攻击技战术双层关联建模的个性化风险评估方法

仇 晶[1*],农李晨[1],孙一飞[1],操晓春[2],陈玺名[1],张睿智[1]
(1. 广州大学网络空间安全学院,广东广州 510006;2. 中山大学网络空间安全学院,广东深圳 519082)

摘 要: 以MITRE ATT&CK框架为指导,通过刻画攻击者的战术目标与技术手段,利用攻击图进行网络安全风险建模与评估,已成为当前应对复杂多步攻击威胁的重要手段之一。然而,随着攻击场景和攻击链条日益复杂,现有基于ATT&CK的攻击路径建模与风险评估方法仍存在一定局限性。一方面,现有攻击路径建模过程仅考虑ATT&CK框架中攻击技术间的直接转移关系,忽略了战术层面的攻击语义,削弱了对复杂多阶段攻击路径的高层次语义约束能力。另一方面,依赖通用漏洞特征的攻击图风险量化评估方法,忽略了不同组织对关键资产的关注差异,导致评估结果缺乏资产个性化适配。针对上述挑战,本文提出攻击技战术双层关联建模的个性化风险评估方法。首先,通过构建技战术双层关联模型对技战术间潜在关系建模,结合维特比算法求解攻击战术阶段演变路径,在路径推理过程中引入战术层面的阶段约束。随后,构建融合攻击行为属性与资产个性化的定制化威胁量化模型,通过前向算法将状态转移概率与威胁量化指标耦合,实现对网络整体安全风险评估。实验结果表明,所提出的方法在实际网络环境中,路径建模与风险评估能力均优于其他现有主流评估模型,其综合风险评估准确率相较对比方法平均提升48.95%,验证了该方法在复杂攻击场景下的有效性与实用价值。

关键词: 网络安全;逻辑攻击图;风险评估;隐马尔可夫模型;ATT&CK框架;风险路径识别

基金项目: 国家自然科学基金(No.U24A20336);国家科技重大专项(No.2022ZD0119602);广州市科技计划项(No.2024A03J0399);鹏程实验室重大重点项目(No.PCL2024A05)

中图分类号: TN915.08 **文献标识码:** A **文章编号:** 0372-2112(2026)01-0001-18

电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20250681

A Personalized Risk Assessment Approach for Two-Layer Association Modeling of Attack Techniques and Tactics

QIU Jing[1*], NONG Lichen[1], SUN Yifei[1], CAO Xiaochun[2], CHEN Ximing[1], ZHANG Ruizhi[1]
(1. *Cyberspace Institute of Advanced Technology*, *Guangzhou University*, *Guangzhou*, *Guangdong* 510006, *China*;
2. *Cyberspace Institute of Advanced Technology*, *Sun Yat-sen University*, *Shenzhen*, *Guangdong* 519082, *China*)

Abstract: Guided by the MITRE ATT&CK framework, modeling and assessing cybersecurity risks by modeling attackers' tactical objectives and technical methods through attack graphs have become one of the key approaches to countering complex multi-step attack threats. However, as attack scenarios and attack chains grow increasingly intricate, existing ATT&CK-based attack path modeling and risk assessment methods exhibit certain limitations. On the one hand, current attack path modeling processes only consider direct transition relationships between attack techniques within the ATT&CK framework, overlooking tactical-level attack semantics and weakening the ability to impose high-level semantic constraints on complex multi-stage attack paths. On the other hand, attack graph-based risk quantification methods relying on generic vulnerability characteristics overlook differences in organizational focus on critical assets, resulting in assessment outcomes that lack personalized asset adaptation.To address these challenges, this paper proposes a personalized risk assessment method based on dual-layer association modeling of attack techniques and tactics. First, a dual-layer association model is constructed to capture potential relationships between techniques and tactics. Combined with the Viterbi algorithm, this model infers the evolution paths of attack tactics, introducing tactical-level stage constraints during path inference. Subsequently, a customized threat quantification model is developed by integrating attack behavior attributes with asset-specific characteristics. Through a forward algorithm, state transition probabilities are coupled with threat quantification metrics to achieve holistic network security risk assessment. Experimental results demonstrate that the proposed method outperforms existing mainstream assessment models in both path modeling and risk evaluation capabilities in real-world network environments. Compared with competing approaches, the proposed method achieves an average improvement of 48.95% in comprehensive risk assessment accuracy, validating its effectiveness and practical value in complex attack scenarios.

收稿日期:2025-08-04;录用日期:2026-01-07;责任编辑:覃怀银
*通信作者:仇晶

Keywords: cybersecurity; logical attack diagram; risk assessment; hidden Markov model; ATT&CK framework; risk path identification

Foundation Item(s): National Natural Science Foundation of China (No.U24A20336); National Science and Technology Major Project of China (No.2022ZD0119602); Guangzhou Science and Technology Program (No.2024A03J0399); Major Key Project of Pengcheng Laboratory (No.PCL2024A05)

0 引言

最近几年,全球网络安全态势呈现出攻击链条复杂化与攻击策略高度针对性的双重趋势,网络攻击的多阶段性与隐蔽性显著增强。数据显示,超过74%的数据泄露事件涉及外部攻击者,其中约67%的攻击路径包含多阶段渗透行为[1]。多阶段攻击通过社会工程、横向移动、权限提升等手段,在多个节点之间实现跳跃式推进,严重削弱了传统纵深防御机制的有效性[2]。如2024年深信服在服务器端拦截的恶意程序数量高达153.16亿次,这类高级持续性威胁(Advanced Persistent Threat,APT)正通过多阶段、隐蔽性强的攻击手段突破传统安全防线,给企业和社会带来严峻挑战[3]。在此背景下,安全检测系统面临攻击归因困难、数据缺失、误报率高等共性问题[4-5],尤其是在日志跨度大、上下文缺失和攻击行为难以溯源的情况下[6],需要结合威胁报告中的结构化知识提取以增强安全画像与关联分析能力[7],对威胁建模的完整性和风险评估的准确性提出了更高要求。

攻击图是一种广泛用于建模网络中潜在攻击路径的方法,应用于漏洞分析、风险评估等多个领域[8]。随着网络环境日益复杂化,该方法在建模粒度、表达能力与推理效率方面面临诸多挑战。为此,研究者提出以MulVAL框架[9]为典型代表的逻辑攻击图模型,其利用逻辑推理机制整合网络拓扑结构、漏洞信息、权限配置等多维度数据构建多阶段攻击路径。近年来,相关研究持续围绕攻击图的建模规模与分析效率展开优化[10-11],借助复杂网络建模方法,如节点多阶邻域特征与结构位置耦合机制[12],以提升攻击图中关键节点识别与风险传播分析的精度。在此基础上,如何基于逻辑攻击图对潜在威胁进行有效评估,已成为提升安全态势感知与风险管理水平的关键方向[13-14]。

目前,在基于逻辑攻击图的网络安全风险评估领域,研究主要集中于两个方向:一类是研究聚焦攻击图中攻击路径的建模与分析,通过攻击行为之间的先后关系与传播链条,用模型识别并构建攻击图中的多阶段攻击过程[15-16];另一类是研究尝试将攻击图中攻击行为节点风险量化,借助通用漏洞评分系统(Common Vulnerability Scoring System,CVSS)[17]对攻击行为进行标准化评估[18-19]。在真实网络安全运营中,基于逻辑攻击图的风险评估不仅服务于资源受限条件下的防护优先级决策,也可为攻防演练的攻击过程刻画与网络保险等场景的风险分级与定价提供量化支撑。然而,当前研究在实际应用中仍面临两个关键挑战:(1)攻击行为高层次语义建模不足;(2)攻击路径风险评估缺乏实际资产适配性。

针对挑战(1)攻击行为高层次语义建模不足问题,现有研究在建模攻击行为的风险传导准确性受限。例如,图1以公开披露的APT32入侵事件为例,展示了攻击技术序列及其在战术语义层面的映射过程。攻击者通过钓鱼技术获取初始入口,执行恶意代码建立持久化机制,之后获取凭据并实施横向移动,最终完成目标数据的收集与外传。其中,攻击技术T1543在ATT&CK框架中同时关联持久化与权限提升两类战术,若仅基于技术层进行建模,容易忽略其在具体攻击上下文中的阶段语义差异,导致战术归属不明确,从而在概率建模过程中因技术转移概率被稀释或低估,进而影响对整条攻击路径风险的评估准确性。

针对挑战(2)攻击路径风险评估缺乏实际资产适配性问题,现有方法多基于攻击行为的显性特征进行评估,未能体现不同组织对不同资产的个性化优先级。在建模过程中,尽管已有研究引入机密性、完整性、可用性和攻击路径长度等威胁指标以提升建模精度,但这些方法普遍忽视了资产个性化偏好及其在路径演化过程中的动态风险影响。此外,路径状态变化中的概率性因素未被有效融合,导致评估结果在实际攻击场景中的适应性受限。

针对上述问题,本文基于MITRE ATT&CK(Adversarial Tactics,Techniques,and Common Knowledge)框架[20],引入技战术双层关联建模,将攻击技术视为可观测行为,攻击战术视为不可直接观测的高层意图状态,通过条件概率建模刻画攻击技术在不同战术阶段下出现的概率分布,状态转移概率描述战术阶段之间的演化关系,从而在攻击路径推理过程中引入战术层面的语义约束。引入资产个性化权重对攻击技术风险进行调节,通过对不同资产在数据价值、业务关键性及系统架构特性等方面的差异化建模,风险评估结果能够更加贴近真实攻击场景下防御者的关注重点,并为关键资产识别与防御优先级决策提供有效支持。

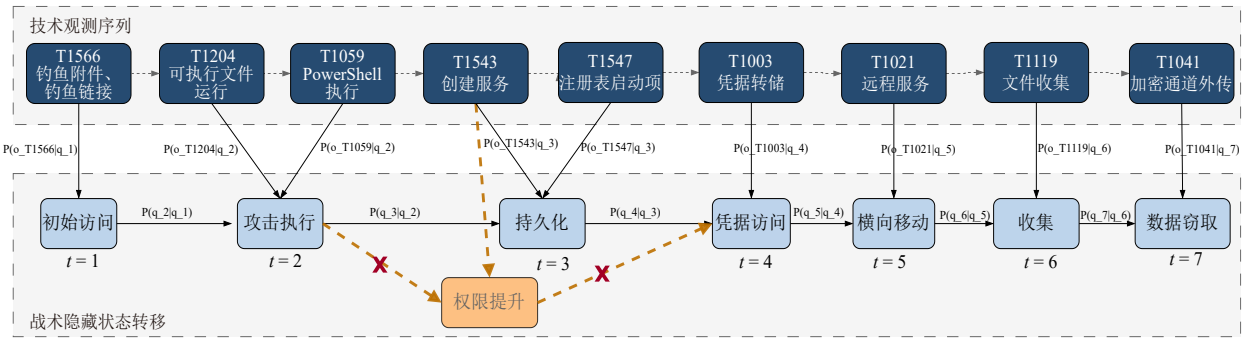

图 1　基于具体攻击技术序列的 HMM 推理示例图

Figure 1　Example diagram of HMM inference based on specific attack sequences

本文的主要贡献概括如下：

(1)本文提出一种基于隐马尔可夫模型(Hidden Markov Model，HMM)的攻击路径建模方法，将攻击技战术间的多对一转移关系建模为隐藏状态与观测状态结构，并基于战术状态转移与观测概率推断攻击行为的阶段演化特征。

