doi:10.11959/j.issn.1000-436x.2016210

基于因果知识网络的攻击路径预测方法

王硕[1]，汤光明[1]，寇广[1,2]，宋海涛[1]
（1. 解放军信息工程大学，河南 郑州 450001；2. 信息保障技术重点实验室，北京 100072）

摘 要：针对现有攻击路径预测方法无法准确反映攻击者攻击能力对后续攻击路径的影响，提出了基于因果知识网络的攻击路径预测方法。借助因果知识网络，首先通过告警映射识别已发生的攻击行为；然后分析推断攻击者能力等级，进而根据攻击者能力等级动态调整概率知识分布；最后利用改进的 Dijkstra 算法计算出最有可能的攻击路径。实验结果表明，该方法符合网络对抗实际环境，且能提高攻击路径预测的准确度。
关键词：攻击路径预测；因果知识网络；攻击者能力；概率知识分布；Dijkstra 算法
中图分类号：TP393.8 **文献标识码**：A

Attack path prediction method based on causal knowledge net

WANG Shuo[1], TANG Guang-ming[1], KOU Guang[1,2], SONG Hai-tao[1]
(1. PLA Information Engineering University, Zhengzhou 450001, China;
2. Science and Technology on Information Assurance Laboratory, Beijing 100072, China)

Abstract: The existing attack path prediction methods can not accurately reflect the variation of the following attack path caused by the capability of the attacker. Accordingly an attack path prediction method based on causal knowledge net was presented. The proposed method detected the current attack actions by mapping the alarm sets to the causal knowledge net. By analyzing the attack actions, the capability grade of the attacker was inferred, according to which adjust the probability knowledge distribution dynamically. With the improved Dijkstra algorithm, the most possible attack path was computed. The experiments results indicate that the proposed method is suitable for a real network confrontation environment. Besides, the method can enhance the accuracy of attack path prediction.
Key words: attack path prediction, causal knowledge net, attacker capability, probability knowledge distribution, Dijkstra algorithm

1 引言

随着网络攻击技术的不断发展，多步性成为目前网络攻击行为的主要特点之一。攻击行为的多步性是指攻击者利用目标网络中的一些漏洞，通过实施蓄意的多步骤攻击行为来达到最终的攻击目的。具有多步性的攻击行为简称为多步攻击，它给政府、企业乃至个人带来了巨大的威胁，如 Zeus 僵尸网络通过扫描探测、溢出攻击、感染目标主机、病毒传播和窃取用户信息这 5 个攻击步骤使数以万计的网民遭受了无法挽回的经济损失[1]。目前，威胁极大的 APT 攻击也属多步攻击范畴。多步攻击威胁受到广泛的关注，防护多步攻击刻不容缓。攻击路径预测旨在通过告警关联技术分析已发生的攻击行为，揭示其中隐藏的相关逻辑，构建攻击场景，进而推测攻击者后续的攻击步骤，为网络安全主动防御提供重要依据，成为目前应对多步攻击威胁的重要手段之一。

攻击路径预测的关键分为 2 个部分：1) 理解当前已发生的攻击行为；2) 预测攻击者未来可能实施的攻击步骤。目前，针对第一部分的研究主要是通过关联告警构建攻击场景。具体而言，分为数据挖

收稿日期：2016-02-22；**修回日期**：2016-08-18
基金项目：国家自然科学基金资助项目（No.61303074）；信息保障技术重点实验室开放基金资助项目（No.KJ-14-106）
Foundation Items: The National Natural Science Foundation of China(No.61303074), Foundation of Science and Technology on Information Assurance Laboratory (No.KJ-14-106)

掘、事先构建攻击过程和因果关联。数据挖掘的方法主要是通过机器学习算法发现告警中隐藏的攻击行为模式，形成过滤或关联规则，在此基础上进行攻击场景构建，如 Qin 等[2]的时间序列模型和梅海彬等[3]利用告警间相似度函数来构建攻击活动序列集的方法。此种方法依赖专家知识较少，但是存在准确度低、结果难以理解等缺陷。事先构建攻击过程的方法则大多通过专家知识来得到各种攻击过程模板，然后将新的告警同这些攻击过程模板相匹配，进行实时关联[4]。这种方法的难点是如何获得用于描述攻击过程的关联规则，此外，这种方法无法检测出未知攻击行为。因果关联的方法是利用各个攻击步骤之间的因果逻辑关系，通过制定因果关联规则来构建攻击场景。此方法成为目前攻击场景构建的主流方法，具有代表性的是 Jajodia 等[5]的攻击图模型和 Yu 等[6]的隐彩色 Petri 网络。前者通过有向图描述不同攻击步骤之间依赖关系，结合目标网络进行告警关联。而后者将资源状态、攻击行为及攻击证据作为彩色 Petri 网络的不同类型节点，并将其互相关联以完成攻击预测。针对第二部分的研究主要是在第一部分的基础上，设计相应的推理规则以实现对后续攻击路径的预测。Wang 等[7]根据通用漏洞评分系统（CVSS, common vulnerability scoring system）对漏洞复杂度的评分，赋予攻击图以概率属性，并定义累积概率来计算整个网络的安全属性。然而该方法忽略了漏报、误报等不确定事件对概率的影响。在 Wang 等的基础上，苏婷婷等[8]将攻击图直观地表示为属性邻接矩阵，并通过矩阵算法计算攻击成功的概率。陈小军等[9]则利用累积概率计算目标攻击节点的最大可达概率，有效推断攻击意图和计算攻击路径。吕慧颖等[10]深入分析了网络对抗的时空特性，利用威胁状态转移图挖掘威胁事件的时空关联关系，实时识别威胁状态、预测攻击路径。然而，由于网络攻防过程的动态性和不确定性，导致攻击图节点概率不能客观反映攻防双方对抗状态，从而影响攻击路径预测的准确性。针对此问题，Xie 等[11]首先深入分析了攻击图中的 3 种不确定性，即攻击图结构的不确定性、攻击行为发生的不确定性以及触发告警的不确定性，并考虑了它们对攻击路径预测的影响。张少俊等[12]提出了一个在满足观测事件偏序条件下，利用贝叶斯推理计算攻击图节点的置信度方法，用于提高不确定性处理的准确度。Abraham 等[13]通过引入漏洞生命周期来实现时变的攻击路径预测。Fredj[14]则提出利用攻击行为的危害大小来区分不同的攻击者。冯学伟等[15]通过构建马尔可夫链模型，利用告警流挖掘不同攻击类型之间的转移概率，一定程度上解决了人工设定概率带来的主观性缺陷。然而，目前的研究通常是静态的分析，不能根据攻击行为和防御措施及时调整相关概率的生成，不能反映攻击者攻击能力的不同对后续攻击路径的影响，影响了攻击路径预测的准确性。

基于以上分析，本文充分考虑了网络攻防实战环境，提出了基于因果知识网络的攻击路径预测方法。借助因果知识网络，综合利用图关系进行告警映射，实时检测已发生的攻击行为。在此基础上，推断攻击者能力等级，进而根据攻击者能力等级自适应地调整攻击行为发生及成功的概率，最终利用改进的 Dijkstra 算法计算得出攻击者最有可能的后续攻击路径。

