基于贝叶斯攻击图的校园局域网入侵路径预测研究

王 慧[1]
WANG Hui

摘 要 当前，校园局域网遭受入侵攻击呈现出多阶段且可持续的特性，这种动态性导致网络中的节点关系不再局限于静态的低阶成对关联。传统的预测方法仅关注于低阶成对关联，难以适应这种动态变化。在多阶段入侵过程中，难以挖掘节点之间的高阶联系，从而限制了入侵路径预测的准确性。为此，文章提出了一种新的基于贝叶斯攻击图的校园局域网入侵路径预测方法。该方法构建了校园局域网入侵贝叶斯攻击图，该图能够明确局域网入侵的因果关系以及节点间高阶联系。通过利用节点间的高阶关联性预测各个局域网节点被入侵的概率。在此基础上，结合贝叶斯攻击图进一步构建校园局域网入侵路径预测模型。该模型将各个节点被入侵的概率作为模型的输入，通过量化这些概率来识别校园局域网中存在的脆弱点，再将这些脆弱点连接起来形成潜在的入侵路径，输出校园局域网入侵路径的预测结果。实验结果表明，该方法在预测校园局域网入侵路径方面具有更高的准确性，实际应用效果也更加显著。这一研究成果为提升校园局域网的安全防护能力提供了有力的技术支撑。

关键词 贝叶斯攻击图；校园局域网；入侵路径；预测方法

doi：10.3969/j.issn.1672-9528.2025.02.023

0 引言

随着信息技术的飞速发展，校园局域网作为学校信息化建设的重要基础设施，承载着教学、科研、管理等多方面的重要任务。然而，随着网络环境的日益复杂，校园局域网面临着来自各方面的安全威胁，如黑客攻击、病毒传播、信息窃取等。这些安全威胁不仅可能导致数据的丢失和损坏，还可能对学校的正常运营和师生的隐私造成严重影响。为了有效应对这些安全威胁，校园局域网入侵路径预测研究显得尤为重要。入侵路径预测旨在通过分析网络中的节点、漏洞、攻击手段及其相互关系，预测攻击者可能采取的入侵路径，从而提前采取相应的防护措施，降低被攻击的风险。这一研究不仅有助于提升校园局域网的安全性，还能为其他类似网络环境的安全防护提供有益的参考。

当前，针对校园局域网入侵路径预测这一研究课题，学术界已取得了一系列显著成果。例如，卓群忠[1]提出了一种基于深度神经网络的预测方法，该方法充分利用深度神经网络在特征学习和分类方面的强大能力，对网络流量数据进行深度建模与分析，旨在揭示并预测潜在的入侵路径。然而，深度神经网络模型往往基于固定的网络结构构建，在校园局域网入侵攻击的动态背景下，这种固定结构无法很好地适应不断变化的攻击模式，导致模型在面对这种新攻击时预测能力不足。另一方面，孙澄等人[2]提出了基于网络防御知识图谱的预测方法。该方法将威胁、脆弱性、资产等离散的安全数据提炼为互相关联的安全知识，并深入分析攻击者的行为模式，进而在知识图谱中建立起攻击者实体与设备实体之间的复杂关系。通过计算不同攻击路径的发生概率，该方法能够预测并分析可能的入侵路径。但在可持续的入侵攻击中，攻击者可能会利用多个看似不相关的脆弱点（涉及高阶关联）进行攻击，但该方法只关注到低阶的直接关联，从而在知识图谱中遗漏重要的关系信息，导致计算出的概率与实际情况存在较大偏差，从而影响预测准确性。为解决上述问题，特别是节点间高阶关联特征难以捕捉导致的入侵路径预测准确性下降问题，本文创新性地结合贝叶斯攻击图的优势，设计了一种全新的校园局域网入侵路径预测方法。该方法旨在通过贝叶斯攻击图更准确地揭示网络中的因果关系及节点间的高阶联系，从而提升入侵路径预测的准确性和可靠性。

1 局域网入侵路径预测方法设计

1.1 校园局域网入侵贝叶斯攻击图构建

当前，校园局域网面临着复杂多变的入侵攻击态势，这些攻击往往不是单一的、瞬间的行为，而是多阶段、持续性的过程。这种特性使得网络中的节点关系变得异常复杂和动态，不像此前只是简单的、静态的低阶成对关联。传统的入