(2)本文提出一种融合攻击行为属性与路径演化概率的综合风险评估方法，引入攻击行为与资产的映射关系，构建面向组织自身风险偏好的定制化威胁评估模型，将其与前向算法耦合，实现对攻击路径的风险评估。

(3)将所提出的方法部署于不同复杂度的内网环境中，并通过实验验证其在路径建模与风险评估方面的有效性。实验结果表明，该方法在路径建模、动态风险感知方面表现优异，能有效反映攻击者可能采取的攻击路径。

1　相关工作

1.1　逻辑攻击图

逻辑攻击图将网络中的资产、漏洞、权限等要素抽象为节点，并用有向边表示攻击者利用漏洞从一个节点转移到另一个节点的过程。这种结构化表示方法能够直观展示攻击者如何从初始状态逐步推进，最终推理出攻击目标的所有可能路径。

如表 1 所示，逻辑攻击图作为网络安全风险分析的核心工具，在技术演进历程中，Swiler 等人[21]率先开发自动化生成工具，通过融合攻击模板、网络配置与攻击者能力信息构建攻击图，优化冗余结构，为工程化应用奠定基础。针对逻辑攻击图的特性，Zenitani 等人[22]全面梳理了攻击图分析的理论与实践体系，提出 AND-OR 节点攻击图，构建起完备的知识框架。Ou 等人[9]提出的 MulVAL 框架采用声明式逻辑编程语言(datalog)描述漏洞传播规则，结合网络配置生成攻击图，开启了逻辑攻击图的自动化建模研究路径。其后，多项研究在此基础上进行了优化。Jing 等人[23]提出从通用漏洞披露(Common Vulnerabilities and Exposures，CVE)描述中自动提取信息生成交互规则的方法，以此优化 MulVAL 攻击图的生成过程。此外，Tayouri 等人[24]对 MulVAL 的扩展进行了全面调研，不仅收集了新的交互规则，还将其映射到 MITRE ATT&CK 技术框架，评估其对各类攻击场景的覆盖能力。

表 1　攻击图构建工具对比

Table 1　Comparison of attack graph construction tools

相关研究	构图方式	主要输入	版本
文献[21]	模板驱动、基于攻击步骤枚举	漏洞表、网络拓扑	无公开版本
文献[22]	AND-OR 逻辑攻击图	漏洞知识库、攻击逻辑	概念模型
文献[9]	AND-OR-LEAF 逻辑攻击图	CVE/配置/主机关系	MulVAL1.2.1(默认 Datalog 规则)
文献[24]	增强规则库、引入 ATT&CK 映射	CVE/ATT&CK/配置	兼容 MulVAL

尽管上述研究在构建逻辑攻击图和优化 MulVAL 攻击图评估方面取得了显著进展，但这些改进方案依旧采用 MulVAL 攻击图传统的三种节点类型划分方式，未能突破固有攻击图结构。虽然部分研究实现了与 ATT&CK 技术的关联映射，但研究视角仍以规则整合与场景覆盖为主，缺乏对攻击行为演变逻辑的系统性剖析。因此，本文需要一种新的构图范式，聚焦于攻击行为的潜在转移机制，深入解析其演变规律。

1.2　针对攻击行为的量化指标

在网络安全评估领域，诸多研究围绕攻击行为的全生命周期特征、多维度量化指标和动态演化规律等展开，形成了多层次的评估体系构建思路。

早期研究中，为了实现网络安全评估从经验判断向结构化评估的转变，Gao 等人[25]提出从攻击影响角

度出发，利用保密性、完整性、可用性、认证、授权和审计六个安全属性来衡量攻击对目标系统的影响，为攻击行为评估搭建起较为系统的框架。此后，鉴于MITRE ATT&CK框架在攻击行为描述领域的全面性与标准化优势，Zhang等人[26]提出基于MITRE ATT&CK知识库的量化指标，通过评估单个技术的权限要求，对保密性、完整性和可用性的影响等级，以及使用该技术所涉及的软件数量等方式，实现对攻击技术的量化评估。针对现有网络主机风险评估方法中资产价值评估主观性强及忽略节点关联性的问题，杨宏宇等人[27]提出一种基于主机重要度的网络主机节点风险评估方法，从保密性、完整性、可用性三个维度评估资产价值，采用熵权法结合多专家评分，通过量化指标权重与标准化评分，客观计算主机节点的资产保护价值。

然而，以上研究虽针对攻击行为构建了类似CVSS的评估标准，但在场景适配性层面，由于不同组织的网络架构、业务特性与安全需求差异显著，通用标准难以精准映射个性化安全诉求，导致用户难以基于自身业务特征完成网络安全状况的精细化评估。如何在标准化评估框架与定制化需求间建立适配机制，成为本文的关键研究方向。

1.3 基于攻击图的风险评估

逻辑攻击图虽能有效刻画网络系统中潜在攻击路径的关系结构，但其往往未充分融合路径攻击可能性的量化差异，尤其忽视攻击行为所处攻击阶段的动态演化特征。

在攻击路径概率建模与动态行为分析方向，Zhang等人[26]提出的结合攻击图和马尔可夫链的网络安全风险评估模型，该模型利用马尔可夫链的状态转移特性，通过构建攻击行为的状态转移矩阵，有效刻画了攻击实体在不同阶段的风险转移过程。类似地，Zheng等人[28]提出了一种基于主机粒度的贝叶斯攻击图（Bayesian Attack Graph，BAG）的动态分析方法，通过将攻击场景转化为贝叶斯概率模型，并引入改进的BAG生成算法与前向—后向概率传播机制，实现了攻击路径的实时更新与动态风险评估。

在量化评估与应用拓展方面，Homer等人[29]提出一种基于攻击图的企业网络脆弱性度量聚合方法，该方法将CVSS漏洞评分与网络拓扑结构深度融合，通过计算关键节点的累积脆弱性指标，不仅考虑了单个漏洞的风险程度，还结合网络结构特征评估攻击传播的潜在影响，实现了对网络系统脆弱性的综合量化评估。

以上现有研究，基于攻击图的风险评估方法虽在不同程度上解决了针对攻击路径重要性评估的问题，但仍未能全面考虑攻击技术特性、攻击行为变化等多维因素的综合影响，未考虑基于ATT&CK框架中的技战术的多对一关系，难以准确反映复杂网络环境中的实际安全风险状况。

2 预备知识

为实现攻击路径中战术阶段的建模与评估，本文采用隐马尔可夫模型（HMM）作为核心建模工具。本节将介绍HMM的基本原理，并结合MITRE ATT&CK知识库框架说明其在本方法中的变量设定与参数构建方法。

2.1 MITRE ATT&CK框架

MITRE ATT&CK框架由美国MITRE机构在长期红队演练与真实攻击研究基础上提出，是目前应用最广泛的对抗性攻击行为知识体系之一[30]。与传统Kill Chain模型侧重对攻击生命周期进行宏观阶段划分不同，MITRE ATT&CK通过战术（tactic）与技术（technique）的分层结构，对攻击者在不同阶段的行为意图及其具体实现方式进行细粒度刻画。该框架以攻击者在不同阶段的目标为主线，将攻击过程划分为一系列战术，并在每个战术下定义攻击者实现该目标所采用的具体技术，从而形成意图到手段的两层语义结构[31]，其清晰的战术与技术层级关系及技术对战术的多对一映射特性，为本文构建技战术双层关联模型提供了统一的数据语义基础和行为描述框架。

2.2 HMM基本原理

隐马尔可夫模型（HMM）是一种时序统计模型[32]，近年来，被广泛应用于网络安全领域，尤其适用于建模攻击行为的阶段性演化过程。在实际攻击活动中，攻击者往往以链式方式逐步推进，每一步对应一个特定的意图阶段与行为模式，而这些意图往往不可直接观测，仅能通过攻击技术等显性行为加以推测。这类隐藏状态与观测行为之间的依赖关系，符合HMM所针对的建模范畴与刻画目标。

HMM假设系统在时间t的状态q_t仅依赖于前一时刻状态q_{t-1}，满足马尔可夫性。同时，每个隐藏状态并不可直接观测，但可通过一定概率输出一个观测值o_t。据此，HMM的建模对象由一组不可直接观测的隐藏状态Q与对应的可观测状态O构成。模型以三组参数描述系统行为：隐藏状态转移概率矩阵$\boldsymbol{A}$、观测概率矩阵$\boldsymbol{B}$，以及初始状态概率向量$\boldsymbol{\pi}$，合称为模型三元组$\boldsymbol{\lambda}=(\boldsymbol{A},\boldsymbol{B},\boldsymbol{\pi})$。

2.3 攻击语义映射与模型变量构建

本方法基于MITRE ATT&CK Enterprise V18.0知识库构建HMM模型，以建模攻击者在多阶段攻击路径中的行为演化过程。然而，真实攻击数据通常缺乏

对战术阶段的明确标注,且攻击技术与战术之间的非确定性映射关系,这一特性使得传统HMM所依赖的方法在该场景中难以直接适用。为克服上述问题,本文结合领域专家知识与历史攻击事件的统计特征,显式构建三元组参数$(\boldsymbol{A},\boldsymbol{B},\boldsymbol{\pi})$。该组参数将作为后续攻击路径推理、风险评估模块的输入。具体构建方法如下:

(1)战术状态转移概率矩阵$\boldsymbol{A}$

设攻击战术隐藏状态序列为$Q=\{q_1,q_2,\cdots,q_t\}$,攻击技术集合为$O=\{o_1,o_2,\cdots,o_t\}$。状态转移矩阵$\boldsymbol{A}=a_{ij}=P\left(q_t=q_j\middle|q_{t-1}=q_i\right)\in\mathbb{R}^{N\times N}$表示攻击战术之间的转移概率,其中$a_{ij}$为从战术$q_i$转移到战术$q_j$的概率。原始数据中记录的是攻击技术之间的关系,因而基于攻击技术对$\left(o_x,o_y\right)$构建技术层转移频次矩阵$\boldsymbol{C}=C_{xy}\in\mathbb{R}^{M\times M}$,并定义技术层面的转移概率如式(1)所示。

$$P_{xy}=\frac{C_{xy}}{\sum_{x=1}^{M}\sum_{y=1}^{M}C_{xy}} \tag{1}$$

考虑到攻击技术与攻击战术的多对一映射关系,设前置技术o_x对应的战术集合为T_i,后置技术o_y对应的战术集合为T_j,则战术层面的转移概率如式(2)所示。

$$a_{ij}=\sum_{x\in T_i}\sum_{y\in T_j}P_{xy} \tag{2}$$

对矩阵$\boldsymbol{A}$的每一行逐一进行归一化处理,确保每个战术状态的转移概率总和为1。

(2)技术状态观测概率矩阵$\boldsymbol{B}$

观测概率矩阵$\boldsymbol{B}=\left\{b_{jk}=P\left(o_t=o_k\middle|q_t=q_j\right)\right\}\in\mathbb{R}^{N\times M}$表示各战术阶段下攻击者可能采取的技术行为及其分布规律,其中b_{jk}为在战术q_j下观测到技术o_k的条件概率。设D_{jk}为攻击战术q_j相关事件中攻击技术o_k出现的次数,D_{j*}为攻击战术q_j下攻击技术出现的总次数,则b_{jk}计算方式如式(3)所示。

$$b_{jk}=\frac{D_{jk}}{D_{j*}} \tag{3}$$

对矩阵$\boldsymbol{B}$的每一行逐一进行归一化处理,确保每个战术状态下的技术发生概率总和为1。由于ATT&CK框架中同一攻击技术可能隶属于多个攻击战术,矩阵$\boldsymbol{B}$在不同战术对应的行上允许同一技术列取非零值,从而在概率意义上体现攻击技术与攻击战术之间的非确定性关联特征。

