基于知识图谱与HMM的入侵路径分析方法

李志辉,王德军*,孙贝尔
(中南民族大学 计算机科学学院,武汉 430074)

摘 要 入侵路径分析在深入理解入侵者的危险行为和改进安全防护系统方面具有重要意义.提出了一种基于知识图谱与隐马尔科夫链的入侵路径分析方法.该方法将安防区域划分为最小单元的安防节点,并将入侵路径抽象为知识图谱.同时,通过隐马尔科夫链对入侵事件的发生与发展进行处理,并计算出安防节点的安防效能.与传统的深度优先遍历算法相比,所提出的方法时间复杂度为O(n),且满足实际入侵行为的选择过程.实例分析表明:该方法能够直观有效地反映出入侵者的入侵路径,并计算出不同入侵路径的安防效能,从而为现有的安防系统提供全面且科学的分析指导.

关键词 入侵路径分析;隐马尔科夫链;知识图谱
中图分类号 TP391.4 **文献标志码** A **文章编号** 1672-4321(2025)02-0226-11
doi:10.20056/j.cnki.ZNMDZK.20250212

Intrusion path analysis method based on knowledge graph and HMM

LI Zhihui, WANG Dejun*, SUN Beier
(College of Computer Science, South-Central Minzu University, Wuhan 430074, China)

Abstract Intrusion path analysis is of great significance in understanding the dangerous behavior of intruders and improving security protection systems. An intrusion path analysis method based on knowledge graph and hidden Markov chain is proposed . The security area is divided into the smallest unit of security nodes, and the intrusion path is abstracted into a knowledge graph. At the same time, the occurrence and development of intrusion events are processed through the hidden Markov chain, and the security efficiency of the security node is calculated. Compared with the traditional depth-first traversal algorithm, the proposed method has a time complexity of O(n) and satisfies the selection process of the actual intrusion behavior. The case analysis shows that the method can intuitively and effectively reflect the intruder's intrusion path and calculate the security efficiency of different intrusion paths, so as to provide comprehensive and scientific analysis guidance for the existing security system.

Keywords intrusion path analysis; hidden Markov chain; knowledge graph

安全防范系统是一种复合电子系统,旨在保护安防目标的安全[1].根据《国家安全防范工程技术规范》的规定,文物保护单位、博物馆、银行和民用机场等高风险对象必须配备相应的安全防范系统.然而,付萍等[2]指出如果不能准确评估安防系统,可能会导致过度保护和资源浪费,或者导致安防目标未得到适当的保护.

入侵路径是对入侵者入侵行为的分步描述,通过模拟入侵行为,分析安全防范系统的脆弱性,并提出改进建议.目前,主流的入侵路径分析方法有抽象建模和模拟仿真两种.模拟仿真通过对安防系统进行精确建模,并进行大量的计算机仿真实验,得出系统的最脆弱路径,是一种概率评估模型.抽象建模将安防系统抽象为区域或节点,有利于分析路径节点之间的关系,计算入侵路径,从入侵者的角度进行分析.KEREM[3]综述了入侵路径研究的现

收稿日期 2023-08-30
* **通信作者** 王德军(1974-),男,副教授,博士,研究方向:人工智能,E-mail:dejun@scuec.edu.cn
基金项目 国家重点研发计划资助项目(2020YFC1522900)

状，入侵路径研究的重点之一是攻击图，如何依靠入侵模型进行分析，决定了评估的准确性，也是当前研究的主流.

目前，有许多用于安防入侵路径分析的模型.例如，DU[4]在传统ASD入侵序列图的基础上提出了一种可视化评估算法，直接将安防系统平面图建模，计算最薄弱的入侵路径.但是使用平面图分析入侵路径忽视了各区域的安防功能差异，同时成本过高.WANG[5]引入区域模块划分安防系统，并制定了一系列划分依据，形成安防系统的路径模型.但是没有考虑到各区域中的安防子系统要素.HU[6]认为现有研究主要集中于理想攻击场景中的路径预测，提出了多步攻击路径预测方法.除了模型外，入侵路径的研究还包括路径数量评估[7]、路径长度的中位值分析[8]和平均路径长度度量最短耗时路径预测[9]等.目前针对安防效能的评估集中于对区域的划分与指标评估，没有考虑安防子系统的实际运行效能.

本文将首先研究传统的敌手序列图，并提出一种基于知识图谱的安防系统图解模型，用来替代敌手序列图.然后，结合隐马尔可夫链模型，计算各入侵路径的安防效能，并对路径计算方法进行优化改进.通过使用知识图谱来描述入侵路径，各路径节点的安防效能可以实时更新，最薄弱的入侵路径也会随之更新，从而能够实时评估入侵路径的安防效能.具体流程如图1所示.

1　入侵路径图解模型

1.1　传统ASD模型

桑迪亚实验室在二十世纪七十年代开始了安全防范系统的效能评估相关研究，并于1998年提出了ASSESS评估分析工具[10].该工具利用路径模型的探测分析方法来评估安防效能，并引入了敌手序列图的概念.敌手序列图的核心是构建安防系统的图解模型，用于表示入侵者完成盗窃或破坏行为的路径以及该路径上的安防系统部件.敌手序列图的优势在于，通过图解模型可以直观地表示安全防范系统的组成部分，清晰地反映安全防范系统的纵深防御.入侵者是由外向内逐层突破的.此外，各安防系统的组成部件相互影响，形成一条入侵路径，因此对安防系统的效能分析不再局限于局部区域的评估，而是考虑了整体性.因此，敌手序列图是一种可靠的描述安防系统的方法.

如图2所示，敌手序列图是一种描述安全防范系统的图解模型，用于表示入侵者的入侵行为和安防系统的应对.敌手序列图将安防系统分割成不同的地理区域，称为保护层.然后通过研究分析找出不同保护层之间的路径元件，即连接不同保护层的路径.这些路径元件组成了安防系统的图解模型.

