计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2018.20160940
55(12):2620-2636,2018

基于因果知识网络的攻击场景构建方法

王 硕 汤光明 王建华 孙怡峰 寇 广
(解放军信息工程大学 郑州 450001)
(WaltShuo@163.com)

Attack Scenario Construction Method Based on Causal Knowledge Net

Wang Shuo, Tang Guangming , Wang Jianhua, Sun Yifeng, and Kou Guang
(*PLA Information Engineering University*, *Zhengzhou* 450001)

Abstract In view of the problem that the existing attack scenario construction methods are not accurate due to the lack of consideration of alarm missing and alarm redundancy, a new attack scenario construction method based on causal knowledge net is put forward. The causal knowledge net is composed of causal relationship and causal knowledge. Firstly, the causal relationship of single-step attacks is defined according to the expert knowledge, and then the real alarms are utilized to mine the causal knowledge, which can be used to quantitatively describe the causal relationship. In particular, the significance testing mean is designed to guarantee the consistency and accuracy of the causal relationship as well as causal knowledge among the mining causal knowledge. Additionally, the attack scenario construction method can be divided into two different steps with the help of causal knowledge net: the initiatory attack scenario can be obtained by means of alarm mapping and clustering in the first step, and in the second step, the initiatory attack scenario is reconstructed and the intact attack scenario is achieved by taking advantage of the theory named maximum a posteriori estimation. Experimental results show that the proposed method can improve the accuracy of attack scenario construction by combining the advantages of expert knowledge and data mining.

Key words attack scenario construction; causal knowledge network; data mining; alarm; maximum a posteriori estimation

摘 要 针对现有因告警缺失及冗余造成的攻击场景构建不准确的问题,提出了基于因果知识网络的攻击场景构建方法.首先依据专家知识定义因果关系,利用真实告警数据挖掘出能够定量刻画因果关系的因果知识,并对其进行显著性检验,以保证因果关系与因果知识的一致性和准确度,进而构成因果知识网络;然后借助因果知识网络,将攻击场景的构建分为初建与重构2步:1)通过告警映射与聚类定性得到初步的攻击场景;2)利用最大后验估计原理对其进行定量推理重构,得到完整的攻击场景.实验结果表明:该方法能利用专家知识和数据挖掘相结合的优势能够提高攻击场景构建的准确度.

关键词 攻击场景构建;因果知识网络;数据挖掘;告警;最大后验估计

中图法分类号 TP393.8

在当今这个全球化的时代,网络技术就像整个社会的神经,深刻影响着国际政治、经济、文化、社会、军事等领域的发展.随着网络结构日趋复杂、规模日渐庞大,入侵过程也向复杂性、多样性和分布性

收稿日期:2016-12-09;**修回日期**:2018-02-24
基金项目:国家自然科学基金项目(61303074)
This work was supported by the National Natural Science Foundation of China (61303074).

的趋势发展.根据国家计算机网络应急技术处理协调中心的年度网络安全工作报告[1],近几年来大部分攻击尤其是危害大的攻击几乎都是复杂的多步攻击.对于复杂的多步攻击,攻击者对网络目标设施的渗透破坏过程往往是渐进的,通过执行多个攻击步骤实现最终目的,使得传统的面向单个安全事件检测的网络安全设备失效.多步攻击成为目前网络攻击主要手段之一,严重危害着网络信息安全.攻击场景构建技术将庞杂、无序的告警流转换为易于理解的攻击场景,大大提高了告警信息的可用性,能够为发现攻击者的攻击策略和预测下一步可能的攻击行为提供依据,便于管理员做出及时有效的应急响应.因此,研究如何掌握攻击活动的全貌、重建攻击场景是应对多步攻击威胁的重要手段,并逐渐成为网络安全防御领域的研究热点.

攻击场景构建是对告警事件的实际分析和应用,实现攻击场景重建的方法为告警关联.告警关联是将经过告警聚合和告警确认后的超告警与网络的实际背景知识相结合,挖掘出其中存在的真正网络威胁和安全事件,进而揭示出各个安全事件背后的逻辑关联,发掘攻击者的真正攻击意图.目前,基于告警关联的攻击场景构建方法主要分为3类:1)基于机器学习的方法[2-3].构建的攻击场景虽然对专家知识依赖较少,但存在准确度低、结果难以理解、计算量大和实时性差等缺陷.2)基于已知攻击场景的方法[4-5].虽然准确度相对较高,但是事先获得攻击过程和关联规则比较困难,此外这种方法无法检测出未知攻击场景的多步攻击行为.3)通过原子攻击前因后果关系进行关联的方法[6-8].只需获取原子攻击的前因后果关系,不必事先知道整个攻击过程,更加灵活,同时这种方法可以识别和检测不同原子攻击组合形成的新攻击过程,因此成为目前攻击场景构建技术的研究趋势.