2　因果知识网络模型

2.1　因果知识网络的提出

定义 1　因果知识网络(CKN, causal knowledge net)，$CKN=(N,E,\Delta)$。CKN 为有向无环图。

1) N 为节点集合，$N=\{S\cup A\cup AS\cup AE\}$。其中，$S=\{s_i|i=1,\cdots,n\}$为状态节点集合，节点 s_i 的变量取值为 true 或 false，表示当前攻击者是否占有该资源。$A=\{a_i|i=1,\cdots,m\}$为攻击行为节点集合，节点 a_i 的变量取值为 true 或 false，表示当前攻击行为是否已经发生。$Pre(s_i)$表示状态节点 s_i 的前置条件，为一个或多个攻击行为节点，且攻击行为节点之间为“或”的关系，即每一个攻击行为都能使之达到此状态节点。$Post(s_i)$表示状态节点 s_i 的后置条件，为一个或多个攻击行为节点，表示当前状态能够作为多个攻击行为的前置条件。$Pre(a_i)$表示攻击行为节点 a_i 的前置条件，为一个或多个状态节点，且状态节点之间为“与”的关系，即只有满足所有前置条件，攻击行为才有可能发生。如果一个攻击行为节点的前置条件不止一个，则称其为特殊攻击行为节点。$Post(a_i)$表示攻击节点 a_i 的后置条件，为一个状态节点，表示当前攻击只能达到一个状态节点。$AS=\{as_i|i=1,\cdots,n\}$为状态型告警节点集合。定义映射 $f_{AS\to S}$: $as_i\to s_i$ ($i=1,\cdots,n$)，表示一个状态型告警 as_i 能且仅能证明一个状态节点 s_i 的变量取值为 true。$AE=\{ae_i|i=1,\cdots,m\}$为事件型告警节点集合。定义映

射 $f_{AE\to A}$: $ae_i\to a_i$ (i=1,⋯,m)，表示一个事件型告警 ae_i 能且仅能反映一个攻击节点 a_i 发生的概率。

2) E 为有向边集合，E={$E_1\cup E_2\cup E_3\cup E_4$}。其中，$E_1\subseteq S\times A$ 表示只有攻击者占有某些资源，攻击行为才能发生；$E_2\subseteq A\times S$ 表示攻击行为能够使攻击者占有某些资源；$E_3\subseteq AS\times S$ 表示状态型告警能够证明某个状态为 true；$E_4\subseteq AE\times A$ 表示事件型告警能够推断某个攻击行为已经发生。

3) Δ为概率知识分布，Δ=(Δ_1,Δ_2,Δ_3,Δ_4)。其中，Δ_1 是依附于有向边 E_1 上的概率知识，$\Delta_1(ij)$表示在状态 s_i 下可能发生后续攻击 a_j 的概率。Δ_2 是依附于有向边 E_2 上的概率知识，$\Delta_2(ij)$表示在攻击行为 a_i 发生后达到下一状态 s_j 的概率。Δ_3 是依附于有向边 E_3 上的概率知识，$\Delta_3(i)$表示状态型告警 as_i 出现时能证明状态 s_i 为 true 的概率。Δ_4 是依附于有向边 E_4 上的概率知识，$\Delta_4(i)$表示事件型告警 ae_i 出现时能证明攻击行为 a_i 发生的概率。

本模型通过概率知识分布来推理实时的攻击行为和预测后续攻击路径。对于攻击行为节点，Δ_4 的推理优先级高于Δ_1，即当事件型告警出现时，可以不用考虑其前置条件是否满足，即可推断该攻击行为可能发生了；否则，通过已经满足的状态条件来推断攻击行为发生的可能性。对于状态节点来说，Δ_3 的推理优先级高于Δ_2，即状态型告警出现时，可以确定该状态为 true，同时证明相应攻击已经发生且成功；否则，通过攻击行为发生和成功的概率来推断相应状态为 true 的可能性。

2.2 因果知识网络的构建方法

因果知识网络的构建分为 2 个部分：网络基本结构的确定和概率知识分布Δ的生成。本文的网络基本结构假定利用专家知识库确定，而重点研究概率知识分布Δ的生成。

由 2.1 节知Δ=(Δ_1,Δ_2,Δ_3,Δ_4)。

1) Δ_3为利用状态型告警推断相应状态为true的概率，由 IDS 的特性知，此概率常置为 1，即状态型告警的出现能完全证明相应的状态为 true。

2) Δ_4 为利用事件型告警推断攻击行为发生的概率，由于 IDS 对攻击行为的检测存在误差，此概率分 3 种情况进行修正。

①正常情况

正常情况的形式化描述为：$ae_i\in AE_T$ 且 $Pre(a_i)$= true。由于 IDS 告警不能完全证明攻击行为已经发生，为了客观描述这种不确定性，结合贝叶斯定理，给出了事件型告警出现时推断攻击行为发生的概率，如式(1)所示。

$$\begin{aligned}P(a_i\mid ae_i)&=\frac{P(ae_i\mid a_i)P(a_i)}{P(ae_i)}=\frac{(1-P(\neg ae_i\mid a_i))P(a_i)}{P(ae_i)}\\&=\frac{(1-P(\neg ae_i\mid a_i))P(a_i)}{P(ae_i\mid a_i)+P(ae_i\mid\neg a_i)}\\&=\frac{(1-o(a_i))P(a_i)}{d(a_i)+m(a_i)}\end{aligned}\tag{1}$$

其中，$o(a_i)$为 IDS 设备对 a_i 的漏报率；$d(a_i)$为 IDS 设备对 a_i 的检测率，$m(a_i)$为 IDS 设备对 a_i 的误报率，一般与 IDS 的性能有关；$P(a_i)$为攻击行为 a_i 的先验概率。

②误报情况

误报情况的形式化描述为：$ae_i\in AE_T$ 且 $Pre(a_i)$= false，即攻击的前置条件不满足却检测到告警。处理方法为直接去除。

③漏报情况

漏报情况的形式化描述为：$as_i\in AS_T$ 且 $Pre(s_i)$= false，即攻击行为已经发生且成功，但没有产生告警。$Pre(s_i)$中的元素之间为“或”的关系，即只要一个攻击行为节点为真就使 $Pre(s_i)$=true。处理方法为根据因果知识网络以一定的概率补全。假如状态节点 s_i 为假，但没有产生对应的事件型告警，以 $Pre(s_i)$包括 2 个攻击行为节点为例介绍补全方法。首先添加 a_i 和 a_j，然后，由贝叶斯定理知

$$P(a_i\mid as_i)=\frac{P(as_i\mid a_i)P(a_i)}{P(as_i)}=\frac{d(a_i)P(a_i)}{P(as_i)}\tag{2}$$

$$P(a_j\mid as_j)=\frac{P(as_j\mid a_j)P(a_j)}{P(as_j)}=\frac{d(a_j)P(a_j)}{P(as_j)}\tag{3}$$