(3)战术初始状态概率向量$\boldsymbol{\pi}$

初始状态向量$\boldsymbol{\pi}=\left(\pi_1,\pi_2,\cdots,\pi_N\right)^{\mathrm{T}}$表示攻击序列起始阶段各攻击战术出现的概率分布,其中$\pi_i=P\left(q_1=q_i\right)$为攻击路径起始阶段属于战术$q_i$的概率。设$E_i$是以战术$q_i$为起点的攻击路径数,$E$是攻击路径总数,则$\pi_i$计算方式如式(4)所示。

$$\pi_i=\frac{E_i}{E} \tag{4}$$

向量$\boldsymbol{\pi}$经归一化处理后作为模型的初始战术分布。

(4)隐藏状态序列建模

由于ATT&CK中攻击行为在战术层呈现非确定性映射结构,为将该结构纳入HMM的隐藏状态建模,通过上述定义构建的战术转移矩阵$\boldsymbol{A}=\left\{a_{ij}\right\}$与观测概率矩阵$\boldsymbol{B}=\left\{b_{jk}\right\}$,在时间步$t$,基于上一时刻的战术状态后验分布,采用前向递推方式定义当前战术状态的后验概率,如式(5)所示。

$$P(q_t|o_{1:t})=b_{q_t}\left(o_t\right)\sum_{q_{t-1}\in Q}a_{q_{t-1},q_t}P(q_{t-1}|o_{1:t-1}) \tag{5}$$

其中,$\sum a_{q_{t-1},q_t}P(q_{t-1}|o_{1:t-1})$为由战术转移矩阵$\boldsymbol{A}$推导得到的当前战术先验分布,用于刻画攻击者在不同攻击阶段间的演化趋势;$b_{q_t}\left(o_t\right)$为在战术q_t下执行技术o_t的条件概率$P(o_t|q_t)$,用于刻画具体技术行为在战术语义空间中的分布规律。通过上述前向递推过程,战术阶段演化与技术行为生成在概率意义下得以融合,从而实现由攻击技术观测序列到战术隐藏状态序列的推断连接。

3　攻击图风险评估模型

3.1　模型框架

本节介绍了总体框架,并解释了它如何解决上文讨论的挑战。如图2所示,整体系统设计包含三个核心模块:①逻辑攻击图重构模块,基于当前网络场景信息及ATT&CK知识库生成MulVAL攻击图,并针对攻击者位置、攻击行为及影响结果重构攻击图;②技战术双层关联模块,通过引入HMM模型,对攻击路径中存在的多对一攻击技术与战术之间的隐式映射关系进行建模,借助维特比算法推理攻击者可能的战术演化路径;③风险评估模块,结合ATT&CK技术库的攻击行为与实际环境的资产个性化优先级量化评估,并将其嵌入前向算法的递推过程中实现节点、路径及主机层级的风险排序。

3.2　逻辑攻击图重构模块

在传统MulVAL攻击图体系中,节点采用LEAF、OR、AND三类划分:LEAF节点存储系统配置信息,OR节点描述攻击触发条件,AND节点则代表攻击目标。这些节点分别征主机安全状态与系统配置要

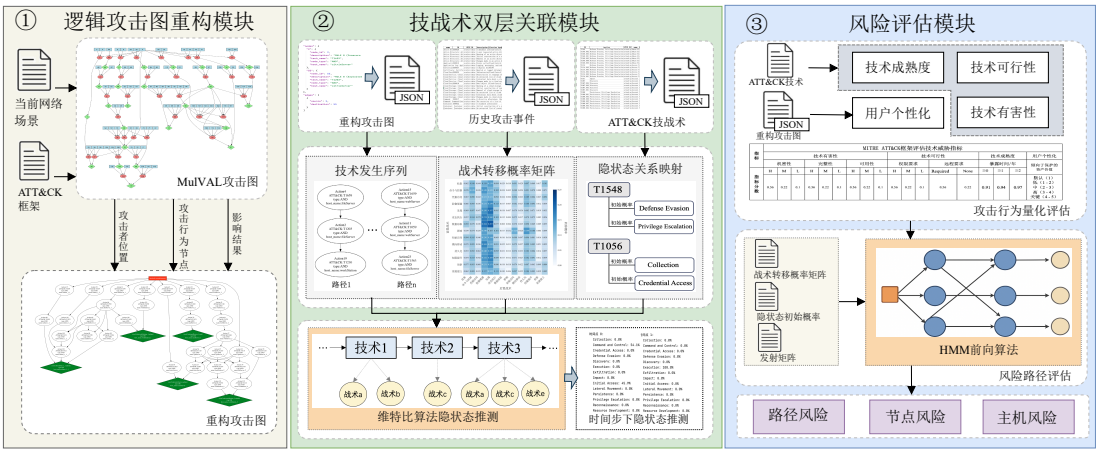

图2 整体框架图

Figure 2 Overall framework diagram

素，而攻击行为则以边的形式连接不同节点，形成攻击路径。本节提出的构图方法，将每个节点明确界定为一个独立的攻击行为，在攻击图中构建主机与攻击行为的映射关系，展现攻击者在网络中的每一步攻击行为。

在节点语义重构过程中，通过分析 Prolog 语法特征，提取攻击图中各节点隐含的主机归属信息，并将其转换为便于处理的 JSON 格式文件。方法依据 MulVAL 攻击图的 XML 文件，识别 LEAF、AND、OR 等不同类型逻辑节点对应的上下文。以 LEAF 节点规则“vulExists（webServer，‘CVE-2020-17519’，httpd）”为例，通过该规则确认该节点属于 webServer 主机，与之相连的 OR 节点及后续的 AND 节点，在主机归属未发生变化前，均默认归属于同一主机，直至遇到下一个 OR 节点的 LEAF 父节点且所属主机不同而发生改变。算法将传统模型中的 AND 节点作为独立的攻击行为节点单元，结合与之关联的 LEAF 节点和 OR 节点信息，使得每个节点单元均完整包含技术标签、行为描述、所属主机等核心属性。

在攻击图重构过程中，则借助 DFS（Depth First Search）深度搜索算法，提取以攻击行为为核心的有效节点信息作为节点。同时，基于 MulVAL 逻辑规则构建节点间的依赖边，具体攻击图重构算法流程如算法 1 所示。其中，currentNode 表示当前遍历的节点，path 为当前路径，allPaths 用于存储所有可能的路径，nodeMap 是节点 ID 到节点对象的映射表，accessP 是访问控制策略函数，用于判断是否允许从一个主机传播到另一个主机。

通过对节点定义的优化和攻击图的重构，有效解决了传统攻击图攻击行为语义模糊的问题，并将重构的攻击图作为模型后续的输入。

算法 1 改进 DFS 攻击路径生成算法

```
1. 函数 DFS(currentNode, path, allPaths, nodeMap, accessP)
2.   如果 currentNode ∈ path:
3.   返回
4.   newPath ← path ∪ [currentNode]
5.   如果 currentNode.nodeType == “AND”:
6.     validChildren ← [ ]
7.     对于 currentNode.children 中的每个 childID:
8.       childNode ← nodeMap[childID]
9.   如果 accessP.permits(currentNode.host, childNode.host):
10.          validChildren.append(childNode)
11.    如果 validChildren 为空:
12.      allPaths.add(newPath)
13.    否则:
14.      对于 validChildren 中的每个 childNode:
15.        DFS(childNode, newPath, allPaths, nodeMap, accessP)
16.  否则:
17.    allPaths.add(newPath)
18.    对于 currentNode.children 中的每个 childID:
19.      childNode ← nodeMap[childID]
20.      如果 accessP.permits(currentNode.host, childNode.host):
21.    DFS(childNode, newPath.copy(),allPaths, nodeMap, accessP)
22. 结束函数
```

3.3 逻辑攻击图重构模块

为了推断攻击技术序列背后的战术演化过程，本节引入基于第 3 章构建的 HMM 模型$(\boldsymbol{A},\boldsymbol{B},\boldsymbol{\pi})$，采用维特比算法对给定攻击技术序列进行战术层推理，以显化攻击行为在战术语义空间中的阶段演化过程，为后续风险评估提供战术级上下文参考。维特比算法是一种用于求解 HMM 中最优隐藏状态序列的动态规划算法，能够在给定观测序列的条件下，寻找使联合概率最大化的状态路径。该算法通过在每个时间步递

归计算并记录到达各状态的最优路径概率,最终通过回溯过程输出完整的最优隐藏状态序列。

维特比算法通过动态规划思想,递归计算最可能的战术序列。该算法包含四个关键步骤:

(1)初始化:对于初始时刻 $t=1$,如式(6)得到每个可能战术状态 i 的初始概率。

$$\delta_1(i)=\pi_i\cdot b_i(o_1) \tag{6}$$

其中,π_i 表示战术 i 的概率;$b_i(o_1)$ 是在采用战术 i 的条件下,观测到特定技术 o_1 的概率。

(2)递推:当观测到一系列技术时,如式(7)得到每个时间步 t 的最优战术路径。

$$\delta_t(j)=\max\left[\delta_{t-1}(i)\cdot a_{ij}\right]\cdot b_j(o_t) \tag{7}$$

其中,a_{ij} 表示攻击者从战术 i 转移到战术 j 的概率;$b_j(o_t)$ 表示在战术 j 下使用技术 o_t 的概率。

(3)终止:如式(8)计算整个攻击链的最大概率 P,并确定最终时刻的隐藏状态 q_t 如式(9)。

$$P=\max\left[\delta_t(i)\right] \tag{8}$$

$$q_t=\arg\max\left[\delta_t(i)\right] \tag{9}$$

其中,$\delta_t(i)$ 为在时刻 t 下,攻击者使用战术 i 的概率。

(4)路径回溯:从终态开始,根据 $q_{t-1}=\psi_t(q_t)$ 回溯,得到完整的战术序列。通过该推理模块,攻击路径中隐藏的战术行为得以显化,为后续的风险评估提供战术级上下文。

3.4　风险评估模块

3.4.1　攻击行为量化评估

借鉴CVSS脆弱性评估模型的相关思想,基于MITRE ATT&CK框架,构建威胁指标体系,该体系包含四个关键维度:技术有害性(TechH)、技术可行性(TechF)、技术成熟度(TechM)和资产个性化(Per),形成了一个多角度、多层次的威胁度量框架,如表2所示。

表2　MITRE ATT&CK框架评估技术威胁指标

Table 2　MITRE ATT&CK framework evaluation technical threat indicators

指标	技术有害性									技术可行性					技术成熟度			资产个性化
	机密性			完整性			可用性			权限要求			远程要求		暴露时间/月			倾向保护的资产
指标分数	高	中	低	高	中	低	高	中	低	高	中	低	需要	不需要	≥0	≥12	≥24	低(1~2) 中(2~3) 高(3~4)
	0.56	0.22	0.1	0.56	0.22	0.1	0.56	0.22	0.1	0.56	0.22	0.1	0.56	0.22	0.91	0.94	0.97	关键(4~5)