目前,通过原子攻击前因后果关系进行关联的方法的难点主要体现在2方面:前因后果关系的获取和关系强度的设定.对于定性的前因后果关系的研究相对已经成熟,受到认可的模型有攻击图[7]、攻击树[9]、Markov链[10]、Petri网[11]等,尤其以攻击图模型最为流行.而针对定量关系强度的设定,目前的研究还不充分,主要思路有2种:1)利用安全脆弱点评估系统(common vulnerability scoring system,CVSS)中的相关指标设定[12];2)利用数据挖掘从告警数据中提取概率.前者仅仅是利用专家知识给出的所有网络的共性度量,主观性较强.鉴于此,王硕等人[13]提出了依据攻击者能力动态调整攻击图中边概率的方法,但其概率设定的原始依据仍是CVSS,并不一定适合具体的网络攻防环境.随着大数据技术的崛起,针对后者的研究相对较多.具体来讲,李之堂等人[14]将告警用它对应的攻击类型属性进行替换,进而利用概率统计挖掘攻击场景,然而由于不同的单步攻击可能有着同样的攻击类型,因此其挖掘出来的概率准确度有待进一步提高.吴庆涛等人[15]提出了一种改进的基于因果关联的攻击场景重构方法,该方法根据告警相关度确定可组合的关联图,利用网络弱点和攻击关系推出漏告警,使得分裂的关联图能够组合起来,进而重建完整的攻击场景;然而,文中并没有考虑误告警的情况.马琳茹等人[16]提出一种基于属性层次树的相似度隶属函数定义方法,用模糊聚类的方法实现攻击场景重构;然而只是将关联图简单地组合起来,而没有对漏掉的攻击进行假设和推理.刘敬等人[17]针对传统网络安全事件分析方法较多依赖人工干预的问题提出了利用神经网络和遗传算法相结合的网络安全事件分析方法,具有较高的自适应能力和自动化程度;然而文中所定义的攻击模式和攻击场景相对简单,不便于网络管理员理解.刘威歆等人[18]综合利用图关系和阈值限制进行联动推断和预测,达到更为全面解决攻击图中的告警漏报和减少误报的目的,然而由于攻击图节点之间的关联强度仅仅依靠相邻节点的消息强度和消息方向累积获取,只能定性分析最大可能攻击路径而不能定量分析其攻击成功的概率.胡亮等人[19]将智能规划的方法应用于多步攻击识别的领域,并以此为基础实现相应的识别算法,但算法没有考虑到漏报误报情况下的求解问题.

综上分析得出,如何从漏报误报的告警流中构建完整的攻击场景仍然是一个极具挑战性的问题.针对此问题,本文提出了基于因果知识网络的攻击场景构建方法.一方面利用有向无环图定义原子攻击中的因果关系;另一方面利用真实告警数据挖掘出能够定量刻画因果关系的因果知识,进而将攻击场景的构建分为初建与重构2步,定性与定量相结合,利用最大后验估计原理重构完整的攻击场景.

1　因果知识网络模型

基于因果知识网络的攻击场景构建方法的核

心思想是通过构建因果知识网络,并从告警数据中挖掘出合理的因果知识,进而利用因果知识网络进行攻击场景的推理与构建.模型总体框架如图1所示:

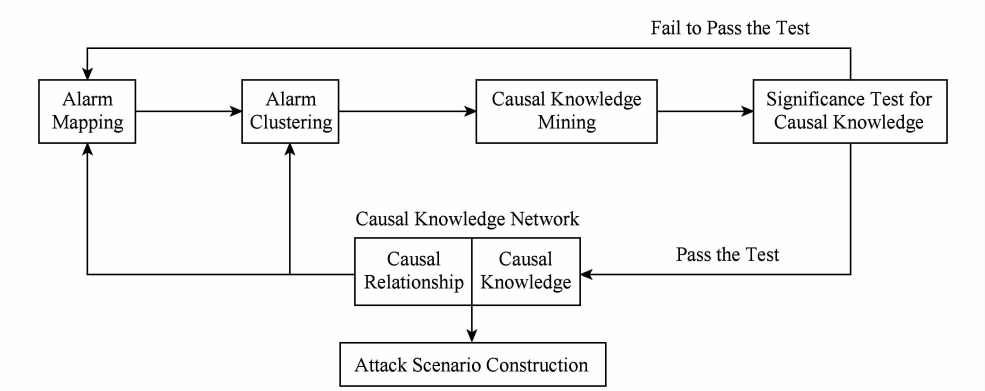

Fig. 1 The overall framework of attack scenario construction method based on causal knowledge network

图1 基于因果知识网络的攻击场景构建方法总体框架

该方法整体分为4个过程:

1)告警映射及聚类.告警映射将告警转换为因果知识网络的节点,用于描述因果知识网络中攻击行为发生的状况;告警聚类将属于同一攻击场景的告警聚为一类,防止告警数据的混乱.通过告警映射及聚类将告警数据转化为按时间排列的节点序列,为因果知识挖掘和攻击场景构建作准备.

2)因果知识挖掘.基于Markov链模型,对节点序列间的一步转移概率进行挖掘,得到初步的因果知识.