1.2　传统ASD模型缺点

入侵行为的完整过程包括入侵者从当前保护层进入下一保护层时选择路径元件，并通过破坏或

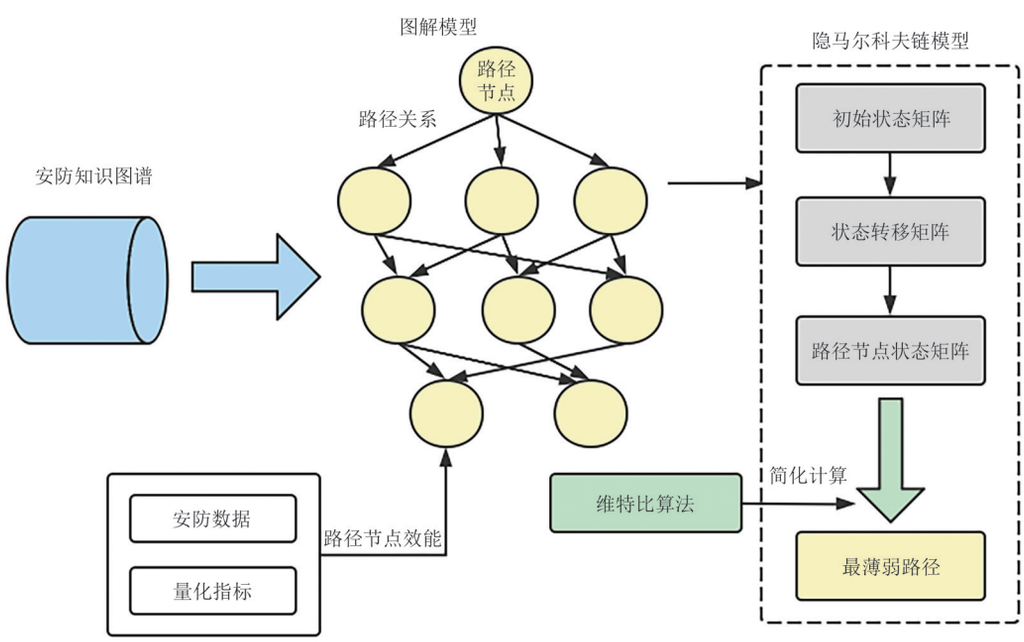

图1　入侵路径评估流程

Fig. 1　Intrusion path assessment process

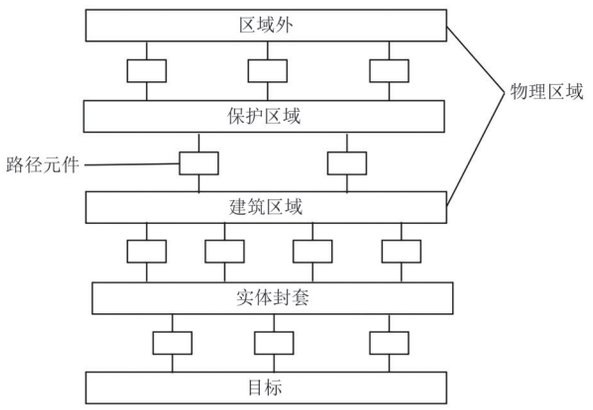

图2 敌手序列图

Fig. 2 Adversary sequence diagram

绕过路径元件来使其失效,最终达到目标区域.因此,敌手序列图可以用来描述入侵者从起点到目标区域的所有实现路径.

在实际情况中,安全防范系统的建设往往是复杂多样的.不同的保护层可能相互嵌套,共用墙体等,这使得入侵者可以绕过多个保护层直接到达目标区域.此外,一个安防设施通常有多个目标,需要建立相应的安防子系统.然而,这些安防子系统与区域之间并不是完全独立的,可能存在部分重叠.传统的敌手序列图无法准确反映这些情况,因为其要求对每个目标进行分析并生成相应的图解模型.此外,传统的敌手序列图注重入侵者的转移行为,简化了保护层之间的安防系统,导致无法真实反映安防系统的情况.因此,有必要改进传统的图解模型,以更准确地模拟和评估安防系统.

1.3 基于知识图谱的图解模型

在实际的安全防范系统建设中,安防基础设施由多个重要的人员和设备组成,而安防系统的保护目标也往往不止一个.然而,传统的图解模型在处理多目标保护时存在两个问题:首先,它忽视了区域内的安防元素,只关注区域之间的转移安防元素,无法准确反映安防系统的真实情况;其次,不同安防目标的安防系统并不是独立的,存在共用和重合的部分,因此对每个安防目标都构建图解模型并不合理.

为了解决这些问题,本研究提出了一种基于知识图谱的安防系统模型构建方法[11].知识图谱可以包含大量的数据,并且其图结构的特点可以直观地表示节点之间的关系.因此,本文利用前面提出的安防知识图谱,将路径节点作为图谱的节点,并根据这些节点的空间关系构建路径节点之间的关系.通过构建这样的知识图谱,本文可以更加细致地建立安防系统的图解模型,典型案例如图3所示.

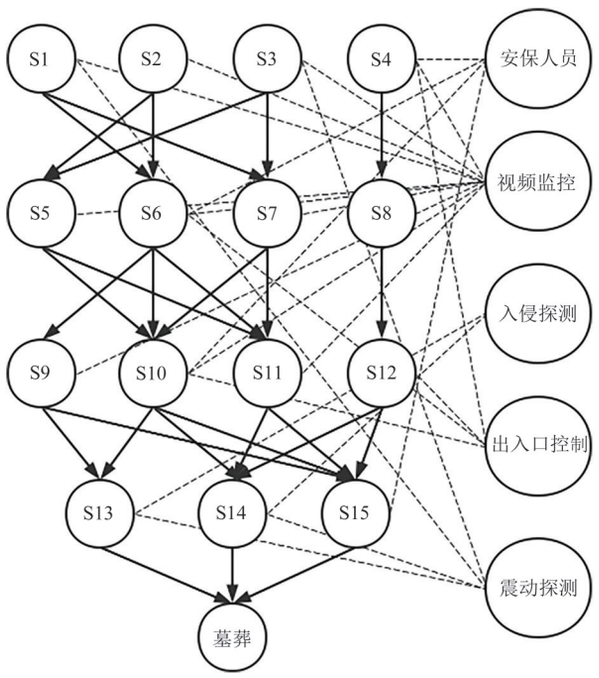

图3 基于知识图谱的图解模型

Fig. 3 Graphic modeling based on knowledge graph

与传统的图解模型相比,该图解模型将安防系统的各区域和安防元素抽象为节点和边,以直观的方式展示了安防系统中的路径.相比传统模型,该图解模型具有以下优势:传统模型通常先确定目标,然后根据已知目标确定流程.然而,在实际情况中,入侵者通常不会仅仅确定一个单一目标,而是根据情况选择多个目标.这对应到图谱中不同目标之间的共享区域和共用安防元素.因此,该图解模型适用于多目标的安防系统.其次,由于知识图谱实际上是一种图数据库,可以实时更新图解模型中各实体节点的数据,使得图解模型更加及时和实用.