技术有害性维度深入探究了攻击技术对信息系统三大安全属性的潜在破坏程度。机密性 $\mathrm{TechH_C}$ 即敏感信息是否会被非法获取与泄露;完整性 $\mathrm{TechH_I}$ 即数据是否会遭到恶意篡改而失去原本的真实性与准确性;可用性 $\mathrm{TechH_A}$ 即关注系统或服务是否能持续正常运行,以满足用户的业务需求。

技术可行性维度从实施难度角度进行评估,综合考量两个关键因素。一是权限要求维度,分析攻击者为达成攻击目的所需获取的系统访问权限级别。二是远程要求维度,探讨攻击者是否能够在无需与目标系统交互的情况下,通过网络远程发动攻击。

技术成熟度维度通过衡量攻击技术在网络环境中的暴露时间TechTIME,评估其被安全研究人员发现并修复的可能性。一般而言,暴露时间越长的攻击技术,被安全社区充分研究并开发出相应防御方案的概率越高。

资产个性化引入技术与目标主机的关联性,允许根据特定环境需求,对数据资产价值(Data Asset Value,DA)、业务流程关键性(Business Process criticality,BP)和系统架构特点(System Architecture characteristics,SA)三个维度制定了明确的量化评分标准。数据资产价值主要依据资产所承载数据的敏感程度及规模大小进行评估,公开或低敏感性数据对应较低评分,而涉及核心业务数据或用户隐私的数据则赋予较高评分;业务流程关键性用于衡量资产在业务流程中的不可替代程度,依据资产中断对核心业务运行及上下游系统的影响程度进行判定,支撑核心业务流程的资产获得更高评分;系统架构特点反映资产在网络中的攻击暴露程度及防御与恢复能力,暴露面越大、防御纵深越弱、恢复难度越高,其评分越高。在统一评分准则下,由三名具备网络攻防与业务系统经验的专家,对每个资产 h,分别给出评分 $\mathrm{DA}_h,\mathrm{BP}_h,\mathrm{SA}_h\in[1,5]$,最终取其平均值作为资产在各维度上的评分结果,形成用于后续技术风险加权计算的资产个性化系数Per。

将上述四个核心维度细化为7个具体指标,并在式(10)中说明了计算方法。威胁指标中的指标分数部分参考已有文献[26]中的专家经验,并结合ATT&CK知识库中的典型案例进行分析。为保证各指标均衡发挥作用,实验中统一采用平均值进行权重分配。

$$\begin{cases}\text{TechH}=10\times\left[1-\left(1-\text{TechH}_{\text{C}}\right)\left(1-\text{TechH}_{\text{I}}\right)\left(1-\text{TechH}_{\text{A}}\right)\right]\\ \text{TechF}=\lambda\times\text{TechPR}+\varphi\times\text{TechUI}\\ \text{TechM}=10\times\text{TechTIME}\\ \text{Per}=\omega_{\text{DA}}\times\text{DA}_h+\omega_{\text{BP}}\times\text{BP}_h+\omega_{\text{DS}}\times\text{SA}_h\\ \text{TechRisk}=\left(\alpha\times\text{TechH}+\beta\times\text{TechF}+\gamma\times\text{TechM}\right)\times\text{Per}\\ \lambda+\varphi=1\\ \omega_{\text{DA}}+\omega_{\text{BP}}+\omega_{\text{DS}}=1\\ \alpha+\beta+\gamma=1\end{cases}\tag{10}$$

3.4.2 风险路径评估

为进一步量化攻击路径的潜在风险水平，引入前向算法对观测序列进行概率评估，并在过程融合攻击技术威胁量化指标，构建路径级的风险评估模型。前向算法是HMM模型中用于计算给定观测序列在特定模型参数下发生概率的核心递推算法。在时间步t时，递归地计算系统处于每个可能隐藏状态的联合概率，直到整个观测序列结束，得到该观测序列在模型下的总体概率。在此基础上，引入攻击技术的风险权重，并结合模型推理得到的状态演化概率，构建每一时间步的动态风险权重，以实现对攻击路径中各观测点技术行为风险贡献的综合建模。

算法2依托前向算法在时间维度上动态更新路径状态概率，结合当前观测节点的风险权重，对潜在路径的风险进行加权计算，并输出其路径风险值。

算法2 基于HMM的路径风险感知前向算法

输入：攻击图G，

观测序列$O=\{o_1,o_2,\cdots,o_T\}$，

隐藏状态转移矩阵$\boldsymbol{A}=\{a_{ij}\}$，

观测概率矩阵$\boldsymbol{B}=\{b_j(o_t)\}$，

技术风险指标$R(o_t)$

输出：攻击路径的风险值Risk

1. FOREACH 每条攻击路径 $P\in G$ DO
2. 步骤1:初始化各隐藏状态的初始概率
3. 设置初始状态概率:$\pi_i=1/N\ (i=1,2,\cdots,N)$
4. FOR $i=1$ TO N DO
5. 计算初始观测概率:$\alpha_1(i)=\pi_i\cdot b_i(o_1)$
6. END FOR
7. 初始时间步观测概率:$\alpha_{\text{sum}}(1)=\sum_{i=1}^{N}\alpha_1(i)$
8. 步骤2:前向递推
9. FOR $t=2$ TO T DO
10. FOR $j=1$ TO N DO
11. 隐藏状态转移概率:$\text{temp}=\sum_{i=1}^{N}\alpha_{t-1}(i)\cdot a_{ij}$
12. 当前隐藏状态发生可能性:$\alpha_t(j)=\text{temp}\cdot b_j(o_t)$
13. END FOR
14. 当前时间步概率:$\alpha_{\text{sum}}(t)=\sum_{i=1}^{N}\alpha_t(j)$
15. 当前时间步条件概率:$P_t=\alpha_{\text{sum}}(t)/\alpha_{\text{sum}}(t-1)$
16. 当前时间步风险:$\text{Risk}_t=P_t\cdot R(o_t)$
17. 路径风险:$\text{Risk}_{P_g}+=\text{Risk}_t$
18. END FOR
19. 输出当前路径风险值Risk_{P_g}
20. END FOR

4 实验与分析结果

本章评估了隐马尔可夫在攻击路径评估方面的性能，并将其与最先进的方法进行了比较，目标是通过回答以下研究问题来评估本文提出的方法。

问题1：在ATT&CK框架下，是否可以通过结合攻击技战术的固有属性与转移关系，实现关键攻击路径的识别与风险排序？

问题2：资产个性化值（Per）的调整，是否会对模型中攻击路径的选择结果产生影响？

问题3：基于已建模的攻击图结构，对比分析不同模型在不同维度（节点、路径、主机）下的风险评估结果，验证本模型评估能力。

4.1 实验设置

本节设计了两个实验场景，以验证所提出的方法在攻击图建模与路径风险评估方面的适应性与有效性，实验场景具体设置如表3所示。

表3 实验场景网络规模、攻击路径复杂性与工具设置

Table 3 Experimental scenario network scale, attack path complexity, and tool configuration

实验场景	行业属性	主机数量	MulVAL节点数量	MulVAL边数量	重构攻击图路径数量	漏洞数量	构图工具
实验场景1	中小型企业内网	3	28	29	2	2	MulVAL1.2.1
实验场景2	政府/关键基础设施内网	13	142	131	24	11	MulVAL1.2.1

4.1.1 实验场景1：单目标攻击路径建模

实验场景1在完全自主搭建的靶场环境中，聚焦于攻击者针对同一目标主机的场景，是中小型企业常见的IT服务架构，环境由Web服务、文件服务与员工终端构成，攻击链长度较短，用以探究本文模型的实现逻辑及资产个性化值调整对路径选择的影响。网

络架构由互联网攻击入口、关键业务服务器与横向移动目标组成,复现了从初始入侵到权限控制再到横向拓展的三阶段攻击生命周期,拓扑结构如图3所示,该环境包含3台核心主机:文件服务器(fileServer)、Web服务器(webServer)和工作站(workStation)。主机所含漏洞如表4所示。

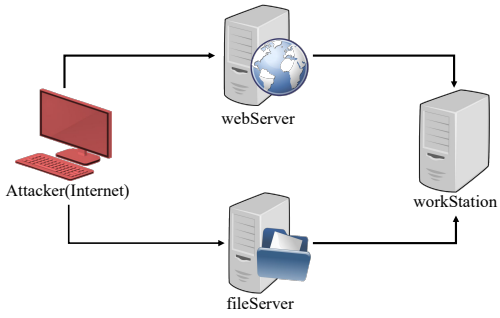

图3　实验场景1拓扑结构

Figure 3　Topology of scenario 1

表4　实验场景1网络主机存在漏洞信息

Table 4　Vulnerabilities information of hosts in scenario 1

主机名	存在漏洞
fileServer	CVE-2008-4250
webServer	CVE-2012-2122
workStation	—

在此场景中,形成了具有2条攻击路径的攻击图,如图4所示。在路径一(Path1)中,攻击者首先利用webServer主机MySQL服务存在的认证绕过漏洞(T1190),成功以root身份登录数据库,并通过写入WebShell或加载恶意插件获取系统初步访问权限(T1059)。随后,攻击者利用计划任务机制提权至root,完全控制webServer。掌控主机后,在内网发现workStation开放的网络文件系统(Network File System,NFS)服务,通过劫持远程文件共享会话,植入安全外壳协议(Secure Shell,SSH)公钥或反向连接脚本,实现对workStation的横向移动与控制(T1563);在路径二(Path2)中,攻击者通过HTTP接口触发VBScript漏洞,利用不安全操作向fileServer注入攻击向量并获得初步访问权限(T1659)。随后,利用系统权限配置缺陷进行本地提权,获取管理员权限(T1203)。掌控主机后,攻击者通过SSH服务,利用远程服务会话劫持技术横向入侵workStation(T1210)。

4.1.2　实验场景2:企业级网络拓扑下的攻击路径建模

实验场景2参考文献[9]所构建的企业分区式网络架构攻击图场景,构建了一个具备真实网络特征的实验环境,用于验证所提方法在复杂环境下不同攻击路径的风险排序表现。拓扑结构如图5所示。该结构划分为边界服务器区、内部业务服务器区与终端子网区,涵盖13台关键主机与设备,以及11类通用漏洞披露(Common Vulnerabilities and Exposures,CVE)漏洞,具体包括:

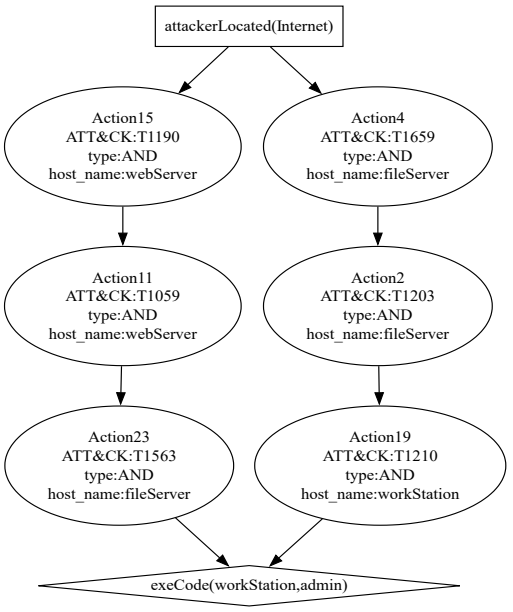

图4　实验场景1场景攻击图

Figure 4　Attack graph of scenario 1

(1)边界服务器:citrixServer(Citrix应用服务器)、commServer_2(通信服务器)、webServer_1/webServer_2(Web服务器)、vpnServer_2(VPN网关);