$P(a_i|as_i)+P(a_j|as_j)$=1，则 a_i 和 a_j 这 2 个攻击行为发生的概率为

$$P(a_i\mid as_i)=\frac{d(a_i)P(a_i)}{d(a_i)P(a_i)+d(a_j)P(a_j)}\tag{4}$$

$$P(a_j\mid as_j)=\frac{d(a_j)P(a_j)}{d(a_i)P(a_i)+d(a_j)P(a_j)}\tag{5}$$

其中，$d(a_i)$和 $d(a_j)$分别为 IDS 设备对攻击行为 a_i 和 a_j 的检测率。

3) Δ_1 表示前置条件满足时后续攻击行为发生的概率，Δ_2 则是攻击行为发生时后续状态为 true 的概率，即攻击行为成功的概率。Δ_1 和Δ_2 是紧密联系的，在攻击路径推理中往往是一起考虑的，即用它

们的乘积$\Delta_1\times\Delta_2$表示攻击行为发生且成功的概率，记$\Delta_{12}=\Delta_1\times\Delta_2$。目前确定$\Delta_{12}$的方法主要是依据攻击行为复杂度来估计。然而在网络攻防实战中，Δ_{12}不仅与攻击行为复杂度有关，还与攻击者能力有关。具有不同攻击能力的攻击者对同一漏洞攻击成功的可能性必然不同。鉴于此，本文综合考虑攻击者能力等级和攻击行为复杂度这 2 个方面，提出一种更加合理的Δ_{12}确定方法，符合网络对抗实战的实际。

定义 2　攻击行为复杂度 $Cpx=\{Cpx_i|i=1,\cdots,m\}$。定义映射 $f_{A\to}Cpx$: $a_i\to Cpx(a_i)$ $(i=1,\cdots,m)$，表示攻击行为 a_i 的攻击复杂度为 $Cpx(a_i)$。攻击复杂度一般由漏洞复杂度来确定，依据 CVSS 对漏洞的评分标准，将攻击行为复杂度设为低（low）、中（mid）、高（high）3 个等级。

定义 3　攻击者能力等级 $Cap=\{\text{low, mid, high}\}$，从网络对抗实战中抽象出来用于刻画不同攻击者攻击能力高低的变量。本文将攻击者能力等级分为低（low）、中（mid）、高（high）3 个等级。

于是，攻击行为 a_i 发生且成功的概率$\Delta_{12}(a_i)$可由式(6)确定。

$$\Delta_{12}(a_i)=f(Cpx(a_i),Cap(attacker)) \tag{6}$$

其中，$Cpx(a_i)$为 a_i 的攻击行为复杂度，$Cap(attacker)$为攻击者能力等级。攻击行为发生且成功的概率$\Delta_{12}(a_i)$的确定依据如表 1 所示。

表 1　攻击行为发生且成功的概率 $\Delta_{12}(a_i)$ 的确定依据

Cpx	*P*(*Cpx*,*Cap*)		
	Cap=low	*Cap*=mid	*Cap*=high
Cpx=low	0.5	0.7	0.9
Cpx=mid	0.3	0.5	0.7
Cpx=high	0.1	0.3	0.5

3　攻击路径预测

攻击路径预测是通过分析已发生的攻击行为，借助因果知识网络，利用概率知识进行推理预测的过程。本文首先通过告警映射识别已发生的攻击行为，即实时攻击迹，然后根据攻击迹动态推断攻击者能力等级，进而自适应地调整概率知识分布，最后利用概率推理确定最有可能的后续攻击路径。

3.1　实时攻击迹的生成

定义 4　告警迹 $Alarm=(AS,AE)$，其中，AS 为状态型告警集合，AE 为事件型告警集合。特别地，T 时刻的状态型告警集合为 $AS_T=\{as_i|i=1,2,\cdots\}$，$T$ 时刻的事件型告警集合为 $AE_T=\{ae_i|i=1,2,\cdots\}$，则 T 时刻的告警迹表示为 $Alarm_T=(AS_T,AE_T)$。

定义 5　攻击迹 $Attack_T=(S_T,A',A'')$，用来刻画 T 时刻已发生的攻击行为。其中，S_T 表示 T 时刻因果知识网络中状态为 true 的状态节点集合；A'为已经发生但失败的攻击行为节点集合，本文设置ε为判定攻击行为发生的阈值，即当攻击行为 a_i 的发生概率$\Delta_1(a_i)>\varepsilon$时，判定 a_i 发生，反之认为 a_i 没有发生；A''为发生且成功的攻击行为节点集合。

告警迹是通过融合多源 IDS 的告警并进行漏报误报处理后的告警集合，攻击迹则反映了攻击者已完成的攻击行为，一方面作为推断攻击者能力等级的依据，另一方面是预测攻击者后续攻击路径的基础。实时攻击迹获取的本质是在 CKN 的基础上建立由实时告警迹 $Alarm_T$ 到实时攻击迹 $Attack_T$ 的映射，具体如算法 1 所示。

算法 1　实时攻击迹识别方法

输入　因果知识网络 $CKN=(N,E,\Delta)$，T 时刻告警迹 $Alarm_T=(AS_T, AE_T)$，判定攻击行为发生的阈值ε;

输出　T 时刻的攻击迹 $Attack_T=(S_T,A',A'')$。

1) $Attack_T=Attack_{T-1}$；//初始化的值
2) for(每一个 $as_i\in(AS_T\backslash AS_{T-1})$)
3)　$S_T=S_T\cup\{f_{AS\to S}(as_i)\}$；
4)　$A''=A''\cup\{Pre(f_{AS\to S}(as_i))\}$；
5)　$AE_T=AE_T\backslash\{f_{A\to AE}(Pre(f_{AS\to S}(as_i)))\}$;
6) end for
7) for(每一个 $ae_i\in AE_T$)
8)　if($\Delta_4(f_{AE\to A}(ae_i))>\varepsilon$)
9)　$A'=A'\cup\{f_{AE\to A}(ae_i)\}$；
10) end for
11) return $Attack_T$；

算法 1 在获取 T 时刻的攻击迹时，为了避免重复计算，初始化 $Attack_T$ 为 $Attack_{T-1}$，很好地继承了前一时刻的计算结果，提高了算法的运算效率。第 3)行是通过状态型告警生成 S_T；第 4)行生成攻击发生且成功地攻击行为集合 A''；第 7)行~第 9)行生成攻击发生但失败的攻击行为集合 A'。算法复杂度为 $O(as\_num\cdot S_T\_num+ae\_num\cdot A\_num)$。

3.2　攻击者能力等级实时推断

定义 6　攻击行为结果 $Res\in\{L_{\text{suc}}, L_{\text{fail}}, M_{\text{suc}}, M_{\text{fail}}, H_{\text{suc}}, H_{\text{fail}}\}$。其中，$L_{\text{suc}}$ 表示攻击者成功实施一次攻击行为复杂度为 low 的攻击，M_{fail} 表示攻击者失败实施