1. 天津医学高等专科学校 天津 300222

侵路径预测方法因仍局限于静态网络结构和低阶成对关联的分析，未能充分考虑网络环境的动态性和节点间的高阶联系，因此难以准确捕捉攻击者在整个网络中的行动轨迹及潜在威胁[3]。而贝叶斯攻击图能够将这种多阶段的攻击过程以概率图的形式表示出来。通过构建贝叶斯攻击图，能够明确校园局域网中各个节点被攻击的因果关系[4]。这种因果关系的确定有助于准确地找到入侵的源头和路径。贝叶斯攻击图利用贝叶斯定理，根据已知的网络状态、节点属性和历史攻击数据等信息，预测各个节点被入侵的概率，从而挖掘出节点间的高阶联系。贝叶斯攻击图如图 1 所示。

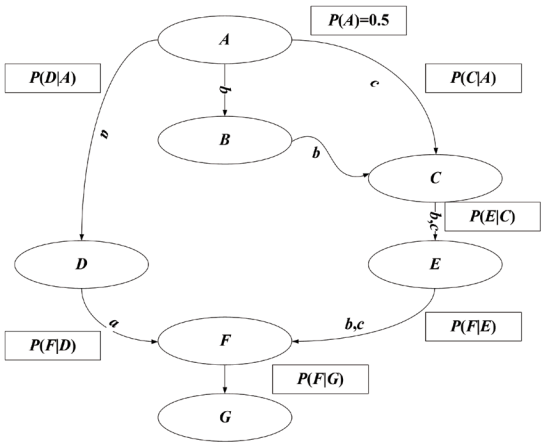

图 1 贝叶斯攻击图

图 1 中，*A*、*C*、*F* 为工控机 1、2、3；*B*、*D*、*E* 为交换机 1、2、3；*G* 为校园局域网的入侵目标；*P*(*A*) 为 *A* 入侵点的概率；*P*(*C*|*A*) 为 *C* 到达 *A* 的概率；*P*(*E*|*C*) 为 *E* 到达 *C* 的概率；*P*(*F*|*E*) 为 *F* 到达 *E* 的概率；*P*(*F*|*G*) 为 *F* 到达 *G* 的概率；*P*(*F*|*D*) 为 *F* 到达 *D* 的概率；*P*(*D*|*A*) 为 *D* 到达 *A* 的概率[5]；*a*、*b*、*c* 为贝叶斯攻击变量。对于入侵者来说，每个设备都会出现不可避免的漏洞，因此通过攻击向量、攻击复杂度和所需权限等级以及用户交互等可利用性的指标要素来衡量节点之间高阶联系，从而预测局域网入侵路径。

通过构建贝叶斯攻击图，能够预测校园局域网中各个节点被入侵的概率。这些概率值反映了攻击者利用漏洞进行入侵的可能性，是后续分析的基础。

1.2 基于贝叶斯攻击图的局域网入侵路径预测

贝叶斯攻击图能够有效地表示网络系统中的节点、漏洞、攻击路径及其之间的依赖关系。通过贝叶斯攻击图能够进一步构建入侵路径预测模型。该模型通过综合考虑节点间的依赖关系和漏洞的组合利用情况，能够更准确地预测攻击者可能采取的攻击路径。在构建入侵路径预测模型的过程中，各个节点被入侵的概率作为模型的输入，通过贝叶斯推理方法，可以计算出不同攻击路径的威胁程度，以反映网络系统中新出现的漏洞或攻击方式[6]。通过模型预测，网络管理员不仅可以了解哪些节点更容易被攻击，还能掌握攻击者可能通过哪些路径入侵，从而有针对性地制定和优化防御策略。此外，模型还具备动态更新能力，能够根据新出现的漏洞或攻击方式，及时调整预测结果，确保网络安全的持续性和有效性[7]。

在上述建立的校园局域网入侵贝叶斯攻击图中，每个被入侵节点与被入侵路径都被赋予了相应的概率值，反映了攻击者利用漏洞进行入侵的可能性。通过量化这些概率，校园网络管理员可以更加准确地评估不同攻击路径的威胁程度，从而判别校园局域网中存在的脆弱点，将各个脆弱点连接成一个入侵路径，构建校园局域网入侵路径预测模型。当校园局域网中出现新的漏洞或攻击方式时，该模型能够迅速捕捉这些变化，并相应地调整预测结果。在贝叶斯攻击图中，各个入侵节点的漏洞情况分别表示为：

$$B_w=\begin{cases}\min\left(1.08\cdot(E_{xp}+I),10\right),S=H\\ \min\left(E_{xp}+I,10\right),S=U\end{cases} \tag{1}$$

$$E_{xp}=V\cdot\zeta\cdot R\cdot\omega \tag{2}$$

$$I=\begin{cases}7.52\cdot(I_{SC}-0.029)-3.25\times\left((I_{SC}-0.02)^{15}\right),S=H\\ 6.42\cdot I_{SC},S=U\end{cases} \tag{3}$$