(2)内部业务服务器:fileServer_1/fileServer_2(文件服务器)、mailServer_1(邮件服务器)、dataHistorian(数据存储服务器);

(3)子网区域:subnet_1_1(业务子网1)、subnet_1_2(业务子网2);

(4)终端设备:workStation_1/workStation_2(工作站)。

主机所含漏洞如表5所示。

在此场景中,攻击者从互联网利用外部访问权限直接连接至边界主机citrixServer、vpnServer_2、webServer_1、workStation_1等,发起初始攻击。边界主机部署的Web服务、VPN服务及弱口令配置成为首要攻击目标。攻破边界主机后,攻击链进一步向内部网络渗透,攻击者进一步将攻击范围扩展至业务子网subnet_1_1和subnet_1_2,通过远程执行、权限提升等手段获取子网内部主机的控制权,并通过横向移动连接至fileServer_1、mailServer_1、dataHistorian等核心服务器,利用服务器消息块(Server Message Block,SMB)、NFS等服务漏洞扩大影响,部分攻击链路进一步深入到workStation_2终端主机,完成了权限控制与

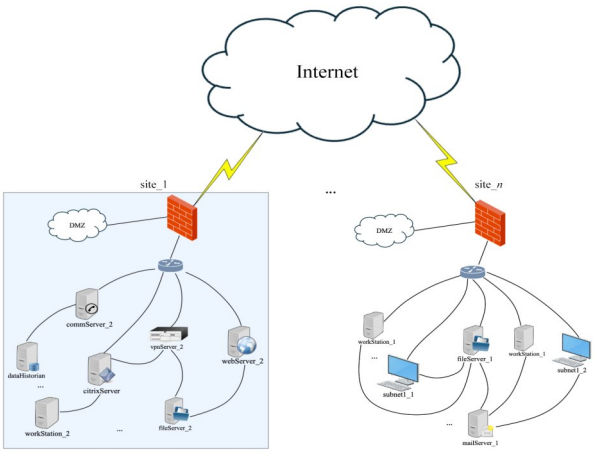

图5 实验场景2拓扑结构

Figure 5 Topology of scenario 2

表5 实验场景2网络主机存在漏洞信息

Table 5 Vulnerabilities information of hosts in scenario 2

主机名	存在漏洞
workStation_1	CVE-2010-0483
webServer_2	CVE-2021-3129
citrixServer	CVE-2010-0490
vpnServer_2	CVE-2013-2092
subnet_1_2	CVE-2010-0490
subnet_1_1	CVE-2010-0483
commServer_2	CVE-2010-0483
workStation_2	CVE-2008-4250
fileServer_1	CVE-2010-0812
webServer_1	CVE-2002-0392
dataHistorian	CVE-2010-0494
fileServer_2	—
mailServer_1	—

数据获取。整体攻击路径呈现由外部互联网发起,穿越边界,控制子网,渗透核心的分阶段演进特性,形成从外到内的24条完整攻击路径,如图6所示。

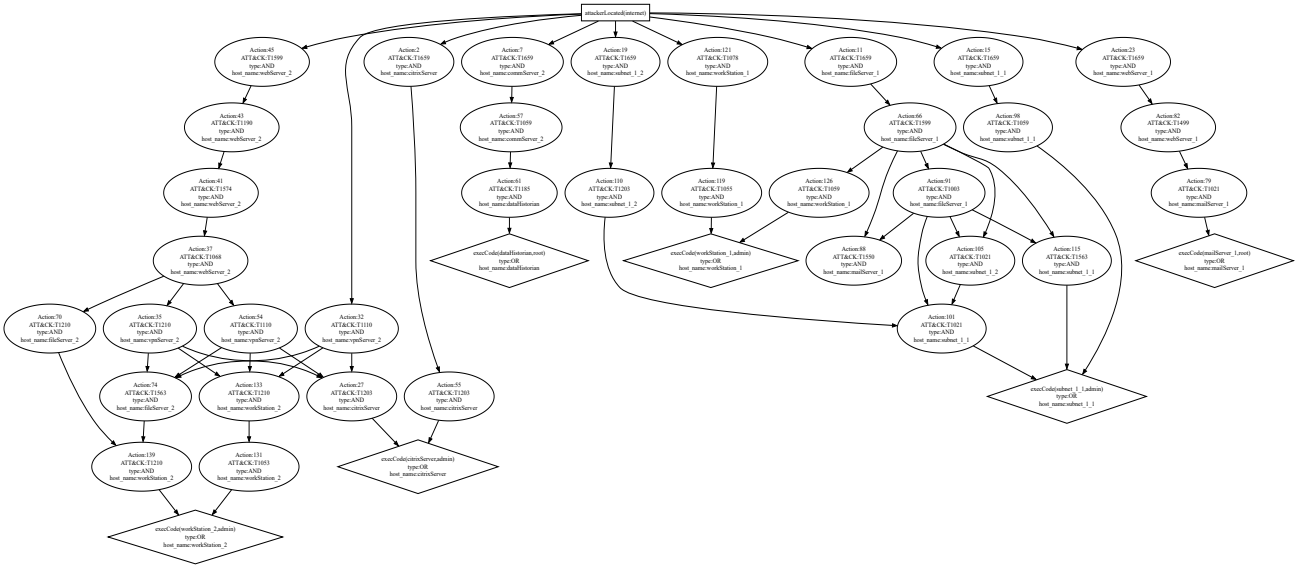

图6 实验场景2攻击图

Figure 6 Attack graph of scenario 2

4.2 攻击技战术风险建模与阶段转移建构

本节旨在为攻击路径识别与风险排序提供建模基础。我们从攻击技战术两个层面入手:一方面,基于ATT&CK技术的固有属性构建技术风险评分体系,识别在一般环境下固有威胁程度较高的攻击行为;另一方面,引入历史攻击数据,依据模型对攻击阶段间的行为转移关系进行建模。

由于资产个性化值反映的是实际网络中主机的受关注程度,而本小节旨在展示节点自身的威胁指标,因此在实验中将攻击图中资产个性化影响参数统一设为默认值1,即资产权重不影响评估结果。基于此,风险量化模型仅考虑权限要求、远程利用要求、机密性、完整性、可行性和漏洞暴露时间等基础指标。ATT&CK技术风险值前15评估结果,详见表6。

鉴于攻击技术的固有属性指标的局限性,引入ATT&CK框架的历史攻击事件库,通过系统的频次统计与深度关联分析,从大量技术数据中筛选出在真实攻击场景中出现概率最高的前15项技术组,并以热力图形式呈现,如图7所示。基于对所有技术组的统计数据,最终生成战术转移概率矩阵构建HMM模型的转移矩阵,并据此生成战术转移态势,如图8所示。从图中分析可知,战术“数据窃取”转移到战术“发

表6　ATT&CK技术风险值前15

Table 6　Top 15 ATT&CK techniques by risk value

MITRE技术	权限要求	远程要求	机密性	完整性	可用性	暴露时间	技术风险权重
T1190	None	None	high	high	high	2018-04-18	9.124 08
T1078	None	None	high	high	high	2017-05-31	9.124 08
T1189	None	Required	high	high	high	2018-04-18	9.124 08
T1195	None	Required	high	high	high	2018-04-18	9.124 08
T1200	None	Required	high	high	high	2018-04-18	9.124 08
T1543	None	None	high	high	high	2020-01-10	9.124 08
T1199	None	None	high	high	medium	2018-04-18	8.794 96
T1176	None	Required	high	high	medium	2018-01-16	8.794 96
T1059	Low	None	high	high	medium	2017-05-31	8.219 96
T1112	Low	None	medium	high	high	2017-05-31	8.219 96
T1110	None	None	high	medium	medium	2017-05-31	8.211 52
T1111	None	Required	high	medium	medium	2017-05-31	8.211 52
T1187	None	Required	high	medium	medium	2018-01-16	8.211 52
T1140	None	None	high	medium	low	2017-12-14	8.005 60
T1041	None	None	high	medium	low	2017-05-31	8.005 60

现”的可能性最大。

为进一步验证本文基于历史攻击技术统计构建的战术转移矩阵的可靠性,本文选取未参与统计构建的MITRE ATT&CK官方公开记录的APT32针对政府机构的入侵事件作为验证样本。攻击者首先通过鱼叉式钓鱼邮件附件和恶意链接(T1566)诱导用户触发载荷,对应初始访问战术。成功取得入口后,APT32启动恶意可执行文件(T1204)并利用PowerShell脚本(T1059)展开执行操作,对应攻击执行战术。在建立立足点后,攻击者通过创建服务(T1543)与修改注册表Run键(T1547)实现持久化战术。利用凭据转储(T1003)与远程服务(T1021)实现横向移动并获取更高权限,收集敏感文档(T1119)并通过加密通道外传数据(T1041)。对应技战术映射关系如表7所示。

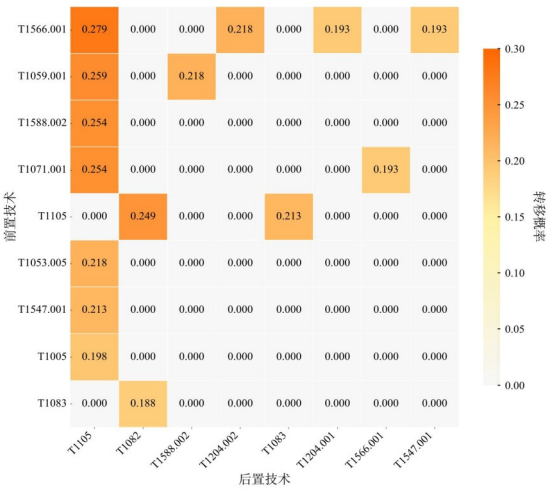

图7　攻击技术转移概率热力图

Figure 7　Heatmap of attack technique transition probability

4.3　攻击路径行为分析与资产个性化风险影响

为验证所提出方法在多阶段攻击路径识别中的应用表现与用户偏好影响方面的能力,本节基于实验一中构建的攻击场景,围绕攻击路径选择机制与资产个性化权重变化两个维度开展深入分析。

4.3.1　攻击路径选择与隐马尔可夫状态分析

根据实验场景1所构建的APT攻击场景,探讨本文的模型在多阶段攻击路径识别中的应用表现。该实验旨在分析:在具有相同攻击目标的多条路径中,本文的模型如何基于攻击阶段的状态演化和历史观测概率,对路径风险值进行排序,从而识别出攻击者更可能采用的优先路径。

表8和图9展示了两条典型攻击路径在主机资产同等重要的条件下的风险评估结果。其中,表8列出了每一步攻击技术的风险权重、观测概率与路径总风险值等,而图9则以时间演进的方式呈现每条路径中各阶段的单步风险值分布情况。

尽管Path2中的攻击技术具有更高的总风险权重,但Path2的整体路径风险得分仍明显低于Path1。这一差异的根本在于,本文的模型不仅整合了攻击技术的风险权重,还引入了攻击行为在不同阶段的隐藏状态依赖与观测频率。以Path2为例,其路径起点根据隐藏状态映射概率,由于“初始访问”阶段的起始概率高于“命令与控制”,因此,Path2从战术“命令与控制”起步,而起点隐藏状态映射可能性仅为54.1%,导致风险值被明显稀释。尽管起点技术T1659的风