一次攻击行为复杂度为 mid 的攻击，以此类推。

攻击行为结果是对实时攻击迹的抽象，能够直观反映攻击者实际的攻击状况，从而为推断攻击者能力等级提供依据。攻击行为结果确定方法如式(7)所示。

$$Res(a_i)=\begin{cases}L_{\text{suc}}, & a_i\in A''且Cpx(a_i)=\text{low}\\ L_{\text{fail}}, & a_i\in A'且Cpx(a_i)=\text{low}\\ M_{\text{suc}}, & a_i\in A''且Cpx(a_i)=\text{mid}\\ M_{\text{fail}}, & a_i\in A'且Cpx(a_i)=\text{mid}\\ H_{\text{suc}}, & a_i\in A''且Cpx(a_i)=\text{high}\\ H_{\text{fail}}, & a_i\in A'且Cpx(a_i)=\text{high}\end{cases} \tag{7}$$

由于网络攻防的实时动态变化，攻击者能力等级与攻防双方的对抗活动紧密相关，且具有客观相对性，故攻击者所处不同能力等级的先验概率相等。由贝叶斯定理得出以下结论。

定理 1 由同一攻击行为结果推断出的攻击者能力等级的概率分布正比于攻击者实施此攻击成功或失败的概率分布。

证明 设同一攻击行为结果 $Res(a_i)$，则由 $Res(a_i)$ 所推断的攻击者能力等级的概率为 $P(Cap(attacker)|Res(a_i))$，攻击成功的概率为 $f(Cpx(a_i),Cap(attacker))$，攻击失败的概率为 $1-f(Cpx(a_i),Cap(attacker))$。由贝叶斯定理知

$$P(Cap(attacter)\,|\,Res(a_i))=\frac{P(Cap(attacter))P(Res(a_i)\,|\,Cap(attacter))}{P(Res(a_i))} \tag{8}$$

又由于攻击者所处的不同能力等级的先验概率 $P(Cap(attacker)$相等，故

$$P(Cap(attacter)\,|\,Res(a_i))\propto P(Res(a_i)\,|\,Cap(attacter)) \tag{9}$$

而当 $Res\in\{L_{\text{suc}}, M_{\text{suc}}, H_{\text{suc}}\}$时，

$$P(Res(a_i)\,|\,Cap)=f(Cpx(a_i),Cap) \tag{10}$$

于是，

$$P(Cap\,|\,Res(a_i))\propto f(Cpx(a_i),Cap) \tag{11}$$

同理，当 $Res\in\{L_{\text{fail}}, M_{\text{fail}}, H_{\text{fail}}\}$时，

$$P(Res(a_i)\,|\,Cap)=1-f(Cpx(a_i),Cap) \tag{12}$$

又有

$$P(Cap\,|\,Res(a_i))\propto 1-f(Cpx(a_i),Cap) \tag{13}$$

综上得证。

由定理 1 能够计算得出由不同攻击行为结果推断攻击者能力等级的概率分布，计算结果如表 2 所示。

3.3 攻击路径实时预测

攻击路径实时预测的形式化表述为：已知因果知识网络 $CKN=(N,E,\Delta)$、T 时刻的攻击迹 $Attack_T$、T 时刻的攻击者能力等级 Cap_T 和攻击目标 $S[y]$，求攻击者从目前状态到达目标 $S[y]$一条攻击路径，使攻击成功的概率最大。

为了解决该问题，首先定义概率邻接矩阵和特殊攻击行为节点列表，然后给出攻击路径实时预测算法，求达目标 $S[y]$的最大可能攻击路径及其攻击成功的概率。

定义 7 概率邻接矩阵 $\boldsymbol{G}$。设 CKN 有 n 个状态型节点，则 $\boldsymbol{G}$ 是一个 $n\times n$ 的矩阵，g_{ij} 表示从状态型节点 i 到状态型节点 j 的攻击行为，如果 $Post(i)\cap Pre(j)=\varnothing$，即表示没有攻击行为节点使状态由 i 转移到 j，则 $g_{ij}=0$；如果 $Post(i)\cap Pre(j)=a_{ij}$，即存在攻击行为 a_{ij} 能使状态由 i 转移到 j，则 $g_{ij}=\Delta_{12}(a_{ij})$。在概率邻接矩阵中忽略特殊攻击行为节点。

定义 8 特殊攻击行为节点列表 L。对于特殊攻击行为节点 a_i，用三元组 $L(a_i)=(Pre(a_i),Post(a_i),\Delta_{12}(a_i))$表示。其中，$Pre(a_i)$表示其前置条件，即不少于 2 个的状态节点；$Post(a_i)$表示其后置条件；$\Delta_{12}(a_i)$表示攻击行为 a_i 发生且成功的概率。如图 1 中的 a_{11} 为特殊攻击行为节点，则其三元组记为 $(S_5\cup S_6,S_9,\Delta_{12}(a_{11}))$。

图 1 表示一个因果知识网络结构，其中，圆表示状态节点，正方形表示攻击行为节点。设 a_1、a_3、

表 2 不同攻击行为结果推断攻击者能力等级的概率分布

x	$P(Cap=x\|Res=y)$					
	$y=L_{\text{fail}}$	$y=L_{\text{suc}}$	$y=M_{\text{fail}}$	$y=M_{\text{suc}}$	$y=H_{\text{fail}}$	$y=H_{\text{suc}}$
x=low	$\frac{5}{9}$	$\frac{5}{21}$	$\frac{7}{15}$	$\frac{3}{15}$	$\frac{9}{21}$	$\frac{1}{9}$
x=mid	$\frac{3}{9}$	$\frac{7}{21}$	$\frac{5}{15}$	$\frac{5}{15}$	$\frac{7}{21}$	$\frac{3}{9}$
x=high	$\frac{1}{9}$	$\frac{9}{21}$	$\frac{3}{15}$	$\frac{7}{15}$	$\frac{5}{21}$	$\frac{5}{9}$

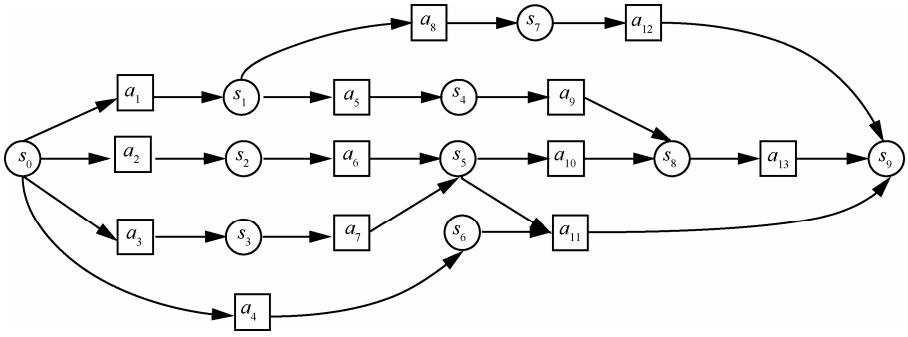


图 1　因果知识网络结构

a_6 攻击行为复杂度为 low；a_2、a_4、a_5、a_7、a_8、a_9、a_{10}、a_{13} 攻击行为复杂度为 mid；a_{11}、a_{12} 攻击行为复杂度为 high。对于一个攻击能力等级为 mid 的攻击者而言，特殊攻击行为节点列表为$(S_5 \cup S_6, S_9, 0.3)$，概率邻接矩阵如图 2 所示。

$$\boldsymbol{G}=\begin{pmatrix}0 & 0.7 & 0.5 & 0.7 & 0 & 0 & 0.5 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0.5 & 0 & 0 & 0.5 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0.7 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.3\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\end{pmatrix}$$