2 安防知识图谱构建方法

传统的安全防范系统效能评估方法主要依赖于专家的知识和经验,通过对安防系统各项属性进行评分来进行评估.然而,当安防系统规模庞大时,仅依靠专家评估很难对整个系统进行实时评估,导致评估结果缺乏时效性.为了实现对安防系统的动态评估,本文需要利用安防系统的实时数据来进行评估,并通过构建安防系统知识图谱来解决以上问题.

安全防范系统的安防任务主要分为探测、延迟和响应三类.根据《安全防范工程技术标准》(GB 50348-2018)的定义,探测任务要求能够及时发现各类风险事件或隐性风险事件,并发出报警信息;延

迟任务要求在入侵行为过程中延迟入侵者的进入或退出，延迟入侵者接近目标的速度；响应任务是制止风险事件发生的行动，对危险事件做出及时响应，其中延迟是基本前提，探测作为响应的依据.

因此，本文将安全防范系统中由人防、物防、技防等安防属性组成的最小安防单元划分为安防节点.一个安防节点由一个或多个安防属性组成，执行一系列的安防任务.通过引入安防节点的概念，根据不同的安防任务对安全防范系统进行区域划分，只需要对各安防节点包含的安防属性进行实时评估，就能够动态得出各局部区域的安防效能.同时，只需要对安防节点局部存在的属性进行计算，就可以实现实时更新，而不依赖于专家评估.

2.1　研究对象

安全防范系统是社会公共安全的一部分.就防范手段而言，安全防范包括人力防范、实体（物）防范和技术防范三个范畴.其中人力防范和实体防范是古已有之的传统防范手段，它们是安全防范的基础，随着科学技术的不断进步，这些传统的防范手段也不断融入新科技的内容.技术防范的概念是在近代科学技术（最初是电子报警技术）用于安全防范领域并逐渐形成的一种独立防范手段的过程中所产生的一种新的防范概念.下面以某一古建筑文物保护安防系统为例，如图4古建筑安防系统节点平面图所示，该系统包括安防人员、监控设备、出入口控制设备和出入口控制系统等安防属性.

2.2　节点类型定义

根据承担安防任务的不同，本文将安防系统划分为不同类型的节点.一个简单的节点划分方法如表1所示，具体的节点划分需要结合安防单位的实际情况进行考虑.

2.3　安防节点定义

根据标准规定的三类安防任务，对安防系统进行区域划分，形成安防节点.安防节点的划分结果和安防属性如表2所示.

2.4　基于路径关系的图谱构建

本文利用前面提出的安防知识图谱，将路径节点作为图谱的节点，并根据这些节点的空间关系构建路径节点之间的关系.使用Neo4j图数据库的Create语句构建针对该安防系统的知识图谱，其中

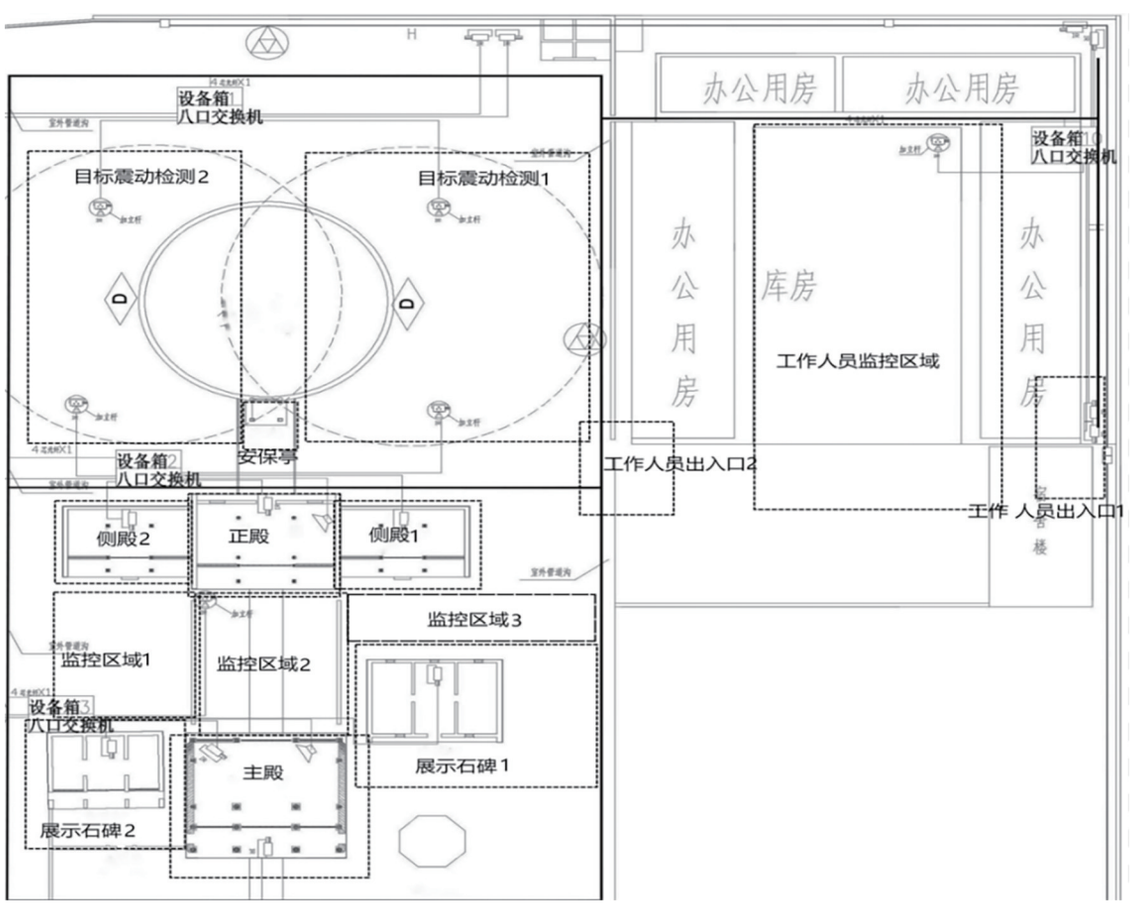

图4　古建筑安防系统节点平面图

Fig. 4　Plan view of the nodes in the security system of ancient architecture

表1 安防节点划分方法

Tab. 1 Security node division method

节点名称	节点类型	物理含义
普通人员出入口	出入口	用于控制各类人员出入的区域,包括身份识别、人员控制系统等安防要素
工作人员出入口	出入口	用于控制单位工作人员出入的区域,对人员身份有要求,包括身份识别、人员控制系统等安防要素
车辆出入口	出入口	用于控制车辆出入的区域,对人员身份有要求,包括身份识别、车辆控制系统等安防要素
目标建筑物	建筑物	目标存放的建筑区域,包含各类安防要素
开放建筑物	建筑物	公共建筑区域,不限制人员身份信息,通常包含视频监控等安防要素
开放区域	单位区域	各类人员可以自由活动的区域
限制区域	单位区域	只有拥有权限的人员可以活动的物理区域
目标禁区	单位区域	禁止人员活动的物理区域