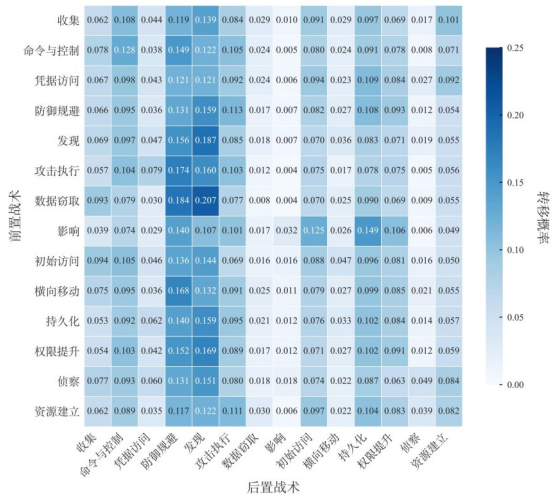

图8 战术隐藏状态转移概率热力图

Figure 8 Heatmap of tactical hidden state transition probability

表7 攻击事件ATT&CK技战术映射关系

Table 7 Mapping between attack events and ATT&CK techniques and tactics

攻击行为	技术	战术
钓鱼附件、钓鱼链接	T1566	初始访问
可执行文件运行	T1204	攻击执行
PowerShell执行	T1059	
创建服务	T1543	持久化
注册表启动项	T1547	
凭据转储	T1003	凭据访问
远程服务	T1021	横向移动
文件收集	T1119	收集
加密通道外传	T1041	数据窃取

险权重较高，但相较于Path1的T1190并无显著优势，因此在当前时间步下的单步风险值仅为0.003 02。相比之下，Path1从战术“初始访问”起步，观测技术与隐藏状态战术映射，且对应技术风险权重为全表最高，随着前向推断的累积效应不断放大起点优势，最终使得Path1整体风险值显著高于Path2。

4.3.2 资产个性化权重对攻击路径风险评估的影响分析

为进一步评估本文所提方法在响应用户风险关注差异方面的能力，在实验场景1构建的攻击场景基础上，引入资产个性化权重参数，以模拟防御者对特定资产主机的关注强度差异，探讨该因素对攻击路径风险评估结果的影响。假设防御者对关键主机webServer的安全状态具有较高敏感性，因此将应用于该主机的相关攻击技术赋予资产个性化权重，并将权重值从默认的1逐步提升至5。为消除其他变量的干扰，Path1所涉及主机的资产个性化权重保持不变。

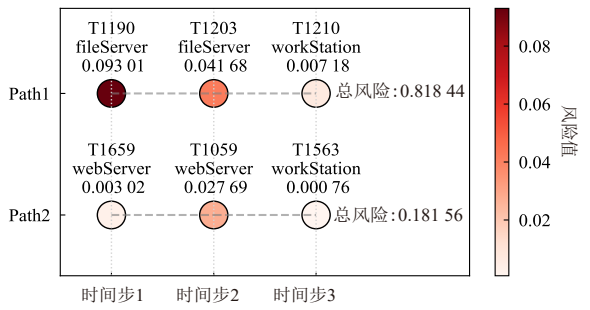

图9 攻击路径时间演进图

Figure 9 Temporal evolution of attack paths

图10展示了在不同资产个性化权重下，两条路径的风险得分变化趋势。从图中可见，随着webServer权重的逐步上调，Path2的风险值持续上升，并在权重值为3.5附近开始超过Path1。这表明当某一资产被赋予更高资产个性化权重后，其所关联的攻击步骤将获得更大的风险贡献值，从而提升其在路径总评分中的影响。此外，如表9中所示，针对攻击图中的节点进行排序，当个性化参数Per值设定为1时，代表资产个性化机制不作用于网络主机，不体现用户差异化关注。分析可知，随着webServer主机资产个性化权重的增加，部署在该主机上的攻击技术节点风险权重显著上升，从而在整体节点排序中排名大幅前移；而部署在普通主机fileServer和workStation上的节点风险权重则基本保持不变。实验结果表明：对于路径中包含关键资产的情形，该调整机制将使模型偏向具有更高防御优先级的攻击路径，体现出高度的定制化适应能力。

表8 实验场景1攻击路径单步技术参数

Table 8 Single-step technique parameters of attack paths in scenario 1

路径	MITRE技术	战术隐藏状态	关联主机	技术风险权重	观测概率	路径总风险值
Path1	T1190	初始访问:100%	fileServer	8.962	1.048×10^{-2}	0.818 44
	T1203	攻击执行:100%	fileServer	6.834	6.33×10^{-5}	
	T1210	横向移动:100%	workStation	5.299	8.58×10^{-8}	
Path2	T1659	命令与控制:54.1% 初始访问:45.9%	webServer	7.709	3.90×10^{-4}	0.181 56
	T1059	攻击执行:100%	webServer	8.222	1.32×10^{-6}	
	T1563	横向移动:100%	workStation	6.174	1.62×10^{-10}	

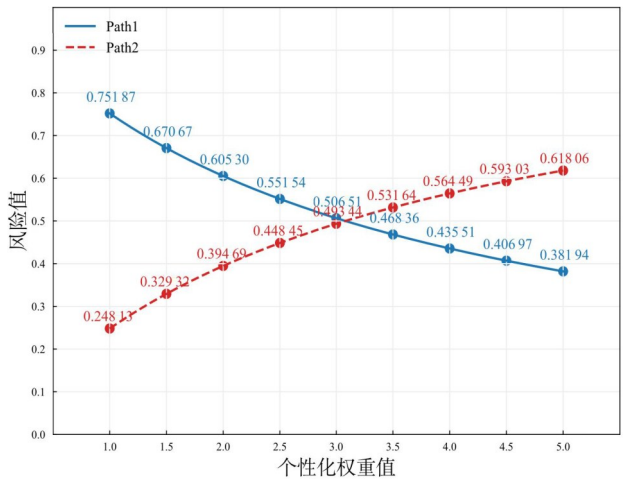

图 10　资产个性化权重对路径选择的影响

Figure 10　Impact of asset-specific weights on path Selection

表 9　实验场景 1 攻击图节点风险权重

Table 9　Node risk weights in attack graph for scenario 1

序号	节点 id	攻击技术	关联主机	节点风险权重		
				Per=1	Per=3	Per=5
1	11	T1190	webServer	0.093 0	0.279 0	0.465 1
2	16	T1053		0.004 3	0.012 9	0.021 5
3	4	T1659	fileServer	0.003 0	0.003 0	0.003 0
4	2	T1203		0.051 1	0.051 1	0.051 1
5	25	T1210	workStation	0.007 2	0.007 2	0.007 2
6	20	T1021		0.004 3	0.004 3	0.004 3

4.4　不同维度下攻击风险评估方法对比实验

本节从节点、主机与路径三个维度出发,选取了两类主流模型作为对比基线:(1)马尔可夫模型(MM)[26];(2)贝叶斯模型(Bayes)[28]。上述两个模型均仅用于攻击路径的概率计算,与本文模型共享相同的攻击图结构,以确保对比结果具有一致性。对比模型的具体设置如下:(1) 马尔可夫模型(MM)采用一阶马尔可夫假设,并基于攻击图中的技术转移频次统计构建转移矩阵,不加入高阶依赖与额外上下文特征。(2)贝叶斯模型基于节点间依赖关系构建贝叶斯网络,条件概率均采用均匀先验或基于攻击图基本关系的标准设置。重点评估本文所提方法在多路径攻击风险识别与关键节点筛选等实际网络中的适用性与有效性。本质上,所探讨的并非模型本身的优劣,而是其在具体风险评估框架下的应用效果对比。

4.4.1　节点维度风险排名对比

根据节点风险权重,对所有攻击路径中的节点进行了统一排序,共涉及 35 个攻击行为节点。表 10 详细列出了攻击节点风险权重排名前 10 的各节点信息,包括攻击技术、关联主机、节点风险权重、度中心性及路径覆盖率等关键指标,其中括号内容代表对应实体在各模型下的风险排序。由于不同攻击路径长度存在差异,本文模型中节点风险评估易受路径规模影响,在计算节点风险权重时采用平均风险值以削弱路径长度干扰。

表 10　实验场景 2 攻击图节点排名前 10

Table 10　Top 10 node rankings in attack graph for scenario 2

序号	节点 id	攻击技术	关联主机	技术风险权重	度中心性	路径覆盖率	节点风险权重		
							Ours	MM[26]	Bayes[28]
1	121	T1078	workStation_1	8.96	0.029 4	0.041 7	0.277 8	0.095 5(7)	1(1)
2	43	T1190	webServer_2	8.96	0.058 8	0.291 7	0.109 2	0.095 0(9)	0.193 5(4)
3	27	T1203	citrixServer	6.83	0.088 2	0.125 0	0.055 3	0.098 2(1)	0.094 4 (5)
4	55	T1203	citrixServer	6.83	0.029 4	0.041 7	0.051 2	0.098 2(1)	0.094 4(5)
5	110	T1203	subnet_1_2	6.83	0.058 8	0.041 7	0.051 2	0.098 2 (1)	0.094 4 (5)
6	119	T1055	workStation_1	7.51	0.029 4	0.041 7	0.049 9	0.096 7(4)	0.175 5(4)
7	32	T1110	vpnServer_2	8.51	0.088 2	0.125 0	0.040 1	0.086 0(13)	1(1)
8	126	T1059	workStation_1	8.22	0.029 4	0.041 7	0.037 1	0.098 2 (1)	0.015 8(11)
9	37	T1068	webServer_2	7.51	0.117 6	0.291 7	0.031 1	0.097 6(2)	0.000 4(18)
10	57	T1059	commServer_2	8.22	0.058 8	0.041 7	0.027 7	0.098 2 (1)	0.311 5 (2)

经分析可知,高风险节点并不一定具备高网络中心性,例如节点 43 度中心性仅 0.058 8,但风险权重较高,表明攻击者更倾向于选择相邻度高、状态转移概率大的节点,而非单纯依赖网络连接性。此外,高路径覆盖率不必然对应高风险权重,如节点 37 虽覆盖率较高,但风险权重却较低,验证了路径覆盖率与风险权重间并无简单线性关系。在对比不同模型的节点风险权重时,模型评估节点 121 风险最高,该节点位于攻击路径起点,且对应攻击技术的观测概率较高,风险值未经过多次转移而被稀释。相比之下,MM 模型将节点 27 评为最高风险节点,由于其仅基于单步转移概率进行评估,未考虑攻击技术的威胁程度,而其关联的 T1203 技术攻击者经常通过该技术来实现对目标系统的入侵或控制,在历史攻击中使用频

繁,因此被 MM 模型赋予较高权重。Bayes 模型认为入口节点 121 和节点 32 风险最高,这是因为在无父节点情况下,默认将入口节点的攻击成功概率设为 1,导致入口节点风险权重最高,但这与实际情况不符,入口节点并非一定能被攻破。实验结果表明:本文的模型通过引入隐藏状态推理机制,在统一节点排序过程中充分考虑了节点所处的攻击阶段以及技术本身的风险权重,能够准确识别具有高风险权重、高转移概率的关键节点。

