将它们进行两两比较,根据专家评分,构建模糊互补判断矩阵,如表6所列。再根据式(3)—式(5)进行计算,得到漏洞可利用性、主机安防强度、漏洞时间可利用性和漏洞来源的相对权重分别为0.315,0.296,0.179,0.21。

表6 Fuzzy-AHP模糊互补判断矩阵

Table 6 Fuzzy complementary judgment matrix of Fuzzy-AHP

	VE	PS	TE	VS
VE	(0.5,0.5,0.5)	(0.4,0.6,0.8)	(0.8,0.9,0.9)	(0.7,0.8,0.9)
PS	(0.2,0.4,0.6)	(0.5,0.5,0.5)	(0.7,0.8,0.9)	(0.7,0.8,0.9)
TE	(0.1,0.1,0.2)	(0.1,0.2,0.3)	(0.5,0.5,0.5)	(0.3,0.4,0.5)
VS	(0.1,0.2,0.3)	(0.1,0.2,0.3)	(0.5,0.6,0.7)	(0.5,0.5,0.5)

然后,使用上述算法1构建静态贝叶斯攻击图,其中包含对原子攻击成功概率和条件节点先验可达概率的计算。

计算各个攻击的成功概率时,首先根据相应漏洞信息,利用式(1)和式(2)分别计算漏洞可利用性和漏洞时间可利用性。再将它们和主机安防强度、漏洞来源的专家评分一起带入式(6),计算得到各个原子攻击成功概率,结果如表7所列。

表7 原子攻击成功概率

Table 7 Successful probabilities of atomic attacks

原子攻击	成功概率	原子攻击	成功概率
E_1	0.356	E_{11}	0.287
E_2	0.215	E_{12}	0.287
E_3	0.181	E_{13}	0.579
E_4	0.523	E_{14}	0.346
E_5	0.523	E_{15}	0.346
E_6	0.364	E_{16}	0.421
E_7	0.287	E_{17}	0.418
E_8	0.364	E_{18}	0.346
E_9	0.287	E_{19}	0.346
E_{10}	0.364	E_{20}	0.346

再利用式(9)计算各个节点的先验可达概率,对实验网络进行静态安全风险评估,结果如表8所列。其中,S_1的先验可达概率最高,说明主机H_1被入侵的风险最大,应当优先采取更新补丁等安防措施。

表8 条件节点先验可达概率

Table 8 Prior reachable probabilities of conditional nodes

条件节点	先验可达概率	条件节点	先验可达概率
S_1	0.482	S_7	0.115
S_2	0.215	S_8	0.048
S_3	0.181	S_9	0.171
S_4	0.278	S_{10}	0.059
S_5	0.161	S_{11}	0.02
S_6	0.273	S_{12}	0.007

因为E_{19}利用的漏洞和E_{17}相同,E_{20}利用的漏洞和E_{18}相同,即存在漏洞重复利用的情况,所以E_{19}和E_{20}的原子攻击成功概率要用式(11)重新计算。根据攻击图中的依赖关系和攻击路径,E_{19}和E_{20}这两次攻击发生时其对应漏洞都已经被成功利用过,前后的主机安防强度也相同,所以计算结果都为

1，相应的 S_{11} 和 S_{12} 的先验可达概率都应修正为 0.059，得到改进静态贝叶斯攻击图。可以看出，修正前 S_{11} 和 S_{12} 的可达概率显著小于 S_{10}，容易误导网络管理员，让其认为 S_{11} 和 S_{12} 被入侵风险远小于 S_{10}，但事实上这三者的风险程度是相近的。因此，利用攻击图中漏洞的重复利用情况来对静态贝叶斯攻击图进改进，可以对网络资产的安全风险进行更加准确的评估，为网络管理员的决策提供参考。

6.4 动态风险分析

根据安防系统提供的情报，主机 H_8 上的 CVE-2016-2193 漏洞已被成功利用，即攻击图中的节点 S_9 已被攻击者占有。根据这一信息，可以使用算法 2 构建动态贝叶斯攻击图，评估当前的动态安全风险。其中包含对条件节点可达概率的更新计算，结果如图 8 所示。

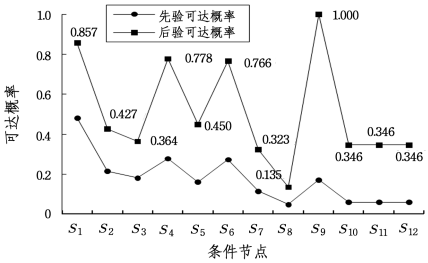


图 8 条件节点可达概率

Fig. 8 Reachable probabilities of conditional nodes

可以看出，S_9 节点发生攻击事件后，实验网络中各个节点的可达概率都呈现上升的趋势，说明网络整体的安全风险正在升高。其中 S_1，S_4，S_6 的后验可达概率显著高于其他节点，说明它们此时很有可能已被攻击，需要尽快采取补救措施。而 S_{10}，S_{11}，S_{12} 的后验可达概率相较于先验可达概率有大幅提升，说明它们接下来很有可能会被攻击。所以，在真实的网络环境中，动态安全风险评估的准确性明显高于静态安全风险评估，可以为网络风险管理提供有效支撑。