图 2　概率邻接矩阵

经典的 Dijkstra 算法常用于计算有向图中一个顶点到其他所有顶点的最短路径。攻击路径预测算法的本质同 Dijkstra 算法类似，只是由于特殊攻击行为节点的存在，使常规的邻接矩阵无法完整表示攻击信息，且攻击路径预测算法只需计算目标节点与攻击迹中集合 S 的最短攻击路径。因此，本文在 Dijkstra 算法的基础上，首先利用概率邻接矩阵求可能的攻击路径预测结果，然后结合特殊攻击行为节点列表进行修正来实现对攻击路径的实时预测。具体算法如下。

算法 2　攻击路径实时预测算法

输入　概率邻接矩阵 $\boldsymbol{G}$，特殊攻击行为节点列表 L，攻击目标 $S[y]$，T 时刻的攻击迹 $Attack_T$;

输出　最大可能攻击路径 *Path* 及攻击成功的概率 *MaxProb*。

1) (*Path*,*MaxProb*)= *ProbPath*[*S*[*y*]] ;

2) if (存在特殊攻击行为节点 a_i 在路径 *ProbPath*[*S*[*y*]].*Path* 中)

3) $Prob(a_i)=\Delta_{12}(a_i)\ \Pi ProbPath(S[i].MaxProb)$其中，$S[i]\in Pre(a_i)$;

4) if ($Prob(a_i)>ProbPath[Post(a_i)].MaxProb$);

5) $Path=(Path\backslash Path[L.Post(a_i)])\cup$each $Path[S[i]]$;

6) $MaxProb = MaxProb / ProbPath\ [Post(a_i)].MaxProb\cdot Prob(a_i)$; //更新路径及概率

7) return *Path* and *MaxProb*;

求解可能攻击路径函数 *ProbPath* 的定义如下。

1) *ProbPath* (*S*[*x*])

2) *Path*=null; *MaxProb*=0; add *S*[*x*] to $Path_0$;

3) for (int $i=x-1$; $i>0$; i−−)

4)　float $MaxProb_0=0$; int $u=x$;

5)　for (int $j=1$; $j<n$; ++j)

6)　　if($S[j]\notin Path_0$ && $Prob[j]>0$)

7)　　$u=j$; $MaxProb_0= Prob[j]$;

8)　end for

9)　add *S*[*u*] to $Path_0$;　//将节点加入路径中

10)　for (int $j=1$; $j<n$; j++)

11)　　if ($S[j]\notin Path_0$ && $\boldsymbol{G}[j][u]>0$)

12)　　if ($Prob[u]\boldsymbol{G}[j][u]>Prob[j]$)

13)　　$Prob[j]=Prob[u]\ \boldsymbol{G}[j][u]$;

14)　end for

15)　if ($S[u]\in Attack_T$)

16)　　$Path =Path_0$; $MaxProb =MaxProb_0$;

17) end for

18) return (*Path*, *MaxProb*); //返回有效路径及其攻击成功的概率

算法 2 借鉴了 Dijkstra 算法在求有向图中单源最短路径的有效性，设计了 *ProbPath* 函数来计算概率邻接矩阵中源到点集之间的最短路径。整个算法主要分为 2 步。

1) 算法 2 第 1)行调用 *ProbPath* 函数，依据概率邻接矩阵求得已知攻击迹 $Attack_T$ 到攻击目标 $S[y]$ 的可能路径，然而由于特殊攻击行为节点的存在，使算法 2 第 1)行中获得的路径可能并不准确。

2) 算法 2 第 2)~7)行根据特殊攻击行为节点列表，判断第 1)行中获取的攻击路径中是否包含特殊攻击行为节点，若存在，则将此路径变换为含有特殊攻击行为节点的路径，并通过比较二者攻击成功的概率大小进行选择，最终确定最大可能攻击路径 *Path* 和其攻击成功的概率 *MaxProb*。

本算法与 Dijkstra 算法复杂度相同，都为 $O(n^2)$，即为因果知识网络中状态节点个数的平方。

4 实验分析

4.1 实验环境

为了验证本文方法的有效性，搭建了一个实际网络环境来进行测试。实验环境拓扑如图 3 所示。

外网用户可通过 Internet 访问本网络。实验网络分为 4 个区域，分别是 DMZ 区、子网 1、子网 2 和子网 3。DMZ 区包含 Web 服务器和 E-mail 服务器。子网 1 由 2 台主机构成。子网 2 由一台工作站和文件服务器组成。子网 3 包括一台工作站和数据库服务器。各区域的 IDS 负责检测各区域中的异常行为并产生告警。网络可达性设为：DMZ 区由防火墙 1 保护并连接 Internet，且只能访问子网 1 中的主机 1、子网 2 中的文件服务器和子网 3 中的数据库服务器；子网 1 中的主机 1 能够访问子网 2 和 3 中的所有机器，主机 3 只能访问主机 1 和数据库服务器，主机 2 只能访问主机 3；子网 2 中的工作站 1 和子网 3 中的工作站 2 能访问数据服务器和文件服务器。通过 Nessus 脆弱点扫描器对网络各网络段进行扫描，得到各主机中漏洞信息如表 3 所示。依据漏洞信息和 CVSS 分析得出的攻击行为信息如表 4 所示。

4.2 实验结果及分析

4.2.1 计算过程及分析

根据图 3 和表 4，确定因果知识网络基本结构。假定攻击目标是获取主机 3 的 root 权限，设计了 3 个实验进行验证，实验结果如表 5 所示。具体推理过程如图 4 所示。图 5 则展示了实验中各个状态节点攻击成功概率变化情况。

为了不失一般性，假定实验 1 中没有观测到任何事件，即 $Alarm_T$=null。由算法 2 知，共有 6 条攻击路径能够实现攻击目标，分别为 path1: $s_1\rightarrow a_1\rightarrow s_2\rightarrow a_5\rightarrow s_8\rightarrow a_{13}\rightarrow s_9$、path2: $s_1\rightarrow a_1\rightarrow s_2\rightarrow a_3\rightarrow s_4\rightarrow a_6\rightarrow s_6\rightarrow a_{11}\rightarrow s_8\rightarrow a_{13}\rightarrow s_9$、path3: $s_1\rightarrow a_1\rightarrow s_2\rightarrow a_4\rightarrow s_5\rightarrow a_7\rightarrow s_6\rightarrow a_{11}\rightarrow s_8\rightarrow a_{13}\rightarrow s_9$、path4: $s_1\rightarrow a_1\rightarrow s_2\rightarrow a_4\rightarrow s_5\rightarrow a_8\rightarrow s_7\rightarrow a_{12}\rightarrow s_8\rightarrow a_{13}\rightarrow s_9$、path5: $s_1\rightarrow a_1\rightarrow s_2\rightarrow a_4\rightarrow s_5\rightarrow a_{10}\rightarrow s_8\rightarrow a_{13}\rightarrow s_9$ 和 path6: $s_1\rightarrow a_2\rightarrow s_3\rightarrow a_1\rightarrow s_2\rightarrow a_4\rightarrow s_5\rightarrow a_9\rightarrow s_9$。对于攻击能力等级为 Low 的攻击者的最有可能攻击路径为 path5，攻击成功率为 0.023；对于攻击能力等级为 mid 的攻击者的最有可能攻击路径同样为 path5，但攻击成功率提高到 0.123；对于攻击能力等级为 high 的攻击者最有可能攻击路径为 path4s，攻击成功率为 0.459。对于实验 2，T 时刻观测到的告警为 $Alarm_T=(as_2,ae_2,\ ae_5)$，由算法 1 得出攻击者的攻击迹描述为攻击者成功发动攻击