3)因果知识的显著性检验.利用基于成对数据的t检验方法对挖掘得到的初步因果知识进行假设检验.若通过检验,则认为因果知识合理;若没有通过检验,则认为因果知识不合理,需要利用扩大告警数据集等方法进行重新挖掘,直到通过显著性检验.

4)攻击场景构建.基于因果知识网络,利用最大后验估计原理,进行攻击场景的构建.

为了方便表述,首先给出一些关键定义.

定义1. 因果知识网络$G_k=(G,K)$.其中$G=(Node,E)$为有向无环图,用于表示因果关系,$Node$是因果知识网络中所有节点的集合;E是连接节点的边的集合,代表节点间即单步攻击之间的关联关系;K是概率知识的集合,表示由当前节点状态转移到下一节点状态的概率,用于量化攻击节点之间的关联关系.

定义2. 节点集$Node=\{s_i\mid i=1,2,\cdots\}\cup\{v_i\mid i=1,2,\cdots\}$.节点集是因果知识网络中状态型节点$s$和攻击行为节点$v$的集合.节点序列指节点集中的若干节点按时间顺序排列而成的序列,用$Nodeseq$表示.

定义3. 告警$a_i=(timestamp,srcIP,srcPort,desIP,desPort,Alarmtype,Class)$表示为七元组.其中,$timestamp$为告警产生的时间,不同网络安全设备的时间要进行统一校对以保证$timestamp$的准确性;$srcIP$和$srcPort$分别为告警的源IP地址和源端口;$desIP$和$desPort$分别为告警的目的IP地址和目的端口;$Alarmtype$为告警的类型,分为状态型告警和事件型告警2种.状态型告警主要反映攻击者拥有的攻击资源及权限能力,由当前网络安全配置及防火墙等网络安全设备获取,状态型告警映射为因果知识网络中的状态节点;事件型告警主要反映攻击者实施的攻击行为,由入侵检测系统等网络安全设备获取,事件型告警映射为因果知识网络中的攻击行为节点.本文设定$Alarmtype=1$表示状态型告警,而$Alarmtype=0$表示事件型告警.$Class$为告警的具体种类,如状态型告警可分为拥有非法权限、非法网络连接等;事件型告警可分为漏洞扫描、缓冲区攻击、DOS攻击等.

定义4. 告警集$Alarm=\{a_i\mid i=1,2,\cdots\}$.告警集是由入侵检测系统等网络安全设备产生的告警集合,则时间窗T内获取的告警集表示为$Alarm^T$.

定义5. 攻击场景$Attack=\{Attackseq_i=s_i^1\rightarrow v_i^1\rightarrow s_i^2\rightarrow v_i^2\rightarrow\cdots\mid i=1,2,\cdots\}$.其中,$Attackseq_i=s_i^1\rightarrow v_i^1\rightarrow s_i^2\rightarrow v_i^2\rightarrow\cdots$表示编号为$i$的攻击序列,它由因果知识网络中的状态型节点$s$和攻击行为节点$v$交错排列而成,是因果知识网络中的1个小片段.由于在一段时间内,可能由多个攻击者同时对目标网络发动入侵活动,且每个攻击者可能在攻击过程中改变攻击策略,故1个攻击场景可能包含1个或多个不同的攻击序列,即攻击场景是攻击序列

$Attackseq_i$ 的集合.特别地,时间窗 T 内攻击场景表示为 $Attack^T=\{Attackseq_i^T=s_i^1\rightarrow v_i^1\rightarrow s_i^2\rightarrow v_i^2\rightarrow\cdots\mid i=1,2,\cdots\}$.

2　基于因果知识网络的攻击场景构建方法

2.1　告警映射及聚类

告警映射是将告警映射到因果知识网络中的节点,即将告警集 $Alarm$ 转化为节点集 $Node$ 的过程.由于 $timestamp$ 反映了攻击发生的时间;源和目的 IP 地址反映了攻击发生的位置;$Class$ 反映了攻击所用的方法,它们共同决定了一次单步攻击行为.因此,本文利用告警的源 IP、目的 IP、告警类型及种类作为告警映射的条件,具体的告警映射方法为

$$map(a)\rightarrow\begin{cases}s,\ Alarmtype(a)=1\ 且\ \exists s\in G,\\ \quad (srcIP(a)=srcIP(s))\wedge\\ \quad (desIP(a)=desIP(s))\wedge\\ \quad (Class(a)=Class(s)),\\ v,\ Alarmtype(a)=0\ 且\ \exists\\ \quad v\in G,(srcIP(a)=srcIP(v))\wedge\\ \quad (desIP(a)=desIP(v))\wedge\\ \quad (Class(a)=Class(v)),\\ \varnothing,\ \text{else}.\end{cases}\tag{1}$$

为了区分不同时间发生的攻击行为,将告警的 $timestamp$ 作为告警映射后节点 v 或 s 的时间标签,用于标识其发生时间.此外,当告警映射为空时,一方面可能是误告警;另一方面可能是因果知识网络的结构不够完整,即缺少相应的节点.针对这种情况要结合专家知识进一步分析,如果确认是误告警则直接去除并加入知识库便于以后的告警处理;如果确认是因果知识网络结构不够完整,则将其更新,这种利用专家知识解决告警异常的方法一定程度上能够识别新的攻击行为,是有效且必要的辅助手段.