6.5 方法对比

攻击图中各条件节点的可达概率是对网络安全风险进行评估的主要指标，为了验证本文模型的优越性，我们在相同的网络环境下，将文献[19]和文献[20]方法与本文方法的实验数据进行对比。

图 9 展示了同样在图 6 所示网络环境中，3 种方法给出的条件节点先验可达概率。文献[19]和文献[20]方法也是利用贝叶斯网络描述攻击行为的因果关系，但是它们对原子攻击成功概率的评估指标过于单一，导致给出的原子攻击成功概率和可达概率不能真实地反映网络资产安全风险。而本文方法从多个维度评估原子攻击成功概率，能更好地反映网络资产安全风险。并且，文献[19]和文献[20]方法都没有考虑漏洞重复利用的情况，所以，我们认为 S_{11} 和 S_{12} 的风险显著小于 S_{10}，但事实上三者的风险是相近的。在 S_{10}，S_{11} 和 S_{12} 先验可达概率接近的情况下，本文方法的先验可达概率标准差依然大于文献[19]和文献[20]方法，分别是 0.121，0.113 和 0.102。这说明本文方法对各节点安全风险的区分度更大，有利于区别并划分各节点的安全等级。

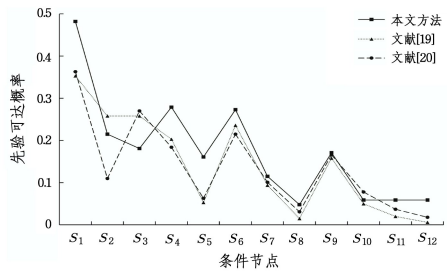


图 9 先验可达概率比较

Fig. 9 Comparison of priori reachable probabilities

图 10 展示了 3 种方法在发生攻击事件时的条件节点后验可达概率。文献[19]和文献[20]方法没有将反向更新和正向更新相融合，在反向更新时只考虑被攻击节点的祖先节点。如图 10 所示，S_9 被攻击时它们会更新 S_4 和 S_6 的可达概率，但却忽略了 S_5，S_7 和 S_8，给出的结果明显低于本文方法，低估了真实安全风险。

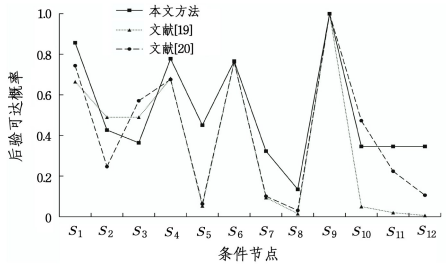


图 10 后验可达概率比较

Fig. 10 Comparison of posterior achievable probabilities

本文在漏洞可利用性、主机安防强度、漏洞时间可利用性、漏洞来源、漏洞重复利用、正向更新、反向更新和正反向融合更新等方面与文献[19]、文献[20]进行了对比，结果如表 9 所列。

表 9 对比分析

Table 9 Contrastive analysis

文献	漏洞可利用性	主机安防强度	漏洞时间可利用性	漏洞来源	漏洞重复利用	正向更新	反向更新	正反向融合更新
[19]	√	×	×	×	×	×	√	×
[20]	√	×	×	×	×	√	√	×
本文	√	√	√	√	√	√	√	√

结束语 为了评估网络资产安全风险，本文提出了一种基于贝叶斯攻击图的网络资产安全评估模型。首先综合分析漏洞可利用性、主机安防强度、漏洞时间可利用性和漏洞来源 4 个维度，并使用 Fuzzy-AHP 方法进行赋权，计算原子攻击成功概率，再结合贝叶斯网络计算节点的先验可达概率。然后根据漏洞的重复利用情况，对部分原子攻击成功概率和相应的先验可达概率进行修正，作为对网络资产静态安全风险的评估。最后根据检测到的实时攻击事件，利用提出的 Dynamic_BAG 算法动态更新受影响节点的可达概率。所提模型既有助于防范和阻止攻击者的进一步行动，也可以校正被攻击节点前驱节点根据经验知识生成的可达概率，实现对网络资产安全风险的动态评估。未来，可以进一步考虑攻击者和网络管理员之间的博弈，分析双方的成本与收益，为网络

管理员提供合理的安全加固策略。

参 考 文 献

[1] ZHAO C, WANG H Q, LIN J Y, et al. Attack Graph Analysis Method for Large Scale Network Security Hardening [J]. Journal of Frontiers of Computer Science and Technology, 2018, 12(2): 263-273.

[2] PHILLIPS C, SWILER L P. A graph-based system for network vulnerability analysis[C]// 1998 Workshop on New Security Paradigms. New York: ACM Press, 1998: 71-79.