表2 安防节点属性

Tab. 2 Security node properties

节点名称	节点编号	安防子系统	安防任务
展示石碑1	S_1	监控设备、震动探测设备	探测、延迟
主殿	S_2	监控设备、出入口控制设备	探测
展示石碑2	S_3	监控设备、震动探测设备	探测
工作人员出入口1	S_4	监控设备、出入口控制设备	探测
监控区域1	S_5	监控设备、身份识别设备	探测、延迟
监控区域2	S_6	监控设备、入侵探测设备、安保人员	探测、延迟、响应
监控区域3	S_7	监控设备、安保人员	探测、响应
工作人员监控区域	S_8	监控设备、安保人员	探测
侧殿1	S_9	监控设备、出入口控制设备	探测
正殿	S_{10}	监控设备、入侵探测设备、安保人员	探测、延迟
侧殿2	S_{11}	监控设备、震动探测设备、安保人员	探测、延迟
工作人员出入口2	S_{12}	监控设备、出入口控制设备	探测、延迟、响应
目标震动检测2	S_{13}	监控设备、震动探测设备	探测、延迟、响应
目标震动检测1	S_{14}	监控设备、震动探测设备	探测、延迟、响应
安保亭	S_{15}	监控设备、安保人员	探测、延迟、响应

节点编号作为知识图谱中节点的ID,安防子系统作为节点的属性.构建的知识图谱如图5所示.

在所构建的知识图谱中,路径节点与安防属性节点之间存在包含关系,并且相邻的安防节点被连接起来,从而形成了表示入侵路径的路径节点.基于这一构建方式,本文生成了一个直观的安防系统图解模型.该图解模型清晰地展示了各路径节点之间的关系,并且准确地呈现了各路径节点的安防属性.

3 基于隐马尔科夫的入侵路径分析

入侵路径计算的核心是通过一定的算法规则,找出安全防范系统图解模型中最薄弱的路径.最简单的路径算法是使用深度优先遍历来找出所有路径,然后分别计算安防效能,最后通过比较找出最薄弱的路径.然而,这种方法仅针对事先确定的单一路径进行分析.实际情况中,多条路径可能都经过同一个节点,而该节点会受到更多的检验.因此,单一路径分析无法考虑到各节点的不同情况.同时,安防系统通常具有多个目标,入侵者在入侵过程中也会选择不同的路径.为了解决上述问题,本文引入了隐马尔可夫链来计算入侵路径的效能,从而实现对多路径和多目标的入侵路径效能评估.

3.1 基于隐马尔可夫链计算最薄弱路径

根据图解模型和知识图谱,入侵路径可以被视为一种时序生成的数据集合.在每个时间点t,入侵者选择当前入侵的路径节点,并根据当前路径节点与其他路径节点的路径关系,在t+1时刻选择下一个路径节点.这个过程一直持续到抵达安防目标,从而生成入侵路径.