通过告警映射,将告警转换为因果知识网络的节点,更利于因果知识的获取和攻击场景的构建.然而,由于大量的告警事件中反映的不止 1 个攻击场景,如果对告警事件不加处理而直接进行关联,必将导致构建的攻击场景混乱.为了解决此问题,首先对告警进行聚类,使得同一攻击场景的告警聚为 1 类,不同攻击场景的告警彼此分开,然后再进行因果知识的挖掘和攻击场景的构建.

针对海量的告警事件,告警聚类依据属于同一攻击场景的告警的性质将告警事件聚为若干类,一方面利于因果知识的挖掘和攻击场景的构建;另一方面有利于告警关联的并行处理,提高效率.针对此问题,梅海彬等人[20]通过定义告警相似度(考虑到时间、IP 相似性)进行聚类;冯学伟等人[21]则认为由同一攻击活动触发的因果告警事件,彼此在地址分布上总是具有关联性,故他通过地址相关性进行告警聚类.本文借助因果知识网络,设计了告警聚类的 3 个原则:

1)考虑到攻击行为的连贯性,规定了相邻攻击步骤或状态转移产生的告警间隔必须在一定的时间窗内;

2)考虑到因果知识网络中父节点早于子节点发生,规定告警间时序关系与其映射到因果知识网络中的节点之间逻辑因果关系一致;

3)考虑到攻击行为的关联性,规定告警映射后的节点符合图距离限制.

其中,原则 3 中因果知识网络中节点的图距离定义如图 2 所示.图 2 中 d 用于表示节点之间的图距离,如 $d(v_2,v_1)=2$ 表示节点 v_2 到节点 v_1 的图距离为 2.

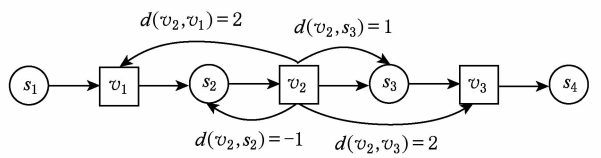

Fig. 2　Definition of distance between nodes in a causal knowledge network

图 2　因果知识网络上的节点之间距离的定义

具体地,告警聚类的 3 个原则形式化表示为:

1) $|timestamp(a_i)-timestamp(a_j)|<Win$;

2) $(timestamp(a_i)-timestamp(a_j))\times d(map(a_i),map(a_j))<0$;

3) $|d(map(a_i),map(a_j))|<L$.

其中,a_i 和 a_j 表示 2 个不同的告警,Win 为时间限制,L 为图距离限制,当它们同时满足这 3 个原则时,可将这 2 个告警聚为 1 类,据此,可将大量的告警事件聚为若干类.通过聚类将告警映射形成的节点集 $Node$ 转化为节点序列集,即 $Node\rightarrow\{Nodeseq^i\mid i=1,2,\cdots\}$,进而为因果知识挖掘和攻击场景构建作准备.

2.2　因果知识挖掘

在物理学中,很多确定性现象遵从演变原则:由时刻 t_0 系统或过程所处的状态,可以决定系统或过程在时刻 $t>t_0$ 所处的状态,而无需借助于以前系统所处状态的历史信息.这种性质称为 Markov 性或无后效性:

$$p(x_{i+1}|x_i,x_{i-1},\cdots,x_1)=p(x_{i+1}|x_i). \quad (2)$$

其中,p 表示概率;x_i 表示系统当前所处的状态,而 x_{i+1} 表示系统下一时刻所处的状态.

在攻击建模的研究中,Ammann 等人[22]首先提出攻击者不会为了获取已有权限而发动攻击的观点,得到相关学者的认可.由于攻击过程中攻击者获得的攻击资源为增量增长的,则依据 Ammann 等人[22]的观点,攻击者下一步的攻击行为只与当前拥有的攻击资源有关,而无需借助于攻击者以前的攻击行为.因此,本文将攻击者实施的多步攻击行为视为符合 Markov 链性质的离散随机过程,进而利用 Markov 链模型进行因果知识挖掘.结合本文的因果知识网络模型,利用节点之间的一步转移概率矩阵来表示 Markov 链模型,即因果知识.