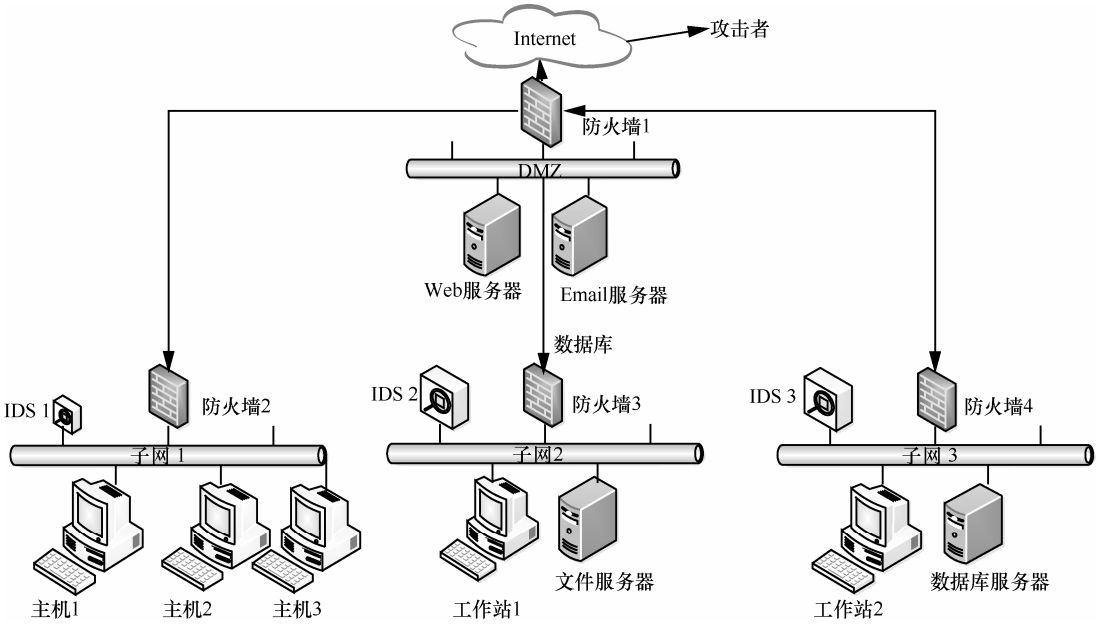


图 3 实验网络拓扑

表 3　　各主机信息及其所含漏洞信息

主机编号	主机信息	漏洞编号	CVE 编号	漏洞描述	漏洞利用攻击编号
H_1	Web 服务器，Apache	V_1	CVE-2013-2249	模块安全漏洞	a_1
		V_2	CVE-2013-3940	图形设备接口整数溢出漏洞	a_6，a_7
		V_3	CVE-2013-5065	内核中的漏洞允许特权提升	a_{11}
H_2	主机 1，Microsoft Windows XP SP2	V_4	CVE-2012-0002	远程桌面协议代码执行漏洞	a_{12}
		V_5	CVE-2013-1727	Mozilla Firefox 安全绕过漏洞	a_5
		V_6	CVE-2007-6473	基于堆的缓冲区溢出漏洞	a_{10}
H_3	主机 2，Microsoft Windows 7 SP2	V_7	CVE-2011-0638	USB 数据任意程序执行漏洞	a_2
H_4	主机 3，Red Hat	V_8	CVE-2014-6271	GNU Bash 远程代码执行漏洞	a_{13}
		V_9	CVE-2012-6137	SSL 证书验证安全绕过漏洞	a_9
H_5	文件服务器，Windows 2000, HFS	V_{10}	CVE-2014-6287	HFS 代码注入漏洞	a_3
H_6	工作站 2，Windows 2000, Funk Proxy v3.0	V_{11}	CVE-2002-0065	Funk 软件代理弱密码存储漏洞	a_8
H_7	数据库服务器，Windows Server 2003	V_{12}	CVE-2004-0119	远程缓冲区溢出漏洞	a_4

表 4　　攻击行为节点的信息

漏洞利用攻击编号	前提条件	后置结果	利用的漏洞（CVE 编号）	攻击行为复杂度
a_1	外部用户	(H_1,root)	CVE-2013-2249	低
a_2	外部用户	(H_3,root)	CVE-2011-0638	高
a_3	(H_1,root)	(H_5,root)	CVE-2014-6287	低
a_4	(H_1,root)	(H_7,root)	CVE-2004-0119	低
a_5	(H_1,root)	(H_2,root)	CVE-2013-1727	高
a_6	(H_5,root)	(H_2,user)	CVE-2013-3940	中
a_7	(H_7,root)	(H_2,user)	CVE-2013-3940	中
a_8	(H_7,root)	(H_6,root)	CVE-2002-0065	低
a_9	(H_1,root), (H_3,root)	(H_4,root)	CVE-2012-6137	低
a_{10}	(H_7,root)	(H_2,root)	CVE-2007-6473	中
a_{11}	(H_2,user)	(H_2,root)	CVE-2013-5065	低
a_{12}	(H_6,root)	(H_2,root)	CVE-2012-0002	低
a_{13}	(H_2,root)	(H_4,root)	CVE-2014-6271	中

表 5　　实验结果

编号	T 时刻的告警迹	攻击者能力等级	最大可能后续攻击路径
1	$Alarm_T$=null	low	$s_1\to a_1\to s_2\to a_4\to s_5\to a_{10}\to s_8\to a_{13}\to s_9$
		mid	$s_1\to a_1\to s_2\to a_4\to s_5\to a_{10}\to s_8\to a_{13}\to s_9$
		high	$s_1\to a_1\to s_2\to a_4\to s_5\to a_8\to s_7\to a_{12}\to s_8\to a_{13}\to s_9$
2	$Alarm_T$=(as_2,ae_2, ae_5)	mid	$s_2\to a_4\to s_5\to a_{10}\to s_8\to a_{13}\to s_9$
3	$Alarm_T$=(as_2,as_5,ae_1, ae_4, ae_{10})	high	$s_5\to a_8\to s_7\to a_{12}\to s_8\to a_{13}\to s_9$