隐马尔可夫链是一种解决时序数据生成的模型,

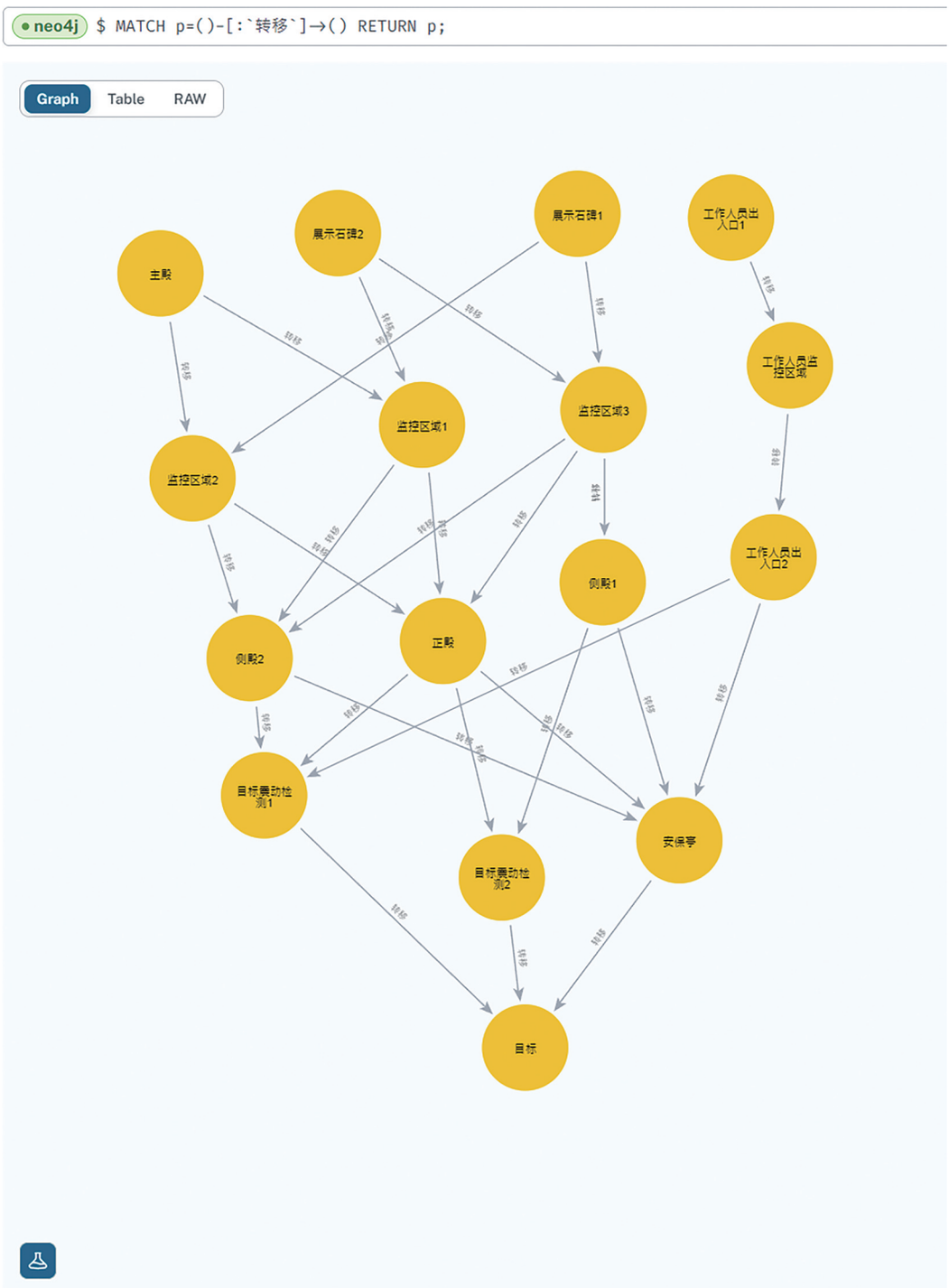

图5　安防系统知识图谱

Fig. 5　Security system knowledge graph

在网络入侵预测问题中得到广泛应用.如图6所示，隐马尔可夫链由两组变量组成.第一组变量是状态变量$\{y_1,y_2\cdots y_n\}$，其中y_i表示系统在第i时刻的状态.通常情况下，系统的状态变量是不可观测的，因此被称为隐变量.第二组变量是观测变量$\{x_1,x_2\cdots x_n\}$，其中x_i表示系统在第i时刻可能处于的观测状态.

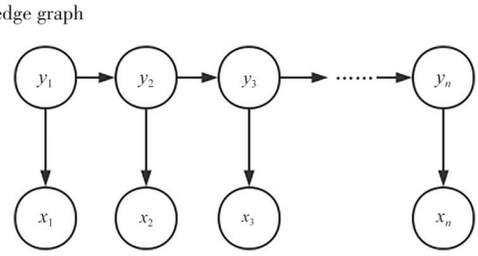

图6　隐马尔可夫链

Fig. 6　Hidden markov chain

在入侵者经过路径节点时，路径节点可能处于

两种状态:有效状态和失效状态.当所有路径节点的状态均为失效状态时,本文将其称为入侵路径.对于任意一个表示安防系统的图解模型,一定存在一条到达安防目标的入侵路径,其中各路径节点的观测状态均为失效状态,并且该路径的失效状态出现概率最高.本文将这条路径称为最薄弱入侵路径.

为了找出最薄弱入侵路径,本文利用隐马尔可夫链的原理.隐马尔可夫链根据可观测的变量,可以找出概率最大的状态变量序列.在入侵路径中,入侵者在不同时刻选择不同的路径节点,而本文根据可观测的路径节点来找出隐藏的安防效能最低的路径.这个问题属于隐马尔可夫链中的预测问题,并且已经开始应用于一些统计评估系统和风险评估研究中.

依据隐马尔可夫链的入侵路径分析,本文需要考虑以下三个参数:

1. 路径转移矩阵:该矩阵表示在不同状态之间的转移概率.在入侵路径计算中,本文将其记为矩阵$\boldsymbol{A}=[a_{ij}]$,其中a_{ij}表示在时间t选择路径节点i的情况下,在时间t+1时选择路径节点j的概率.由于一个节点可能被包含在多条路径中,当多条路径都要经过同一个节点时,该节点也就越容易被选取.因此,矩阵$\boldsymbol{A}$的值由各路径节点的路径数目进行归一化决定.矩阵$\boldsymbol{A}$中的各项可以用公式(2.1)表示.

$$a_{ij}=\frac{v_j}{v_1+v_2+\cdots+v_n},\tag{2.1}$$

其中,v_j为经过路径节点j的路径数目,n为下一节点可以转移节点的数目.

2. 路径节点状态矩阵:该矩阵表示在当前状态Y情况下,选择各观测变量的概率.在入侵路径计算中,本文需要选择一个节点作为最薄弱入侵路径的组成部分.为了确定选择哪个节点,本文考虑各路径节点的失效概率矩阵,记为矩阵$\boldsymbol{B}=[b_i]$.假设本文已知各路径节点的安防效能评分,那么安防效能越低的路径节点,越有可能成为入侵者的目标,被突破的概率也就越大.因此,矩阵B的值由各路径节点安防效能的反比进行归一化处理,可以用公式(2.2)表示.

$$b_i=1-q_i,\tag{2.2}$$

其中,q_i代表路径节点i的安防效能评分,评分越高,制止概率越高,状态为失效状态的概率越低.

3. 初始状态矩阵:由于初始节点不由任何节点转移而来,该矩阵表示模型在初始时刻时,各初始状态的选取概率.在入侵路径计算中,它表现为选取起始路径节点的概率.本文将这些概率组成矩阵$\boldsymbol{C}=[c_i]$,其中c_i代表起始节点i的选取概率,由各起始节点的路径数目进行归一化计算.具体计算方式可以用公式(2.3)表示.

$$c_i=\frac{v_i}{v_1+v_2+\cdots+v_m},\tag{2.3}$$

其中,v_i为经过路径节点i的路径数目,m为可以作为起始节点的数目.

3.2 基于维特比的简化路径算法

通过使用隐马尔可夫链模型,可以计算每条入侵路径作为最薄弱路径的概率,并进行比较以找出最薄弱路径.然而,这种方法的计算成本较高.为了简化计算,维特比提出了一种方法.

维特比算法的核心思想是将隐马尔可夫链模型与动态规划相结合,将入侵路径计算视为由时间决定的动态选择结果.然后,对于每次选择中不可能的路径进行剪枝处理,以找出最薄弱路径.接着,根据最薄弱路径找出安防效能最低的路径节点,并将该路径节点的选取概率设置为零.然后重新计算,找出新的最薄弱路径.如此反复进行,直到入侵路径的安防效能达到要求.目前,该算法主要用于最优路径的研究.

具体的简化算法如下:以图7所示的入侵路径图为例,其中各节点的安防效能通过对应的知识图谱得出.现在需要找出最薄弱的入侵路径.可以将入侵路径分解为时序模型,在t时刻,入侵者到达起始节点,在t+1时刻,从下一个节点中选择路径节点.为了找出从起始节点S到目标节点E的最薄弱路径,当入侵者从t=1时刻转移到t=2时刻时,本文可以分别找出经过各节点的最薄弱路径,并将其他不可能的路径进行剪枝处理.