定义 6. 因果知识 $K=\{\boldsymbol{K}_1,\boldsymbol{K}_2,\boldsymbol{K}_3,\boldsymbol{K}_4\}$.由于本文提出的因果知识网络由 2 种不同性质的节点组成,则共有 4 个不同的一步转移矩阵,分别用 $\boldsymbol{K}_1,\boldsymbol{K}_2,\boldsymbol{K}_3,\boldsymbol{K}_4$ 表示.设因果知识网络中的状态节点 s 的个数为 m 个,攻击行为节点 v 的个数为 n 个,则 $\boldsymbol{K}_1$ 为 $m\times n$ 的矩阵,其每一个元素表示从状态节点到攻击行为节点$(s\to v)$的一步转移概率;则 $\boldsymbol{K}_2$ 为 $n\times m$ 的矩阵,其每一个元素表示从攻击行为节点到状态节点$(v\to s)$的一步转移概率;则 $\boldsymbol{K}_3$ 为 $m\times m$ 的矩阵,其每一个元素表示从状态节点到状态节点$(s\to s)$的一步转移概率;则 $\boldsymbol{K}_4$ 为 $n\times n$ 的矩阵,其每一个元素表示从攻击行为节点到攻击行为节点$(v\to v)$的一步转移概率.$\boldsymbol{K}_1,\boldsymbol{K}_2,\boldsymbol{K}_3,\boldsymbol{K}_4$ 共同构成了因果知识网络的因果知识.

设由告警映射及聚类得到的节点序列集为 $\{Nodeseq^i|i=1,2,\cdots\}$,则基于 Markov 链模型的因果知识挖掘方法通过对 $\{Nodeseq^i|i=1,2,\cdots\}$ 中各个节点序列中的一步转移节点关系提取并计数,再依据 Markov 链所有转移概率之和为 1 的要求进行标准化,进而得到一步转移概率矩阵.以节点序列 $s_1\to s_2\to v_1\to s_3\to v_2\to v_3\to s_4\to v_4\to s_5$ 为例,则满足 $s\to v$ 一步转移节点关系的是 $s_2\to v_1$,$s_3\to v_2$,$s_3\to v_3$,$s_4\to v_4$;满足 $v\to s$ 一步转移节点关系的是 $v_1\to s_3$,$v_3\to s_4$,$v_4\to s_5$;满足 $s\to s$ 一步转移节点关系的是 $s_1\to s_2$,$s_2\to s_3$,$s_3\to s_4$,$s_4\to s_5$;满足 $v\to v$ 一步转移节点关系的是 $v_1\to v_2$,$v_2\to v_3$,$v_3\to v_4$.对 $\{Nodeseq^i|i=1,2,\cdots\}$ 中各个节点序列进行同样的节点关系提取并计数,进而根据所有转移概率之和为 1 的要求进行标准化,从而得到一步转移概率矩阵 $\boldsymbol{K}_1,\boldsymbol{K}_2,\boldsymbol{K}_3,\boldsymbol{K}_4$:

$$\boldsymbol{K}_1=\begin{bmatrix} p(s_1\to v_1) & \cdots & p(s_1\to v_n)\\ \vdots & & \vdots\\ p(s_m\to v_1) & \cdots & p(s_m\to v_n)\end{bmatrix},$$

$$\boldsymbol{K}_2=\begin{bmatrix} p(v_1\to s_1) & \cdots & p(v_1\to s_m)\\ \vdots & & \vdots\\ p(v_n\to s_1) & \cdots & p(v_n\to s_m)\end{bmatrix},$$

$$\boldsymbol{K}_3=\begin{bmatrix} p(s_1\to s_1) & \cdots & p(s_1\to s_m)\\ \vdots & & \vdots\\ p(s_m\to s_1) & \cdots & p(s_m\to s_m)\end{bmatrix},$$

$$\boldsymbol{K}_4=\begin{bmatrix} p(v_1\to v_1) & \cdots & p(v_1\to v_n)\\ \vdots & & \vdots\\ p(v_n\to v_1) & \cdots & p(v_n\to v_n)\end{bmatrix}.$$

满足:

$$\sum_{x=1}^{n}p(s_i\to v_x)=1,\sum_{y=1}^{m}p(v_i\to s_y)=1,$$

$$\sum_{y=1}^{m}p(s_i\to s_y)=1,\sum_{x=1}^{n}p(v_i\to v_x)=1.$$

又由因果知识网络结构得出 2 个修改原则:

1) 对于没有父节点的节点,其他所有节点到此节点的一步转移概率为 0;

2) 对于没有子节点的节点,此节点到其他所有节点的一步转移概率为 0.

根据以上 2 个修正原则,对 $\boldsymbol{K}_1,\boldsymbol{K}_2,\boldsymbol{K}_3,\boldsymbol{K}_4$ 中的相关节点概率进行置 0 操作,即得到初步的因果知识.

2.3 因果知识的显著性检验

因果知识是利用因果知识网络进行定量推理的依据,因此因果知识的合理度直接影响了攻击场景构建的准确度.为保证挖掘得到的因果知识准确合理,本文提出了基于成对数据 t 检验的方法对 2.2 节得到的初步的因果知识进行显著性检验,只有通过显著性检验的因果知识才能作为后续攻击场景构建的依据.