$$I_{SC}=1-\left((1-\zeta)\cdot(1-i)\cdot(1-V)\right) \tag{4}$$

式中：B_w 为贝叶斯攻击图中入侵节点漏洞分值；E_{xp} 为漏洞可利用因子；I 为漏洞影响因子；S 为漏洞影响范围；H 为被入侵者使用的漏洞影响范围超出原本授权资源；U 为被入侵者使用的漏洞影响范围在同一环境下的资源；V 为入侵向量；ζ 为入侵复杂度；R 为入侵所需权限等级；ω 为用户交互指标；I_{SC} 为入侵的临时中间变量；i 为完整性分数。将 B_w 设置在 [0, 10] 之间，表示漏洞 - 入侵的危害程度[8]。其中，低危漏洞分值在 [0, 4) 之间，中危漏洞分值在 [4, 7) 之间，高危漏洞分值在 [7, 9) 之间，严重漏洞分值在 [9, 10] 之间。校园局域网入侵行为能够利用入侵目标的弱点，获得不同级别的权限，实现入侵意图。本文根据 B_w、E_{xp}、I、I_{SC} 等指标的变化情况，建立校园局域网入侵路径预测模型，表达式分别为：

$$Z\left(C\middle|A\right)=\frac{P\left(C=c\middle|A=a\right)\cdot P\left(A\middle|C\right)}{B_w\delta P(C)} \tag{5}$$

$$\delta=\sum_{C_1,C_2,\ldots,C_n}P\left(C_1,C_2,\ldots,C_n\right) \tag{6}$$

式中：$Z(C|A)$ 为校园局域网入侵路径预测模型表达式；$P(C)$ 为节点 C 被入侵的概率；$P(A|C)$ 为节点 C 被入侵的后验概率；δ 为概率函数；$C_1, C_2, \cdots, C_n$ 为隶属于 C 的随机变量；$P(C=c|A=a)$ 为节点被入侵的联合概率分布的链规则；将 $C=c$ 作为假设变量；$A=a$ 作为证据变量[9]。通过贝叶斯攻击图预测情况，了解攻击者的攻击意图和可能的攻击路径，从而有针对性地制定和优化防御策略[10]。

2 实验

为验证本文所设计的方法是否满足校园局域网入侵路径预测的需求，对上述方法进行了实验分析。实验结果的呈现方式是将本文设计的基于贝叶斯攻击图的路径预测方法与基于深度神经网络的路径预测方法、基于网络防御知识图谱的路径预测方法进行对比。

2.1 实验过程

本次实验在实验室内搭建了一个模拟的校园局域网环境，该网络被划分为 DMZ 区域和 Inside 区域，并通过防火墙进行隔离。在 DMZ 区域中，部署 1 台服务器；而在 Inside 区域，则部署了 4 台服务器。在这个局域网环境中，设定了一个入侵场景，即入侵者使用主机 H0 进行远程入侵。DMZ 区域中的 H1 主机与外网直接相连，并且具备访问 Inside 网络中 H2、H3、H4 三台主机的权限，从而构成了一个完整的校园局域网络结构。Inside 区域的主机无法直接与外部网络相连，但 H2 和 H3 可以访问 H4，而 H4 则可以访问一个假定的 H5。这样设置成了 H0、H1、H2、H3、H4、H5 的网络连接结构，具体如图 2 所示。

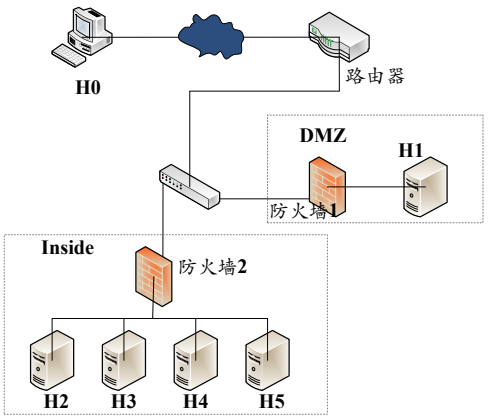

图 2 校园局域网结构示意图

图 2 中，H0 为入侵者；H1 为网络服务器；H2 为 Ftp 服务器；H3 为主机 1；H4 为主机 2；H5 为数据库服务器。将 H0~H5 排列组合，H0 作为入侵者，H5 为被入侵目标，预测最终入侵到 H5 的所有路径，如表 1 所示。PATH1 为口令非法入侵形式；PATH2 为 IP 地址盗用入侵形式；PATH3 为病毒、木马入侵形式；PATH4 为系统漏洞入侵形式；PATH5 为网络扫描器攻击形式；PATH6 为远程控制入侵形式；PATH7 为无线网络攻击形式；PATH8 为移动核心网络攻击形式。a4 的入侵复杂度为高等；a3 的入侵复杂度为中等；a1、a7、a10 的入侵复杂度为低等；a2、a5、a6、a8、a9 的入侵复杂度较低。本次实验将 PATH1、PATH2、PATH3、PATH4 作为校园局域网的入侵路径。PATH5、PATH6、PATH7、PATH8 作为校园局域网入侵的混淆路径，判断入侵路径预测的准确性。