经过剪枝处理后,只保留各节点的最短路径.此时无法确定哪条路径是最薄弱路径的组成部分,但一定有且只有一条路径是最薄弱路径的组成部分.然后分别找出经过t=2和t=3的最薄弱路径,则最薄弱路径只能在剩余路径中选择中进行选择.

与传统的深度优先遍历计算每条安防路径效能的方法相比,维特比算法通过提前排除不可能的路径,极大地减少了计算量.该方法计算比较路径的时间复杂度为$O(n)$,而深度优先遍历的路径计算时间复杂度为$O(n^2)$.

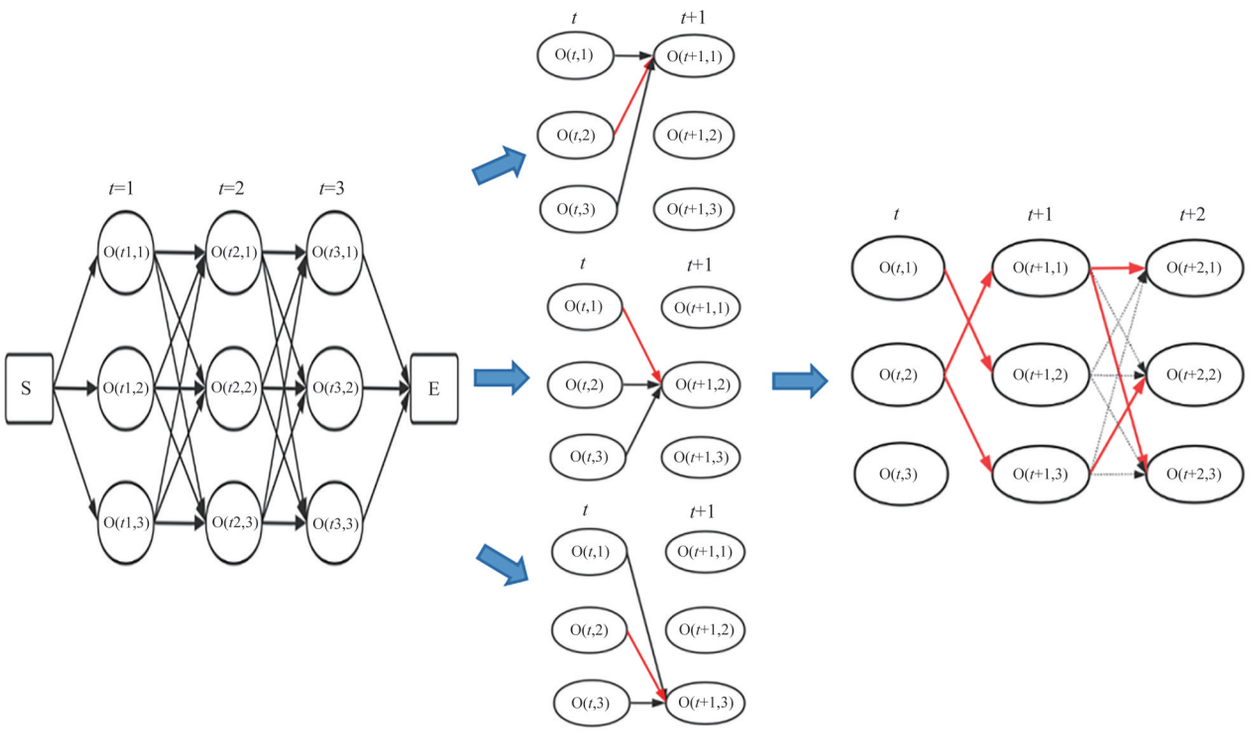

图7　入侵路径图

Fig. 7　Intrusion path map

4　实验分析与比较

4.1　安防节点效能

为了实现安全防范任务的探测、延迟和响应，本文对图4各节点进行了划分[12]. 各节点的安防属性数据通过系统接口或安防文件进行实时更新. 根据指标体系评估，本文已经得出了各安防节点在 t 时刻下的安防效能. 表3展示了各路径节点的当前效能.

表3　路径节点效能表

Tab. 3　Path node effectiveness table

节点名称	编号	安防效能	节点名称	编号	安防效能
展示石碑1	S_1	0.598	侧殿1	S_9	0.772
主殿	S_2	0.864	正殿	S_{10}	0.698
展示石碑2	S_3	0.683	侧殿2	S_{11}	0.741
工作人员出入口1	S_4	0.893	工作人员出入口2	S_{12}	0.886
监控区域1	S_5	0.732	目标震动检测2	S_{13}	0.763
监控区域2	S_6	0.637	目标震动检测1	S_{14}	0.896
监控区域3	S_7	0.746	安保亭	S_{15}	0.937
工作人员监控区域	S_8	0.913			

4.2　薄弱路径分析

该图解模型包含了36条入侵路径，这些路径在表4中有所展示. 每个路径节点都有两种状态. 总共有576种状态序列可以在该图解模型中出现. 其中，有36种状态序列满足所有观测状态都是失效状态.

根据图解模型的分析，本文可以得出共有4个起始节点，分别为 S_1、S_2、S_3、S_4. 通过公式2.3，可以计算初始状态矩阵 **C** 的值，具体的计算过程如公式3.1所示.

$$\begin{cases} c_1 = \dfrac{12}{35} = 0.3429 \\ c_2 = \dfrac{12}{35} = 0.3429 \\ c_3 = \dfrac{10}{35} = 0.2857 \\ c_4 = \dfrac{1}{35} = 0.0285 \end{cases} \tag{3.1}$$

根据图解模型的结构，本文可以确定共有4个路径节点状态矩阵. 通过公式2.2，可以计算得到各个矩阵 **B** 的值. 表5展示了各个矩阵的可能状态以及对应的选取概率.

为了计算路径节点的转移概率，本文可以使用公式2.1来构建路径转移矩阵. 在矩阵中，横坐标表示前一路径节点的编号，纵坐标表示转移路径节点的编号. 如果某个转移路径是不可能的，对应的数值为0. 而矩阵中的 a_{ij} 代表由节点 i 转移到节点 j 的概率.