4.4.2 路径维度评分与识别对比

本小节通过对比各风险评估方法的路径维度,分析本文模型在多路径攻击场景下的评估能力。表 11 展示了以 workStation_1、citrixServer、subnet_1_1 为目标的技术序列、主机及路径风险值。

以 Path20 为例,如图 11 所示,该路径由 6 个连续步骤构成,攻击者首先从 Internet 发起攻击,利用 T1599 突破边界隔离,T1190 攻击 webServer_2 的外部接口,T1574 篡改其执行流程获取控制权限。随后通过经 webServer_2 借助 T1068 提权并渗透至 vpnServer_2,接着经 vpnServer_2 借助 T1210/T1110 对 citrixServer 实施远程服务利用或口令猜测,逐步控制核心主机。在三种模型下,该路径的风险排序表现存在明显差异,本文的模型认为该路径的风险值处于中上水平。尽管路径较长,但模型融合了攻击阶段间的隐藏状态转移机制与每个时间步的观测概率,能够有效缓解路径长度带来的风险稀释问题,并对 T1068、T1203 等高风险技术保持敏感响应,因此评估结果更为平衡。相比之下,MM 模型对 Path20 的风险评估偏低。该模型仅依赖于攻击技术之间的直接转移概率,未能考虑战术阶段等上下文信息,对于路径中相对低频或上下文依赖强的技术处理较弱,影响了整体的风险评分。而在 Bayes 模型中,路径长度对风险评估的影响显著。随着攻击步骤数量增加,累积概率快速衰减,导致长路径风险被严重低估。即便该路径在攻击路径上覆盖了多个关键阶段,其整体风险值依旧低于某些攻击步骤较短的路径。这说明 Bayes 模型在处理复杂多跳路径时,存在高估短链攻击、低估持久多阶段攻击的偏差。

将 Path20 与其他路径比较发现,Path24 以 0.149 56 的最高风险值位居模型排名首位,尽管该路径仅包含两项技术 T1078 与 T1055,节点数量较少,但因其技术风险权重高、观测概率大,在模型中体现出高度集中风险特征。而 Path12 虽然路径更短,但其在本文的模型中风险值依然低于 Path20 与 Path17,进一步印证对于 HMM 模型,攻击路径的长度并非决定性因素。实验结果表明:本文的模型能有效规避路径越短越危险的单一判断倾向,更关注路径内在结构、关键技术与上下文语义的联动作用,从而实现更具实战意义的整体风险评估。

4.4.3 主机维度风险聚合分析

主机作为网络中防御和资源配置的基本单元,基于主机粒度的风险评估不仅能有效整合节点风险信

表 11 实验场景 2 攻击图路径排名

Table 11 Path rankings in attack graph for scenario 2

路径	相关技术	节点 ID	主机	Ours	MM[26]	Bayes[28]
Path24	T1078,T1055	121,119	workStation_1	0.149 56(1)	9.17×10^{-3}(1)	9.43×10^{-2}(2)
Path20	T1599,T1190,T1574,T1068,T1110,T1203	45,43,41,37,54,27	webServer_2,vpnServer_2,citrixServer	0.103 69(2)	7.06×10^{-7}(20)	1.95×10^{-11}(18)
Path17	T1599,T1190,T1574,T1068,T1210,T1203	45,43,41,37,35,27	webServer_2,vpnServer_2,citrixServer	0.097 82(3)	7.88×10^{-7}(18)	1.42×10^{-12}(19)
Path12	T1659,T1203,T1021	19,110,101	subnet_1_2,subnet_1_2,subnet_1_1	0.025 96(10)	8.69×10^{-4}(5)	6.09×10^{-5}(10)
Path1	T1659,T1203	2,55	citrixServer	0.024 72(12)	9.07×10^{-3}(3)	9.43×10^{-2}(3)
Path10	T1659,T1599,T1059	11,66,126	fileServer_1,workStation_1	0.018 94(14)	8.59×10^{-4}(7)	8.00×10^{-4}(6)
Path2	T1659,T1059,T1185	7,57,61	commServer_2,dataHistorian	0.014 63(15)	8.59×10^{-4}(6)	9.70×10^{-3}(5)
Path11	T1659,T1059	15,98	subnet_1_1	0.014 02(16)	9.07×10^{-3}(2)	3.12×10^{-1}(1)
Path5	T1659,T1599,T1003,T1021,T1021	11,66,91,105,101	fileServer_1,subnet_1_2,subnet_1_1	0.010 93(17)	6.90×10^{-6}(17)	7.70×10^{-11}(17)
Path4	T1659,T1599,T1003,T1021	11,66,91,101	fileServer_1,subnet_1_1	0.008 89(18)	7.20×10^{-5}(14)	1.19×10^{-7}(13)
Path6	T1659,T1599,T1003,T1563	11,66,91,115	fileServer_1,subnet_1_1	0.007 66(20)	7.20×10^{-5}(15)	1.19×10^{-7}(14)
Path8	T1659,T1599,T1021,T1021	11,66,105,101	fileServer_1,subnet_1_2,subnet_1_1	0.006 08(21)	8.03×10^{-5}(13)	1.13×10^{-8}(16)
Path9	T1659,T1599,T1563	11,66,115	fileServer_1,subnet_1_1	0.002 57(24)	8.38×10^{-4}(8)	1.75×10^{-5}(11)

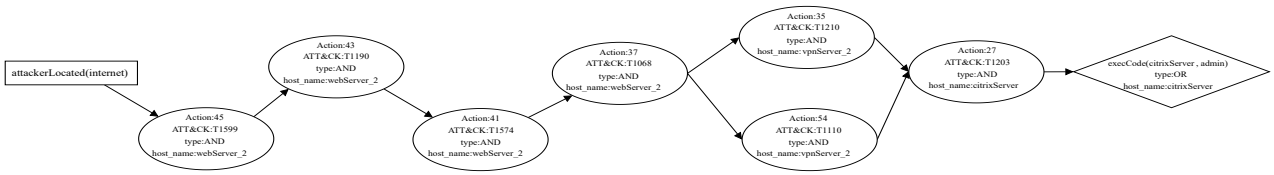

图 11　Path20 攻击路径图

Figure 11　Attack path diagram of Path20

息,降低分析复杂度,还能为高风险资产的优先加固、访问控制策略调整及资源调度提供直接指导,提升整体安全防护的效率与精准性。表 12 展示了各主机的总风险、平均风险、包含节点数及跨主机路径数等指标。

从总风险排序来看,主机 workStation_1 以 0.364 8 的风险值位居首位,显著高于其他主机。从攻击技术层面看,该主机涉及的攻击技术为 T1078、T1055 和 T1059。其中,T1078 通过滥用合法账户实现初始访问,T1055 通过进程注入规避检测,T1059 则通过脚本执行恶意指令,且 T1078 与 T1059 风险权重较高并在历史事件中频繁出现,使 workStation_1 成为攻击者优先突破的目标。分析平均风险与节点分布,workStation_1 平均每个节点的风险值达到 0.121 6,明显高于其他主机,反映出该主机不仅存在单点高危节点,同时具备较高的整体脆弱性。相比之下,webServer_2 虽包含最多的攻击节点,但平均风险仅为 0.036 9,表明其整体风险更多源于多节点累积,而非单点威胁突出。在跨主机路径分析中,vpnServer_2 参与的跨主机攻击路径数量最多,达到 9 条,高于其他主机,但其总风险值相对较低。这表明路径参与度高的节点未必具有高风险值,节点的风险评估需综合考虑其在攻击链中的路径覆盖特性与自身攻击威胁程度。

对比分析不同模型的主机风险权重,以 workStation_1 为例,本文的模型通过融合主机内攻击技术的自身风险权重与攻击技战术演进机制,将其列为风险最高的主机。相比之下,MM 模型由于忽视了在主机上执行的攻击技术威胁程度,仅依据跳转概率进行风险评估,将 webServer_2 列为最高风险主机。Bayes 模型由于路径长度增加导致累积概率减小的特性,处于攻击阶段后期的 webServer_2 主机风险值偏低。

此外,为量化不同粒度风险评估结果之间的一致性,实验基于 Top-K 排序结果引入跨尺度命中准确性指标。该指标用于衡量在不同分析尺度下,高风险实体排序结果的一致程度,本文分别从节点到路径、路径到主机和主机到路径三个映射方向进行评估:若低粒度排序结果中对应的实体在高粒度排序结果所覆盖的风险实体集合中出现,则视为一次命中。在实验中,节点层面取 Top-K(K=5),路径与主机层面分别取 Top-C(C=3)与 Top-Z(Z=3),并对三个方向的命中率取平均作为综合命中准确率。实验结果表明,本文模型的综合命中准确率达到 86.7%,明显高于 MM 模型的 34.4% 与 Bayes 模型的 41.1%,平均提升 48.95%,说明所提出的方法在不同风险评估尺度之间具有更强的高风险实体命中能力。

表 12　实验场景 2 攻击图主机排名

Table 12　Host rankings in attack graph for scenario 2

序号	主机名	平均风险	包含节点数	跨主机路径数	总风险		
					Ours	MM[26]	Bayes[28]
1	workStation_1	0.121 6	3	1	0.364 8	0.289 9(3)	1.191 3(4)
2	webServer_2	0.036 9	4	7	0.147 5	0.383 0(1)	0.000 4(14)
3	citrixServer	0.036 5	3	3	0.109 5	0.288 9 (4)	1.188 7(5)
4	vpnServer_2	0.025 4	3	9	0.076 1	0.267 6(8)	1.000 4(9)
5	subnet_1_2	0.019 4	3	3	0.058 3	0.286 4(6)	1.094 7(6)
6	subnet_1_1	0.008 9	4	6	0.035 7	0.382 0(2)	1.312 5(1)
7	commServer_2	0.015 4	2	1	0.030 7	0.190 7(11)	1.311 5 (2)
8	workStation_2	0.009 1	3	7	0.027 2	0.288 1(5)	0.086 7 (10)
9	fileServer_1	0.005 2	3	8	0.015 7	0.273 3(7)	1.057 5 (7)
10	fileServer_2	0.006 4	2	4	0.012 9	0.191 3(9)	0.052 6(11)
11	mailServer_1	0.003 4	2	3	0.006 9	0.190 9(10)	0.012 4(13)
12	webServer_1	0.002 1	2	1	0.004 6	0.185 0 (12)	1.051 0 (8)
13	dataHistorian	0.001 3	1	1	0.001 3	0.094 8(13)	0.031 2(12)

4.5 复杂度分析

为验证所提模型的计算效率,本文在实验场景2所构建的攻击图环境下,对多条不同长度的攻击路径进行了测试。实验结果表明,在实验场景2中完整执行前向算法与维特比算法的总耗时约为1.72 ms,能够在毫秒级时间内完成攻击路径的战术状态推断与动态风险评估任务。从理论上分析,模型的总体计算开销主要来自技战术概率矩阵的构建、攻击路径上的推演过程和历史事件的增量更新。战术层转移矩阵与技术层观测矩阵均基于历史攻击事件统计生成,其规模由ATT&CK框架的战术与技术数量决定,为固定常量,因此矩阵计算属于一次性离线操作,复杂度可视为$O(1)$,且在实际运行中仅涉及常数时间的索引查询。路径推演阶段,前向算法与维特比算法均以时间序列递推形式工作,每一时刻仅依赖上一步的状态概率进行更新。由于战术状态数固定,设路径长度为T,其计算复杂度线性依赖于路径长度,即$O(T)$,不会因网络规模扩大而显著增长。当新的攻击事件加入统计时,模型仅需更新相关技术的共现次数及其战术映射频次,并对矩阵执行归一化处理,由于矩阵维度固定,该增量更新的复杂度同样为常数时间$O(1)$。