2.3.1 显著性检验理论依据

由因果知识网络的网络结构与贝叶斯推理规则知,满足 $s\to s$ 和 $v\to v$ 关系的一步转移概率可由满足 $s\to v$ 和 $v\to s$ 关系的一步转移概率计算得出.不妨设,由满足 $s\to v$ 和 $v\to s$ 关系的一步转移概率得出的满足 $s\to s$ 和 $v\to v$ 关系的一步转移概率矩阵为 $\boldsymbol{K}'_3$ 和 $\boldsymbol{K}'_4$,则对于 $\boldsymbol{K}'_3$ 中的每一个元素 $K'_{3_{ij}}$ 满足:

$$K'_{3_{ij}}=p(s_i\to s_j)=\sum_{x=1}^{n}p(s_i\to v_x)\times p(v_x\to s_j)=\sum_{x=1}^{n}K_{1_{ix}}\times K_{2_{xj}}, \quad (3)$$

即得出 $\boldsymbol{K}'_3=\boldsymbol{K}_1\times\boldsymbol{K}_2$.同理,由:

$$K'_{4_{ij}}=p(v_i\rightarrow v_j)=\sum_{y=1}^{m}p(v_i\rightarrow s_y)\times p(s_y\rightarrow v_j)=\sum_{y=1}^{m}K_{2_{iy}}\times K_{1_{yj}},\tag{4}$$

得出 $\boldsymbol{K}'_4=\boldsymbol{K}_2\times\boldsymbol{K}_1$.

$\boldsymbol{K}_3$ 和 $\boldsymbol{K}_4$ 是由告警挖掘得到的满足 $s\rightarrow v$ 和 $v\rightarrow s$ 关系的一步转移概率矩阵,而 $\boldsymbol{K}'_3$ 和 $\boldsymbol{K}'_4$ 是由 $\boldsymbol{K}_1$ 和 $\boldsymbol{K}_2$ 计算得来.由因果知识网络定义知,$\boldsymbol{K}_3$ 和 $\boldsymbol{K}'_3$、$\boldsymbol{K}_4$ 和 $\boldsymbol{K}'_4$ 的实际含义一致,深入分析得出:

定理 1. 假设由告警产生的节点序列集与因果知识网络中的节点序列完全匹配,则 $\boldsymbol{K}'_3=\boldsymbol{K}_3$ 且 $\boldsymbol{K}'_4=\boldsymbol{K}_4$.

证明. 由于告警产生的节点序列集与因果知识网络中的节点序列完全匹配,则由告警产生的各个节点序列必满足状态型节点与攻击行为节点相间排列,即状态型节点 s 的子节点必为攻击行为节点 v,而攻击行为节点 v 的子节点必为状态型节点 s.于是,对于 $\boldsymbol{K}_3$ 中的任何一个元素 $K_{3_{ij}}=p(s_i\rightarrow s_j)=\frac{1}{\lambda}$($\lambda$ 为状态型节点 s_i 的出度),不妨假设,状态型节点 s_i 和 s_j 中间的攻击行为节点为 v_x,显然 $K_{1_{ix}}=p(s_i\rightarrow v_x)=\frac{1}{\gamma}$($\gamma$ 为状态型节点 s_i 的出度),且 $\lambda=\gamma$ 均为状态型节点 s_i 的出度.又由因果知识网络结构知,任意攻击行为节点的出度均为 1,故 $K_{2_{xj}}=p(v_x\rightarrow s_j)=1$.于是:$K_{3_{ij}}=p(s_i\rightarrow s_j)=\frac{1}{\lambda}=\frac{1}{\gamma}=\frac{1}{\gamma}\times1=K_{1_{ix}}\times K_{2_{xj}}=K'_{3_{ij}}$,即得出 $\boldsymbol{K}'_3=\boldsymbol{K}_3$ 同理可证 $\boldsymbol{K}'_4=\boldsymbol{K}_4$. 证毕.

如图 3 所示因果知识网络,则与其节点序列完全匹配的告警产生的节点序列集为 $s_1\rightarrow v_1\rightarrow s_2\rightarrow v_2\rightarrow s_3\rightarrow v_3\rightarrow s_4$ 和 $s_1\rightarrow v_4\rightarrow s_4$.

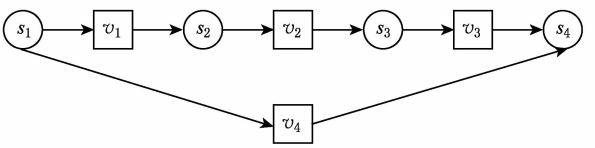

Fig. 3　An example of causal knowledge network

图 3　因果知识网络 1

则由告警产生的节点序列集挖掘计算得到的因果知识转移矩阵为

$$\boldsymbol{K}_1=\begin{pmatrix}\frac{1}{2}&0&0&\frac{1}{2}\\0&1&0&0\\0&0&1&0\\0&0&0&0\\0&0&1&0\end{pmatrix},$$

$$\boldsymbol{K}_2=\begin{pmatrix}0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix},$$

$$\boldsymbol{K}_3=\begin{pmatrix}0&\frac{1}{2}&0&0&\frac{1}{2}\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&0\\0&0&0&1&0\end{pmatrix},$$

$$\boldsymbol{K}_4=\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&0\\0&0&1&0\end{pmatrix},$$