在本例中，本文可以得到转移矩阵 A 如(3.2).

$$A=\begin{bmatrix}
0&0&0&0&0&0.5834&0.4166&0&0&0&0&0&0&0&0\\
0&0&0&0&0.4166&0.5834&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0.5&0&0.5&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0.6207&0.3793&0&0&0&0\\
0&0&0&0&0&0&0&0&0.1176&0.5294&0.3530&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0.6&0.4&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0.3478&0&0.6255\\
0&0&0&0&0&0&0&0&0&0&0&0&0.2286&0.3429&0.4285\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0.4444&0.5556\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{bmatrix}. \quad (3.2)$$

表4 入侵路径表

Tab. 4 Intrusion path table

路径编号	入侵路径
1	S_1->S_6->S_9->S_{13}->D
2	S_1->S_6->S_9->S_{15}->D
3	S_1->S_6->S_{10}->S_{13}->D
4	S_1->S_6->S_{10}->S_{14}->D
5	S_1->S_6->S_{10}->S_{15}->D
6	S_1->S_6->S_{11}->S_{14}->D
7	S_1->S_6->S_{11}->S_{15}->D
8	S_1->S_7->S_{10}->S_{13}->D
9	S_1->S_7->S_{10}->S_{14}->D
10	S_1->S_7->S_{10}->S_{15}->D
11	S_1->S_7->S_{11}->S_{14}->D
12	S_1->S_7->S_{11}->S_{15}->D
13	S_2->S_5->S_{10}->S_{13}->D
14	S_2->S_5->S_{10}->S_{14}->D
15	S_2->S_5->S_{10}->S_{15}->D
16	S_2->S_5->S_{11}->S_{14}->D
17	S_2->S_5->S_{11}->S_{15}->D
18	S_2->S_6->S_9->S_{13}->D
19	S_2->S_6->S_9->S_{15}->D
20	S_2->S_6->S_{10}->S_{13}->D
21	S_2->S_6->S_{10}->S_{14}->D
22	S_2->S_6->S_{10}->S_{15}->D
23	S_2->S_6->S_{11}->S_{14}->D
24	S_2->S_6->S_{11}->S_{15}->D
25	S_3->S_5->S_{10}->S_{13}->D
26	S_3->S_5->S_{10}->S_{14}->D
27	S_3->S_5->S_{10}->S_{15}->D
28	S_3->S_5->S_{11}->S_{14}->D
29	S_3->S_5->S_{11}->S_{15}->D
30	S_3->S_7->S_{10}->S_{13}->D
31	S_3->S_7->S_{10}->S_{14}->D
32	S_3->S_7->S_{10}->S_{15}->D
33	S_3->S_7->S_{11}->S_{14}->D
34	S_3->S_7->S_{11}->S_{15}->D
35	S_4->S_8->S_{12}->S_{14}->D
36	S_4->S_8->S_{12}->S_{15}->D

表5 路径选择矩阵中各节点的突破概率表

Tab. 5 Breakthrough probability table for each node in the path selection matrix

节点名称	编号	所属矩阵编号	失效概率
展示石碑1	S_1	1	0.402
主殿	S_2	1	0.136
展示石碑2	S_3	1	0.317
工作人员出入口1	S_4	1	0.107
监控区域1	S_5	2	0.268
监控区域2	S_6	2	0.363
监控区域3	S_7	2	0.254
工作人员监控区域	S_8	2	0.087
侧殿1	S_9	3	0.228
正殿	S_{10}	3	0.302
侧殿2	S_{11}	3	0.259
工作人员出入口2	S_{12}	3	0.114
目标震动检测2	S_{13}	4	0.237
目标震动检测1	S_{14}	4	0.104
安保亭	S_{15}	4	0.023

得到各路径节点之间的转移概率矩阵后,本文可以利用计算维特比算法的思想对概率计算进行简化.具体而言,本文可以根据表6中所示的剪枝处理方法对各入侵路径进行处理.

经过剪枝处理后,本文得到了三条可能的路径,如图8所示.这三条路径分别编号为3、35和7.本文需要对这三条路径进行比较,以找出概率最大的入侵路径.通过比较,发现当路径节点均为失效状态时,路径编号为3的路径(S_1->S_6->S_{10}->S_{13})具有最大的概率成为最薄弱路径,因此可以认为路径编号为3的路径是安防系统的最薄弱路径.

4.3 与深度优先遍历方法的比较分析

与传统的先确定入侵路径的方法相比,本文提出的方法利用动态规划的思想,提前剪枝排除不满

表6　路径剪枝处理表

Tab. 6　Path pruning process table

节点编号	经过该节点的路径	最大概率路径	剪枝处理的路径	状态均为失效的概率
S_5	S_2->S_5 S_3->S_5	S_3->S_5	S_2->S_5	0.11732
S_6	S_1->S_6 S_2->S_6	S_1->S_6	S_2->S_6	0.14051
S_7	S_1->S_7 S_3->S_7	S_1->S_7	S_3->S_7	0.01223
S_8	S_4->S_8	S_4->S_8	无	0.00034
S_9	S_1->S_6->S_9	S_1->S_6->S_9	无	0.00875
S_{10}	S_3->S_5->S_{10} S_1->S_6->S_{10} S_1->S_7->S_{10}	S_1->S_6->S_{10}	S_3->S_5->S_{10} S_1->S_7->S_{10}	0.02487
S_{11}	S_3->S_5->S_{11} S_1->S_6->S_{11} S_1->S_7->S_{11}	S_1->S_6->S_{11}	S_3->S_5->S_{11} S_1->S_7->S_{11}	0.02133
S_{12}	S_4->S_8->S_{12}	S_4->S_8->S_{12}	无	0.00026
S_{13}	S_1->S_6->S_9->S_{13} S_1->S_6->S_{10}->S_{13}	**S_1->S_6->S_{10}->S_{13}**	S_1->S_6->S_9->S_{13}	0.017167
S_{14}	S_1->S_6->S_{10}->S_{14} S_1->S_6->S_{11}->S_{14} S_4->S_8->S_{12}->S_{14}	S_4->S_8->S_{12}->S_{14}	S_1->S_6->S_{10}->S_{14} S_1->S_6->S_{11}->S_{14}	0.00126
S_{15}	S_1->S_6->S_{10}->S_{15} S_1->S_6->S_{11}->S_{15} S_4->S_8->S_{12}->S_{15}	S_1->S_6->S_{10}->S_{15}	S_1->S_6->S_{11}->S_{15} S_4->S_8->S_{12}->S_{15}	0.00027