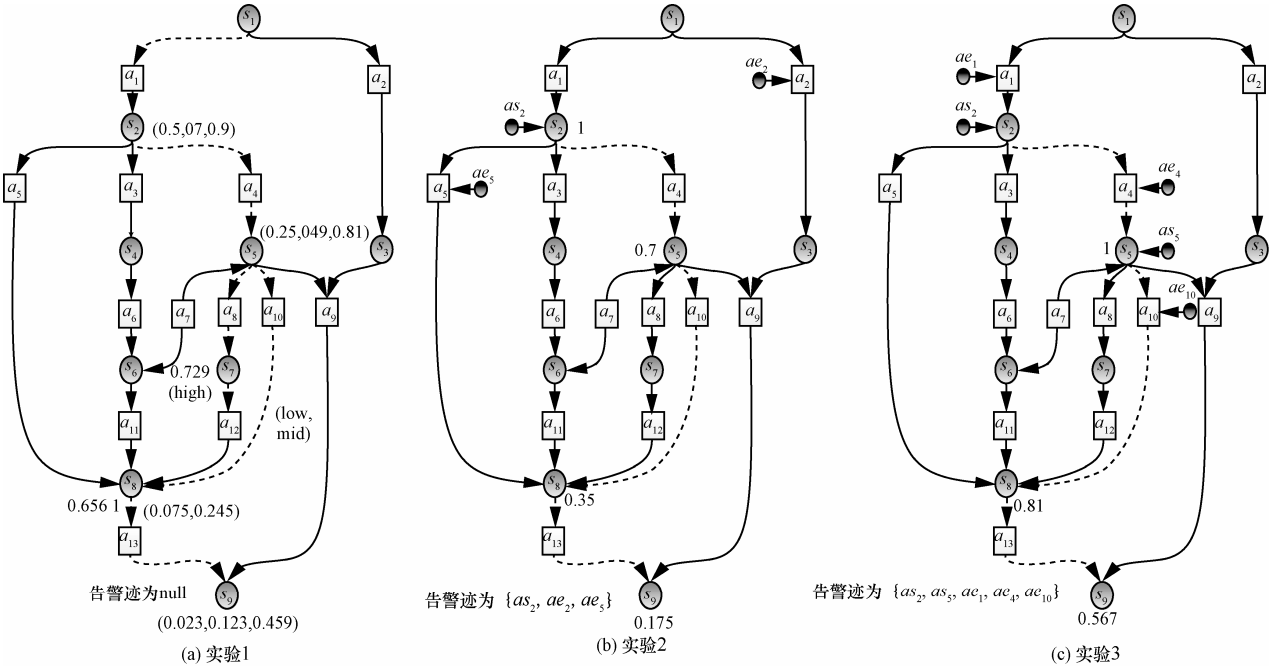


图 4　不同告警迹条件下攻击路径推断过程示意

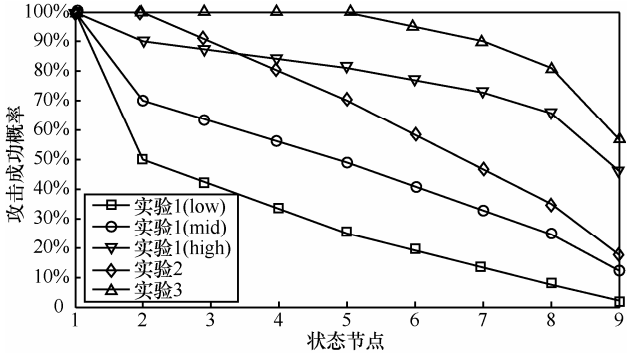


图 5　实验中各个状态节点攻击成功概率

行为 a_1 使攻击状态达到 s_2，但发动攻击 a_2 时遭遇了失败，这个概率达到 0.95。由算法 2 推断攻击者的攻击能力等级为 mid，由算法 3 能得出攻击者最有可能的后续攻击路径为：$s_2 \rightarrow a_4 \rightarrow s_5 \rightarrow a_{10} \rightarrow s_8 \rightarrow a_{13} \rightarrow s_9$，攻击成功的概率为 0.175。对于实验 3，$T$ 时刻观测到的告警为 $Alarm_T=(as_2,as_5,ae_1,ae_4,ae_{10})$，由算法 1 得出攻击者的攻击迹描述为：攻击者成功实施攻击行为 a_1 和 a_4 使攻击状态达到 s_5，但发动攻击 a_{10} 时遭遇了失败，这个概率达到 0.95。由算法 2 推断攻击者的攻击能力等级为 high，由算法 3 能得出攻击者最有可能的后续攻击路径为：$s_5 \rightarrow a_8 \rightarrow s_7 \rightarrow a_{12} \rightarrow s_8 \rightarrow a_{13} \rightarrow s_9$，攻击成功的概率为 0.567。对于本文提出的模型而言，随着时间的不断推进，攻击者暴露的攻击行为越多，攻击迹越完整，对攻击者能力的推断越合理，后续攻击路径的预测也就更准确。

4.2.2　测试结果的比较与分析

利用网络安全专业的 50 名学员作为攻击者，分别就图 3 所示的网络进行攻击测试实验，事先给定攻击者该网络的拓扑结构、漏洞信息及因果知识网络结构。每名攻击者均尝试因果知识网络中的 6 条攻击路径，总共形成 300 个攻击迹。本文算法计算结果与攻击测试实验统计结果对比如表 6 所示。

依据 50 名攻击者的攻击迹，利用本文的攻击者能力等级推断算法能够将这些攻击者分类 3 类：攻击者能力等级为 low 的学员 9 人、攻击者能力等

表 6　　**本文算法计算结果与攻击测试实验统计结果对比**

攻击者能力	攻击成功概率					
	path1	path2	path3	path4	path5	path6
low	(0.015，0)	(0.011，0)	(0.011，0.111)	(0.019，0)	(0.023，0.111)	(0.013，0)
mid	(0.105，0.108)	(0.086，0.081)	(0.086，0.081)	(0.120，0.108)	(0.123，0.135)	(0.103，0.108)
high	(0.315，0.25)	(0.357，0.25)	(0.357，0.25)	(0.459，0.50)	(0.397，0.25)	(0.365，0.25)

级为 mid 的学员 37 人和攻击者能力等级为 high 的学员 4 人。表 6 每一组结果由 2 个数字构成：前者表示利用本文算法得出的不同能力等级的攻击者利用不同攻击路径的攻击成功概率；后者带下划线，表示由攻击测试实验统计得出的实际攻击成功概率，如 0 表示 9 名能力等级 low 的攻击者中没有 1 名能够攻击成功；0.108 表示 37 名能力等级为 mid 的攻击者中有 4 名攻击成功，实际攻击成功概率为 $\frac{4}{37}\approx 0.108$。由表 6 的统计结果对比分析得出以下结论。

1) 不同能力等级的攻击者之间攻击成功概率有着较大差别，故本文通过区分攻击者能力进行细粒度的攻击路径预测方法有重要意义。

2) 由于攻击者数目等客观条件约束的影响，本文算法计算的结果与攻击测试实验统计结果有一定的差异，但本文算法计算结果能够较为准确地反映实际的攻击成功概率，能够从攻击者角度有效预测攻击路径，为网络安全漏洞修复及实时防护提供依据。