表 1 预测路径

路径编号	入侵点	名称	路径
PATH1	a1,a3,a7,a10	H1, H2, H4, H5	(H1,a1) → (H2,a3) → (H4,a7) → (H5,a10)
PATH2	a1,a2,a7,a10		(H1,a1) → (H2,a2) → (H4,a7) → (H5,a10)
PATH3	a1,a3,a8,a10		(H1,a1) → (H2,a3) → (H4,a8) → (H5,a10)
PATH4	a1,a4,a8,a10	H1, H3, H4, H5	(H1,a1) → (H3,a4) → (H4,a8) → (H5,a10)
PATH5	a1,a4,a9,a10		(H1,a1) → (H3,a4) → (H4,a9) → (H5,a10)
PATH6	a1,a5,a8,a10		(H1,a1) → (H3,a5) → (H4,a8) → (H5,a10)
PATH7	a1,a5,a9,a10		(H1,a1) → (H3,a5) → (H4,a9) → (H5,a10)
PATH8	a1,a6,a10	H1, H4, H5	(H1,a1) → (H4,a6) → (H5,a10)

2.2 实验结果

在上述实验条件下，选取 PATH1 至 PATH8 路径进行预测分析。实验中，横坐标代表服务器名称，纵坐标表示校园局域网入侵路径有效预测的概率。在保持其他条件一致的前提下，对比了基于深度神经网络的路径预测、基于网络防御知识图谱的路径预测，以及本文设计的基于贝叶斯攻击图的路径预测方法的性能。使用基于深度神经网络的校园局域网入侵路径预测方法后，预测结果如图 3 所示。

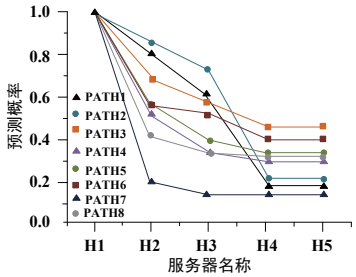

图 3 深度神经网络预测结果图

如图 3 所示，该方法在服务器 H1 上的路径预测准确性较高，接近 1.0。然而，随着服务器数量的增加，预测准确性在 H4 和 H5 上出现了较大波动，波动范围在 0.1 到 0.6 之间。特别是 PATH7 的预测准确性较低，而 PATH3 虽然预测准确性较高，但整体预测效果波动性较大，这可能对校园局域网的安全运行构成潜在威胁。接下来，采用基于网络防御知识图谱的校园局域网入侵路径预测方法，预测结果如图 4 所示。PATH1、PATH2、PATH3 以及 PATH7 的路径预测结果展现出了较高的准确性；相比之下，PATH4、PATH5、PATH6 以及 PATH8 的预测准确性则较低。在实验情境下，根据预测结果

得出的可能入侵路径为 PATH1、PATH2、PATH3、PATH7，但这与实际情况并不完全吻合。这一结果表明，使用基于网络防御知识图谱的校园局域网入侵路径预测方法时，预测结果存在偏差，因此有必要对其进行进一步的优化。