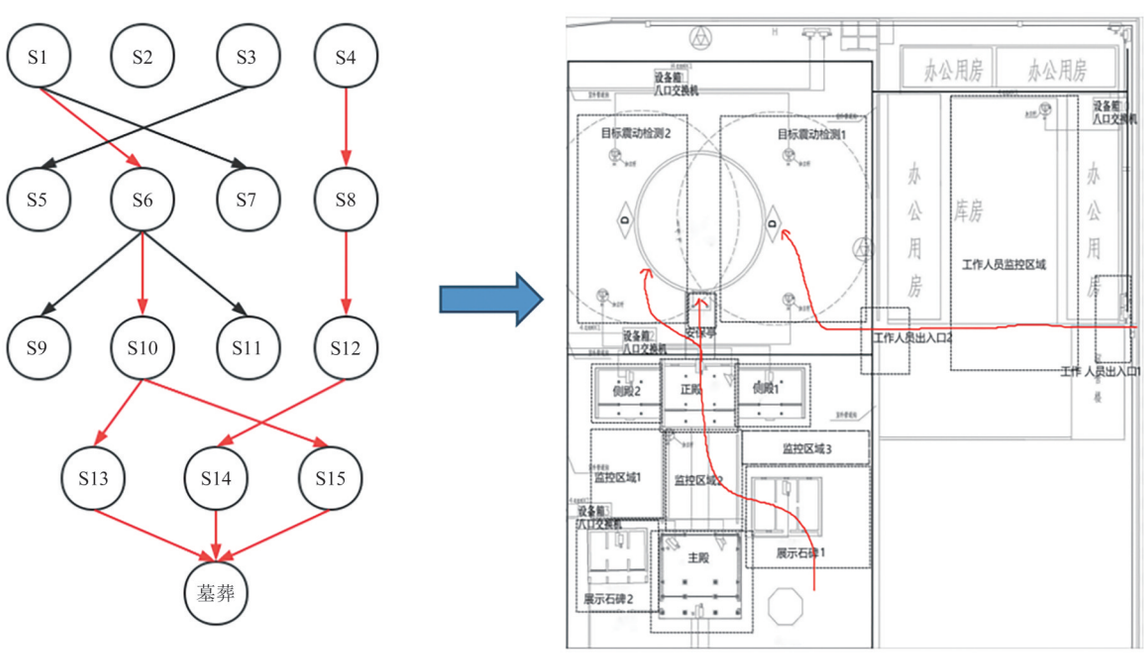

图8　最薄弱路径图

Fig. 8　The weakest path map

足条件的入侵路径，时间复杂度更低．针对一个包含 n 个节点的入侵路径图谱，深度优先遍历[13]计算入侵需要先确定路径，之后计算每条入侵路径的实际安防效能，时间复杂度为 $O(n^2)$，同时需要将每条入侵路径从图解模型中剥离，无法考虑到其他不在该路径上节点对入侵路径的影响．对比如表7所示．

表7 实验方法对比表

Tab. 7 Comparison of experimental methods table

方法名称	时间复杂度	入侵路径分析	目标分析	是否考虑其他路径节点的影响
维特比算法	$O(n)$	动态规划	多目标	是
深度优先遍历	$O(n^2)$	静态	单一目标	否

5 结论

入侵者的入侵过程十分复杂,因此使用直观的入侵路径模型具有重要的意义.然而,现有方法[14]虽然考虑了各节点之间的路径关系,却缺乏安防系统本身的基本信息,并未考虑安防事件的影响.这导致只能以路径节点的路径期望作为转移依据,无法在实际安防系统上反映入侵路径的分析结果,也无法为安防系统的改进提供指导性意见.为了解决这一问题,本文将传统的攻击图转变为知识图谱,并结合通用安防效能指标和知识图谱所包含的节点属性,提出了计算路径节点安防效能与入侵事件状态转移概率的方法.在此基础上,本文重点研究了实际环境中不同时序下的安防路径效能,用于分析节点的安防效能,辅助安全管理员全面分析不同攻击路径下的实际安防效能,并为安全防范系统提供指导性意见.

未来的研究方向包括如何提取各节点属性与入侵事件之间的关系[15],并通过实时数据的传入进行更新,以提高不同场景下的评估准确率.这将是下一步研究的主要工作.

参 考 文 献

[1] 陈志华.安全防范系统建设与运用过程中的效能评估[J].中国人民公安大学学报(自然科学版),2008,14(1):51-55.

[2] 付萍.安全防范系统效能评估研究综述[J].科技资讯,2008,6(22):13-14.

[3] KAYNAR K. A taxonomy for attack graph generation and usage in network security [J]. Journal of Information Security and Applications, 2016, 29(C): 27-56.

[4] 郑舟毅,杜治国,王欣.安防系统弱点评估算法的可视化实现[J].计算机工程与应用,2014,50(5):70-73,82.

[5] 王洪苹.安全防范系统的风险评估[D].重庆:西南大学,2017.

[6] 胡浩,刘玉岭,张红旗,等.基于吸收Markov链的网络入侵路径预测方法[J].计算机研究与发展,2018,55(4):831-845.

[7] ZHU B, GHORBANI A A. Alert correlation for extracting attack strategies [J]. International Journal of Network Security, 2006, 3(3): 244-258.

[8] ORTALO R, DESWARTE Y, KAANICHE M. Experimenting with quantitative evaluation tools for monitoring operational security[J]. IEEE Transactions on Software Engineering, 1999, 25(5): 633-650.

[9] IDIKA N, BHARGAVA B. Extending attack graph-based security metrics and aggregating their application [J]. IEEE Transactions on Dependable and Secure Computing, 2012, 9(1): 75-85.

[10] 杨智君,田地,马骏骁,等.入侵检测技术研究综述[J].计算机工程与设计,2006,27(12):2119-2123,2139.

[11] 张吉祥,张祥森,武长旭,等.知识图谱构建技术综述[J].计算机工程,2022,48(3):23-37.

[12] 费智涛,郭小东,王志涛.多源异构数据环境下不可移动文物灾害风险图构建方法研究[J].西北大学学报(自然科学版),2022,52(4):700-709.

[13] 刘萍,冯桂莲.图的深度优先搜索遍历算法分析及其应用[J].青海师范大学学报(自然科学版),2007,23(3):41-44.

[14] 关健.入侵检测系统数据分析方法及其相关技术的研究[D].哈尔滨:哈尔滨工程大学,2004.

[15] 赵培祥.基于入侵路径分析的安防系统效能分析与仿真研究[D].北京:中国人民公安大学,2023.

(责编&校对 雷建云)