5 结论

本文针对网络攻击路径建模与风险评估问题,提出了一种基于隐马尔可夫模型(HMM)的攻击路径建模与风险识别方法。首先,通过对MulVAL攻击图进行重构,生成聚焦于攻击行为的攻击图。在此基础上,引入HMM建模攻击技战术间潜在的多对一演化关系,并在此基础上推理攻击战术阶段的演化过程,提升模型对攻击阶段语义结构的表达能力。随后,设计攻击技术属性与资产个性化威胁量化模型,将其与前向算法的过程耦合,实现对复杂攻击路径的风险评估,提升模型在复杂网络环境下对关键资产的感知与适配能力。在多组复杂网络环境下的实验评估结果表明,所提方法在风险路径识别准确性和攻击链演化捕捉能力方面优于其他现有主流评估模型,展现出良好的网络威胁识别能力。

未来工作将从以下几个方面展开。第一,当前方法基于静态网络配置与一次性攻击数据进行建模与评估,未能充分反映网络资产、系统配置及攻击路径在真实环境中的动态演化。后续将引入对网络状态变化的建模机制,结合实时漏洞扫描结果与日志流,实现攻击行为的实时建模,提升方法在复杂环境下的时效性与鲁棒性。第二,针对更大规模网络环境下的运行效率问题,后续将探索在攻击路径推理与风险评估过程中引入路径剪枝策略与启发式搜索算法,以减少候选攻击路径空间和不必要的状态计算,从而进一步降低计算开销并提升模型在大规模场景下的可扩展性。第三,现有模型在参数构建与路径推理过程中依赖预设规则与固定统计特征,尚缺乏对新兴威胁模式的响应能力。未来将探索融合大语言模型(LLM)等生成式工具,从安全情报、漏洞通报等非结构化文本中自动提取技战术知识,用于动态调整模型结构与转移概率,实现对攻击策略演变的敏感感知与持续适应。

参考文献

[1] Business Verizon. 2024 Data Breach Investigations Report [R/OL]. (2024-05-01)[2025-04-25]. https://www.verizon.com/business/resources/reports/dbir/.

[2] Buchta R, Gkoktsis G, Heine F, et al. Advanced persistent threat attack detection systems: A review of approaches, challenges, and trends[J]. Digital Threats: Research and Practice, 2024, 5(4): 1-37.

[3] 周勇, 陈玺名, 程度, 等. 基于服务器主动安全的自动化红队测试技术研究[J]. 微电子学与计算机, 2026, 43(2): 126-138.
Zhou Yong, Chen Ximing, Cheng Du, et al. Research on automated red teaming technique based on server active security[J]. Microelectronics & Computer, 2026, 43(2): 126-138. (in Chinese)

[4] Ye Mai, Men Shiming, Xie Lei, et al. Detect advanced persistent threat in graph-level using competitive AutoEncoder[C]// Proceedings of 2023 2nd International Conference on Networks, Communications and Information Technology. Qinghai: ACM, 2023: 28-34.

[5] Li Zitong, Cheng Xiang, Sun Lixiao, et al. A hierarchical approach for advanced persistent threat detection with attention-based graph neural networks[J]. Security and Communication Networks, 2021, 2021(1): 9961342.

[6] 仇晶, 陈荣融, 朱浩瑾, 等. 基于溯源图的网络攻击调查研究综述[J]. 电子学报, 2024, 52(7): 2529-2556.
Qiu Jing, Chen Rongrong, Zhu Haojin, et al. A survey of network attack investigation based on provenance graph[J]. Acta Electronica Sinica, 2024, 52(7): 2529-2556. (in Chinese)

[7] Cai Yongxin, Qiu Jing, Zhang Fan, et al. A knowledge extraction framework on cyber threat reports with enhanced security profiles[C]//Proceedings of the 48th international ACM SIGIR conference on research and development in information retrieval. Padua: ACM, 2025: 326-336.

[8] Sheyner O, Haines J, Jha S, et al. Automated generation

and analysis of attack graphs[C]//Proceedings of 2002 IEEE Symposium on Security and Privacy. Berkeley: IEEE, 2002: 273-284.

[9] Ou Xinming, Govindavajhala S, Appel A W. MulVAL: A logic-based network security analyzer[C]//Proceedings of the 14th Conference on USENIX Security Symposium. Baltimore: USENIX Association, 2005: 8.

[10] Zhou Weidong, Xia Chunhe, Feng Nan, et al. AIDE: Attack inference based on heterogeneous dependency graphs with MITRE ATT&CK[C]//Proceedings of 2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications. Sanya: IEEE, 2024: 410-417.

[11] Saint-Hilaire K A. Automatic Generation of Attack and Remediation Graphs[D]. Montreal: Ecole Polytechnique de Montreal, 2025.

[12] 胡钢, 卢志宇, 王乐萌, 等. 基于复杂网络多阶邻域贡献度的节点重要性序结构辨识[J]. 电子学报, 2023, 51(7): 1956-1963.
Hu Gang, Lu Zhiyu, Wang Lemeng, et al. Identification of node importance order structure based on multi-order neighborhood contribution of complex network[J]. Acta Electronica Sinica, 2023, 51(7): 1956-1963. (in Chinese)

[13] Wang Lingyu, Islam T, Long Tao, et al. An attack graph-based probabilistic security metric[C]//Proceedings of the 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security Data and Applications Security. London: Springer, 2008: 283-296.

[14] Homer J, Xinming Ou, Schmidt D, et al. A sound and practical approach to quantifying security risk in enterprise networks[R]. Moscow: University of Idaho, 2009: 1-15.

[15] Wang Lingyu, Singhal A, Jajodia S. Toward measuring network security using attack graphs[C]//Proceedings of 2007 ACM Workshop on Quality of Protection. Alexandria: ACM, 2007: 49-54.

[16] Noel S, Jajodia S. Managing attack graph complexity through visual hierarchical aggregation[C]//Proceedings of 2004 ACM Workshop on Visualization and Data Mining for Computer Security. Washington: ACM, 2004: 109-118.

[17] Scarfone K, Mell P. An analysis of CVSS version 2 vulnerability scoring[C]//Proceedings of 2009 3rd International Symposium on Empirical Software Engineering and Measurement. Lake Buena Vista: IEEE, 2009: 516-525.

[18] Mell P, Scarfone K, Romanosky S. A complete guide to the common vulnerability scoring system version 2.0[R]. Gaithersburg: NIST, 2007.

[19] 董洋, 历超, 杨英奎, 等. 基于漏洞信息和攻击图的信息路径风险评分系统[J]. 自动化技术与应用, 2024, 43(10): 122-125.
Dong Yang, Li Chao, Yang Yingkui, et al. Information route risk scoring system based on vulnerability information and attack graphs[J]. Techniques of Automation and Applications, 2024, 43(10): 122-125. (in Chinese)

[20] MITRE Corporation. ATT&CK[EB/OL]. [2025-05-30]. https://attack.mitre.org/.

[21] Swiler L P, Phillips C, Ellis D, et al. Computer-attack graph generation tool[C]//Proceedings of DARPA Information Survivability Conference and Exposition II. DISCEX'01. Anaheim: IEEE, 2001: 307-321.

[22] Zenitani K. Attack graph analysis: An explanatory guide[J]. Computers & Security, 2023, 126: 103081.

[23] Jing J T W, Yong L W, Divakaran D M, et al. Augmenting MulVAL with automated extraction of vulnerabilities descriptions[C]//Proceedings of TENCON 2017 - 2017 IEEE Region 10 Conference. Penang: IEEE, 2017: 476-481.

[24] Tayouri D, Baum N, Shabtai A, et al. A survey of MulVAL extensions and their attack scenarios coverage[J]. IEEE Access, 2023, 11: 27974-27991.

[25] Gao Jianbo, Zhang Baowen, Chen Xiaohua, et al. Ontology-based model of network and computer attacks for security assessment[J]. Journal of Shanghai Jiaotong University (Science), 2013, 18(5): 554-562.

[26] Zhang Jingci, Zheng Jun, Zhang Zheng, et al. ATT&CK-based advanced persistent threat attacks risk propagation assessment model for zero trust networks[J]. Computer Networks, 2024, 245: 110376.

[27] 杨宏宇, 袁海航, 张良. 一种基于主机重要度的网络主机节点风险评估方法[J]. 北京邮电大学学报, 2022, 45(2): 16-21.
Yang Hongyu, Yuan Haihang, Zhang Liang. A risk assessment method of network host node with host importance[J]. Journal of Beijing University of Posts and Telecommunications, 2022, 45(2): 16-21. (in Chinese)

[28] Zheng Dongyang, Gao Chengliang, Xing Jiaxu, et al. Dynamic analysis of attack paths based on Bayesian attack graph[C]//Proceedings of the 3rd international conference on cyberspace simulation and evaluation. Shenzhen: Springer, 2024: 60-76.

[29] Homer J, Zhang Su, Ou Xinming, et al. Aggregating vulnerability metrics in enterprise networks using attack graphs[J]. Journal of Computer Security, 2013, 21(4): 561-597.
[30] MITRE Corporation. What is ATT&CK?[EB/OL]. (2023-07-19)[2025-04-08]. https://attack.mitre.org/resources/.
[31] Strom B, Applebaum A, Miller D, et al. MITRE ATT&CK: Design and philosophy[R]. Bedford: MITRE, 2020.
[32] Rabiner L R. A tutorial on hidden Markov models and selected applications in speech recognition[J]. Proceedings of the IEEE, 1989, 77(2): 257-286.

作者简介

仇 晶 女,1983年5月出生于河北省石家庄市,现为广州大学网络空间安全学院教授,博士生导师。主要研究方向为网络安全、人工智能及大数据安全。中国电子学会会员编号:E190035636M。
E-mail: qiujing@gzhu.edu.cn

农李晨 女,2002年8月出生于广西壮族自治区百色市,现为广州大学网络空间安全学院硕士研究生。主要研究方向为攻击图风险评估、攻击预测。
E-mail: 2112433038@e.gzhu.edu.cn

孙一飞 男,1996年5月出生于安徽省马鞍山市,现为广州大学网络空间安全学院在站博士后。2024年获广东工业大学计算机科学与技术博士学位。主要研究方向为边缘计算、车联网、边缘智能。
E-mail: asunyifei@gzhu.edu.cn

操晓春 男,1980年3月出生于安徽省安庆市,现为中山大学网络空间安全学院院长、校学术委员会委员、教授。主要研究方向为人工智能基础研究、网络空间内容安全应用研究等。中国电子学会会员编号:E190013018F。
E-mail: caoxiaochun@mail.sysu.edu.cn

陈玺名 男,1996年11月出生于辽宁省营口市,现为广州大学网络空间安全学院博士研究生。主要研究方向为威胁预测与风险评估。
E-mail: 2112019039@e.gzhu.edu.cn

张睿智 男,2001年9月出生于山东省泰安市,现为广州大学网络空间安全学院硕士研究生。主要研究领方向为基于攻击图的安全分析。
E-mail: 2112433184@e.gzhu.edu.cn