则:

$$\boldsymbol{K}'_3=\boldsymbol{K}_1\times\boldsymbol{K}_2=\begin{pmatrix}0&\frac{1}{2}&0&0&\frac{1}{2}\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&0\\0&0&0&1&0\end{pmatrix}=\boldsymbol{K}_3,$$

$$\boldsymbol{K}'_4=\boldsymbol{K}_2\times\boldsymbol{K}_1=\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&0\\0&0&1&0\end{pmatrix}=\boldsymbol{K}_4.$$

由此定理知,通过对 $\boldsymbol{K}'_3$ 和 $\boldsymbol{K}_3$、$\boldsymbol{K}'_4$ 和 $\boldsymbol{K}_4$ 分别进行显著性检验,能够推断由告警挖掘的因果知识的准确度.

2.3.2　显著性检验具体方法

显著性检验方法以检验 $\boldsymbol{K}'_3$ 和 $\boldsymbol{K}_3$ 为例,检验 $\boldsymbol{K}'_4$ 和 $\boldsymbol{K}_4$ 的方法类推,且当且仅当 $\boldsymbol{K}'_3$ 和 $\boldsymbol{K}_3$、$\boldsymbol{K}'_4$ 和 $\boldsymbol{K}_4$ 均通过了显著性检验,才能将因果知识作为后续攻击场景构建的依据.

对于 $\boldsymbol{K}'_3$ 和 $\boldsymbol{K}_3$,它们可看作是在相同条件下由 2 种不同方法得到的因果知识,而基于成对数据的 t 检验方法能够有效检验 2 种不同方法产生结果是否存在显著性差异,故本文采用此检验方法来推断 $\boldsymbol{K}'_3$ 和 $\boldsymbol{K}_3$ 之间是否存在显著性差异,若检验结果显示 $\boldsymbol{K}'_3$ 和 $\boldsymbol{K}_3$ 存在显著性差异,则需要通过扩大告警数据集等方法重新挖掘因果知识,若不存在显著性差异,则其可作为最终的因果知识,并依此进行基于因果知识网络的攻击场景推理与预测.

设 $\boldsymbol{K}_3$ 为 $m\times m$ 的矩阵,则其可表示为 $\boldsymbol{K}_3=(K_{3_1},K_{3_2},\cdots,K_{3_m})^{\mathrm{T}}$,其中 $K_{3_i}=(K_{3_{i1}},K_{3_{i2}},\cdots,$

$K_{3_{im}})\ i=1,2,\cdots,m$，同样 $\boldsymbol{K}'_3=(K'_{3_1},K'_{3_2},\cdots,K'_{3_m})^{\mathrm{T}}$，其中 $K'_{3_i}=(K'_{3_{i1}},K'_{3_{i2}},\cdots,K'_{3_{im}}),\ i=1,2,\cdots,m$. 由 Markov 链模型知，行向量 K_{3_i}（或 K'_{3_i}）中的各个元素之和为 1，即各个元素之间不是相互独立关系，故（$K_{3_{ij}},K'_{3_{ij}}$）不能作为成对的观察数据进行检验. 然而，行向量 K_{3_i} 和 K'_{3_i} 均表示状态型节点 s_i 到其他状态型节点的一步转移概率，唯一不同的是计算方法，因此（K_{3_i},K'_{3_i}）可看作同一结果 2 个相互独立的观察值，能够作为成对的观察数据进行检验.

具体的显著性检验过程如下：

1）构造成对观察值差. 记为 $D_i=K_{3_{ij}}-K'_{3_{ij}}$，其中 $j=\underset{j=1,2,\cdots,m}{\arg\max}|K_{3_{ij}}-K'_{3_{ij}}|$.

2）作出样本检验假设. 由于 $D_1,D_2,\cdots,D_m$ 相互独立，且 $D_1,D_2,\cdots,D_m$ 是由同一因素引起的，可认为它们服从同一分布. 今假设 $D_i\sim N(\mu_D,\sigma_D^2),\ i=1,2,\cdots,m$，即 $D_1,D_2,\cdots,D_m$ 构成期望为 μ_D、方差为 σ_D^2 的正态分布总体 $N(\mu_D,\sigma_D^2)$的一个样本，其中 μ_D,σ_D^2 未知，则基于这一样本检验假设：

$$H_0:\mu_D=0,$$

$$H_1:\mu_D\neq 0.$$

3）构造拒绝域. 分别记 $D_1,D_2,\cdots,D_m$ 的样本均值和样本方差的观察值为 $\bar{\mu},s_D^2$，则此检验问题的拒绝域为（显著性水平为 α）：

$$|t|=\left|\frac{\bar{\mu}}{s_D/\sqrt{m}}\right|\geqslant t_{\alpha/2}(m-1),\tag{5}$$

其中，$|t|$ 为检验统计量；m 为数据对的个数，即为矩阵 $\boldsymbol{K}_3$ 和 $\boldsymbol{K}'_3$ 的维数，当维数较大时，可采用随机抽样的方法获取矩阵 $\boldsymbol{K}_3$ 和 $\boldsymbol{K}'_3$ 中的若干行作为检验样本，使得 m 的取值保持在一个合适的范围内，以提高检验的效率.