此外，本文与文献[9]和文献[10]的算法进行了比较。一方面利用文献[9]的方法计算本文因果知识网络中最有可能攻击路径为 path2,攻击成功的概率为 0.256，明显大于实际攻击成功概率；另一方面依据文献[9]的攻击图，在没有任何监测事件时，本文算法得出无论攻击者能力处于哪个等级，最大可能攻击路径都为：$s_0\rightarrow a_{10}\rightarrow s_7\rightarrow a_8\rightarrow s_8\rightarrow a_9\rightarrow s_9\rightarrow a_5\rightarrow s_5$，结果与文献[9]的算法一致，然而文献[9]的算法中所定义的累积概率是指达到当前攻击状态或发生当前攻击行为的整个可能性，即累加所有可能攻击路径的概率之和，这与攻击者往往选择一条确定的攻击路径这一实际不符，造成最终计算的攻击成功概率往往偏高，而本文采用的改进 Dijkstra 算法，通过比较每一条可能攻击路径的概率确定最有可能攻击路径，得到的攻击成功概率相对准确合理。

文献[10]利用威胁状态转移图进行实时威胁状态识别时，在推断出目前的威胁状态后，进一步推断 6 条可能的后续路径，而利用本文的算法，根据攻击者已完成的威胁，推断此攻击者的攻击能力等级为 high，进而推断最有可能的攻击路径为 $s_0\rightarrow a_1\rightarrow s_1\rightarrow a_5\rightarrow s_3\rightarrow a_6\rightarrow s_7\rightarrow a_3\rightarrow s_8\rightarrow a_8\rightarrow s_{10}$ 和 $s_0\rightarrow a_1\rightarrow s_1\rightarrow a_5\rightarrow s_3\rightarrow a_6\rightarrow s_7\rightarrow a_7\rightarrow s_8\rightarrow a_8\rightarrow s_{10}$，攻击成功概率为 0.49。横向比较来看，本文的方法优势在于能够根据攻击者能力等级自适应地调整相关概率知识，符合网络对抗实际，更具合理性。

5　结束语

由于网络攻防的动态性和复杂性，攻击路径预测具有不确定性。针对现有攻击路径预测方法无法准确反映攻击者攻击能力对后续攻击路径影响这一问题，本文提出一种基于因果知识网络的攻击路径预测方法。该方法利用因果知识网络模型对攻击行为建模，网络结构定性反映了攻击步骤之间的因果关系，概率知识分布则定量反映了因果知识网络中的不确定性。首先将告警迹映射到因果知识网络以识别攻击迹；然后通过分析实时攻击迹推断攻击者能力等级，进而根据攻击者能力等级自适应调整概率知识分布；最后利用概率知识推理攻击者最有可能的攻击路径。实验结果表明该方法能够提高攻击路径预测的准确度，有效减少告警数量，为网络管理员及时实施防御策略提供了重要依据。下一步工作包括因果知识网络结构的生成研究和实现算法的并行化。

参考文献：

[1] SHAH C. Zeus crime ware toolkit[EB/OL]. http://blogs.mcafee.com/mcafeelabs/zeus-crimeware-toolkit.

[2] QIN X, LEE W. Statistical causality of INFOSEC alert data[C]// Recent Advances in Intrusion Detection 2003. Berlin, 2003: 73-93.

[3] 梅海彬, 龚俭, 张明华. 基于警报序列聚类的多步攻击模式发现研究[J]. 通信学报, 2011, 32 (5): 63-69.
MEI H B, GONG J, ZHANG M H. Research on discovering multi-step attack patterns based on clustering IDS alert sequences[J]. Journal on Communications, 2011, 32(5): 63-69.

[4] VALEUR F, VIGNA G, KRUEGEL C, et al. A comprehensive approach to intrusion detection alert correlation[J]. IEEE Trans. Dependable and Secure Computing, 2004, 1(3): 146-169.

[5] JAJODIA S, NOEL S, KALAPA P, et al. Cauldron: mission-centric cyber situational awareness with defense in depth[C]//The Military Communications Conference. Baltimore, 2011: 1339-1344.

[6] YU D, FRINCKE D. Improving the quality of alerts and predicting intruder's next goal with hidden colored petri-net[J]. Computer Networks, 2007,51(3): 632-654.

[7] WANG L, ISLAM T, LONG T, et al. An attack graph-based probabilistic security metric[C]//Data and Applications Security XXII. Berlin Heidelberg, 2008: 283-296.

[8] 苏婷婷, 潘晓中, 肖海燕. 基于属性邻接矩阵的攻击图表示方法研究[J]. 电子与信息学报, 2012, 34(7): 1744-1747.
SU T T, PAN X Z, XIAO H Y. Research on attack graph based on at-

tributes adjacncy matrix[J]. Journal of Electronics & Information Technology, 2012, 34(7): 1744-1747.

[9] 陈小军, 方滨兴, 谭庆丰. 基于概率攻击图的内部攻击意图推断算法研究[J]. 计算机学报, 2014, 37(1): 62-72.
CHEN X J, FANG B X, TAN Q F. Inferring attack intent of malicious insider based on probabilistic attack graph model[J]. Chinese Journal of Computers, 2014, 37(1): 62-72.

[10] 吕慧颖, 彭武, 王瑞梅. 基于时空关联分析的网络实时威胁识别与评估[J]. 计算机研究与发展, 2014, 51(5): 1039-1049.
LV H Y, PENG W, WANG R M. A real-time network threat recognition and assessment method based on association analysis of time and space[J]. Journal of Computer Research and Development, 2014, 51(5): 1039-1049.

[11] XIE P, LI J H, OU X M, et al. Using Bayesian networks for cyber security analysis[C]//The 40th IEEE/IFIP International Conference on Dependable Systems and Networks(DSN). Chicago, 2010: 211-220.

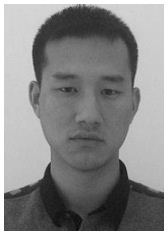
[12] 张少俊, 李建华, 宋珊珊. 贝叶斯推理在攻击图节点置信度计算中的应用[J]. 软件学报, 2010, 21(9): 2376-2386.
ZHANG S J , LI J H, SONG S S. Using Bayesian inference for computing attack graph node beliefs[J]. Journal of Software, 2010, 21(9): 2376-2386.

[13] ABRAHAM S, NAIR S. A predictive framework for cyber security analytics using attack graphs[J]. International Journal of Computer Networks & Communications, 2015, 7(1): 1-17.

[14] FREDJ O B. A realistic graph-based alert correlation system[J]. Security and Communication Network, 2015, 8(15): 2477-2493.

[15] 冯学伟, 王东霞, 黄敏桓. 一种基于马尔可夫性质的因果知识挖掘方法[J]. 计算机研究与发展, 2014, 51(11): 2493-2504.
FENG X W, WANG D X, HANG M H. A mining approach for causal knowledge in alert correlating based on the Markov property[J]. Journal of Computer Research and Development, 2014, 51(11): 2493-2504.

作者简介:



王硕（1991-），男，河南南阳人，解放军信息工程大学硕士生，主要研究方向为网络安全。

汤光明（1963-），女，湖南常德人，解放军信息工程大学教授，博士生导师，主要研究方向为网络信息安全和体系对抗。

寇广（1983-），男，河南许昌人，解放军信息工程大学讲师，主要研究方向为网络安全态势感知、大数据和云计算安全。

宋海涛（1990-），男，山东烟台人，解放军信息工程大学博士生，主要研究方向为网络安全。