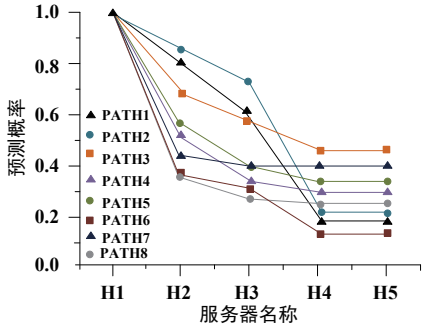

图 4 网络防御知识图谱预测结果图

为了对比和验证，采用了本文设计的基于贝叶斯攻击图的校园局域网入侵路径预测方法，并得出了相应的预测结果，如图 5 所示。

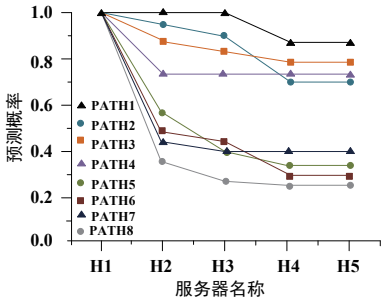

图 5 贝叶斯攻击图预测结果图

如图 5 所示，PATH1、PATH2、PATH3、PATH4 的入侵路径预测准确性较高，而 PATH5、PATH6、PATH7、PATH8 的预测准确性相对较低。在实验情境下，选择与 PATH1、PATH2、PATH3、PATH4 相符的路径作为潜在的入侵路径，这一结果与实际情况相吻合。这表明，运用本文所设计的基于贝叶斯攻击图的校园局域网入侵路径预测方法，可以获得相对较高的预测准确性。本文方法的优势在于构建校园局域网入侵的贝叶斯攻击图。这一构建过程不但明确了局域网入侵的因果关系，而且还揭示了节点间的高阶联系。利用这些高阶关联性，能够更加精准地预测各个局域网节点被入侵的概率。在此基础之上，进一步结合贝叶斯攻击图构建的入侵路径预测模型，可以动态地识别网络中的脆弱点，将这些脆弱点串联起来从而形成潜在的入侵路径，使得预测结果更加准确可靠。

3 结语

当前，校园局域网正面临着一种新型的安全挑战，即入侵攻击展现出多阶段且持续不断的特征。这种动态的攻击模式打破了网络中节点间原有的静态、低阶的相互关联模式。传统的预测手段局限于分析这些低阶的成对关系，无法有效应对这种高度动态的攻击变化。特别是在多阶段的入侵过程中，由于难以捕捉和解析节点间复杂的高阶关联性，导致对入侵路径的预测准确性显著降低。针对这一现状，本文提出了一种创新的基于贝叶斯攻击图的校园局域网入侵路径预测方法。该方法通过构建贝叶斯攻击图，不仅揭示了局域网入侵的因果关系，还深入挖掘了节点间的高阶联系，从而实现了对入侵路径的精准预测。在攻击图建立、预测模型构建等关键环节，充分利用了贝叶斯攻击图的优势，成功识别并刻画了局域网中的潜在入侵点与漏洞，以及它们之间的复杂关系。实验结果表明，本文所提出的方法相较于传统方法，在预测准确性上有了显著提升，为校园局域网的安全防护提供了更为有力的技术支撑，确保了校园网络的安全稳定运行。

参考文献：

[1] 卓群忠 . 基于深度神经网络的网络入侵路径预测数学建模研究 [J]. 宁夏师范学院学报 ,2023,44(4):80-87.

[2] 孙澄 , 胡浩 , 杨英杰 , 等 . 基于网络防御知识图谱的 0day 攻击路径预测方法 [J]. 网络与信息安全学报 ,2022,8(1):151-166.

[3] 朱光明 , 卢梓杰 , 冯家伟 , 等 . 基于攻击上下文分析的多阶段攻击趋势预测 [J]. 计算机技术与发展 ,2023,33(7):104-110.

[4] 钱芬 . 基于轻量级梯度提升机器学习算法的家庭物联网攻击预测模型 [J]. 合肥师范学院学报 ,2023,41(6):128-132.

[5] 蔡娟 , 兰娅勋 , 刘源 . 基于 GBDT 优化算法的局域网入侵定位与检测研究 [J]. 计算机测量与控制 ,2023,31(10):90-96.

[6] 钱建波 , 于正永 , 贾建强 . 一种高职校园网络安全部署解决方案 : 以江苏电子信息职业学院为例 [J]. 网络安全技术与应用 ,2024(5):83-85.

[7] 宋正荣 , 夏美武 . 高校威胁情报融合共享建设与应用研究 : 高校网络安全综合治理 [J]. 电脑知识与技术 ,2023,19(29):94-96.

[8] 吴剑俪 , 杨华 , 张亮 . 基于 HCL 仿真的跨校区校园网 IPv6 安全研究与应用实现 [J]. 杭州师范大学学报 (自然科学版), 2023, 22(3):319-328.

[9] 常晓洁 , 向艳 , 屠佳琪 . 基于 S-OCL 的校园网认证系统中 LDAP 漏洞检测方法 [J]. 网络安全和信息化 ,2022(4):122-127.

[10] 陆振展 , 倪胜 . 静动态路由相结合的多院区三类业务网逻辑隔离和安全域策略设计与实现 [J]. 网络安全技术与应用 , 2024(9):19-25.

【作者简介】

王慧（1979—），女，天津人，硕士研究生，副教授，研究方向：计算机应用、信息技术、网络安全、信息化建设、职业教育等。

（收稿日期：2024-11-01）