[3] AL-MOHANNADI H, MIRZA Q, NAMANYA A, et al. Cyber-Attack Modeling Analysis Techniques: An Overview[C]// 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops. Vienna: IEEE, 2016: 69-76.

[4] YE Z W, GUO Y B, WANG C D, et al. Survey on application of attack graph technology [J]. Journal on Communications, 2017, 38(11): 121-132.

[5] ZHANG J, WANG J D, ZHANG H W, et al. Network Risk Analysis Method Based on Node-Game Vulnerability Attack Graph[J]. Computer Science, 2014, 41(9): 169-173.

[6] HU H, LIU Y L, ZHANG Y C, et al. Survey of attack graph based network security metric [J]. Chinese Journal of Network and Information Security, 2018, 4(9): 1-16.

[7] PEARL J. Probabilistic reasoning in intelligent system[M]// Morgan Kaufinann: Network of Plausible Inference. 1988: 1-86.

[8] WU C S, XIE W Q, JI Y X, et al. Survey on network system security metrics [J]. Journal on Communications, 2019, 40(6): 14-31.

[9] WANG L, ISLAM T, LONG T, et al. An attack graph-based probabilistic security metric[C]// 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security. London: IFIP, 2008: 283-296.

[10] FIRST. Common Vulnerability Scoring System version 3.1 Specification Document Revision 1 [EB/OL]. https://www.first.org/cvss/v3.1/specification-document.

[11] XIE P, LI J H, OU X M, et al. Using Bayesian networks for cyber security analysis[C]// 2010 IEEE/IFIP International Conference on Dependable Systems & Networks. Chicago: IEEE, 2010: 211-220.

[12] WANG J X, FENG Y, YOU R. Network security measurment based on dependency relationship graph and common vulnerability scoring system[J]. Journal of Computer Applications, 2019, 39(6): 1719-1727.

[13] HU W, ZHANG L, LIU X, et al. Research on Automatic Generation and Analysis Technology of Network Attack Graph[C]// 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). Baltimore: IEEE, 2020: 133-139.

[14] YANG H Y, YUAN H H, ZHANG L. Host security assessment method based on attack graph [J]. Journal on Communications, 2022, 43(2): 89-99.

[15] CHEN X J, FANG B X, TAN Q F, et al. Inferring Attack Intent of Malicious Insider Based on Probabilistic Attack Graph Model [J]. Chinese Journal of Computer, 2014, 37(1): 62-72.

[16] WANG Z G, LU Y, LI J D. Network Security Risk Assessment Method Based on Bayesian Attack Graph[J]. Journal of Academy of Armored Force Engineering, 2018, 32(3): 81-86.

[17] YANG Y J, LENG Q, PAN R X, et al. Research on Dynamic Threat Tracking and Quantitative Analysis Technology Based on Attribute Attack Graph [J]. Journal of Electronics & Information Technology, 2019, 41(9): 2172-2179.

[18] LUO Z Y, YANG X, LIU J H, et al. Network intrusion intention analysis model based on Bayesian attack graph [J]. Journal on Communications, 2020, 41(9): 160-169.

[19] GAO N, GAO L, HE Y Y, et al. Dynamic SecurityRisk Assessment Model Based on Bayesian Attack Graph [J]. Journal of Sichuan University (Engineering Science Edition), 2016, 48(1): 111-118.

[20] LI J R, LING X B, LI C X, et al. Dynamic Network Security Analysis Based on Bayesian Attack Graph [J]. Computer Science, 2022, 49(3): 62-69.

[21] GE H H. Research on Multidimensional and Dynamic Information Security Risk Management Model and the Related Assessment Algorithms[D]. Beijing: Beijing University of Posts and Telecommunications, 2015.

[22] FREI S, MAY M, FIEDLER U, et al. Large-scale vulnerability analysis[C]// Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense (LSAD'06). New York: ACM Press, 2006: 131-138.

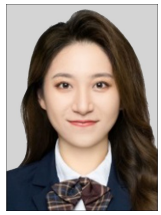
[23] PENG T R, LIU H P, LIU Y, et al. Target Weight Calculation Method Based on FAHP Method and Image Contrast Damage Evaluation Method[J]. Acta Armamentarii, 2021, 42(S1): 173-180.

[24] WANG W X, SUN Z, PAN M Y, et al. Information Security Risk Assessment Method for Electric Vehicle Charging Piles Based on Fuzzy Analytic Hierarchy Process [J]. Electric Power, 2021, 54(1): 96-103.

[25] PAN H W. Research on Information Security Risk Assessment Based on Fuzzy Analytic Hierarchy Process[D]. Nanjing: Nanjing Normal University, 2007.

[26] NIST. National vulnerability database[DB/OL]. https://nvd.nist.gov.

ZENG Kunlun, born in 1998, postgraduate. His main research interest is network security assessment.



LI Weihao, born in 1990, Ph. D. Her main research interests include social network security, privacy preservation, cloud computing and network security assessment.

(责任编辑:何杨)