4）检验结果的判定. 若由 $D_1,D_2,\cdots,D_m$ 样本均值和方差计算得到的 $|t|$ 的值不落在拒绝域内，则接受 H_0，认为 $\boldsymbol{K}'_3$ 和 $\boldsymbol{K}_3$ 无显著性差异，即挖掘的因果知识准确；若 $|t|$ 的值落在拒绝域内，则接受 H_1，认为 $\boldsymbol{K}'_3$ 和 $\boldsymbol{K}_3$ 存在显著性差异，即挖掘的因果知识不准确，需要进一步挖掘或调整.

2.4 攻击场景构建

攻击场景的构建是通过关联多个攻击步骤所引发的告警来重现攻击过程. 设时间窗 T 内获取的告警集为 $Attack^T$，则攻击场景的构建可形式化描述为：已知因果知识网络 G_k，时间窗 T 内告警集为 $Attack^T$，求攻击者最有可能的攻击场景 $Attack^T=\{Attackseq_i^T=s_i^1\rightarrow v_i^1\rightarrow s_i^2\rightarrow v_i^2\cdots|i=1,2,\cdots\}$.

本文提出的基于因果知识网络的攻击场景构建方法，依据因果知识网络，将实时的攻击场景构建分为初建和重构 2 步.

2.4.1 攻击场景初建

攻击场景初建的形式化过程为：$Alarm^T\rightarrow Node^T\rightarrow\{Nodeseq_i^T|i=1,2,\cdots\}$.

利用 2.1 节的告警映射方法，将时间窗 T 内获取的告警集 $Alarm^T$ 映射为因果知识网络中的节点集合 $Node_T$，并利用告警聚类将不同攻击场景的节点集合聚为不同类 $Nodeseq_i^T$，即 $Node^T\rightarrow\{Nodeseq_i^T|i=1,2,\cdots\}$，其中 $Nodeseq_i^T$ 表示由告警聚类形成的第 i 个节点序列. 若把因果知识网络视为攻击序列的集合，则理论上讲，$Nodeseq_i^T\in G$，然而由于 IDS 的漏报或误报情况，可能导致 $Nodeseq_i^T$ 与因果知识网络中的攻击序列并不一致，即 $Nodeseq_i^T\notin G$，故 $Nodeseq_i^T$ 不能看作为一个攻击过程，需要对其进行重构以得到完整的攻击场景.

2.4.2 攻击场景重构

攻击场景重构的形式化过程为：$\{Nodeseq_i^T|i=1,2,\cdots\}\rightarrow\{Attackseq_i^T=s_i^1\rightarrow v_i^1\rightarrow s_i^2\rightarrow v_i^2\cdots|i=1,2,\cdots\}=Attack^T$.

由于 IDS 的漏报或误报情况，导致初建得到的攻击场景往往是断裂或错误的，为了得到更加完整可信的攻击场景，需要对初建生成的攻击场景进行重构，进而得到完整的攻击场景. 本文以节点序列 $Nodeseq_i^T$ 为例，借助因果知识网络，具体给出 $Nodeseq_i^T\rightarrow Attackseq_i^T$ 的推理重构过程，其他节点序列的重构过程类同.

攻击场景构建的关键是结合因果知识网络由节点序列推理出最有可能的攻击序列. 贝叶斯推理中的最大后验估计方法，能够在给定知识时寻找可能性最大的假设，适用于解决此问题. 在本文的攻击场景重构问题中，节点序列 $Nodeseq_i^T$ 可看作是给定数据 Q；因果知识网络中的若干攻击序列集可看作候选假设集合 H；则所求的 $Attackseq_i^T$ 为最大可能假设 h_{MAP}. 于是基于最大后验估计原理的攻击场景重构问题可分 4 个步骤解决：

Step1. 依据因果知识网络，依据节点序列 $Nodeseq_i^T$ 识别所有可能的备选攻击序列集 H；

Step2. 结合因果知识网络和贝叶斯推理方法，赋予每一下备选攻击序列的先验概率 $P(h)$；

Step3. 模拟每一个备选的攻击序列，利用概率推理得出此种攻击序列出现节点序列 $Nodeseq_i^T$ 的概率 $P(Nodeseq_i^T|h)$；

Step4. 取出最大的 $P(Nodeseq_i^T|h)\times P(h)$的那

个攻击序列 h 作为最有可能的攻击序列 $Attackseq_i^T$.

特别地,步骤 2 和步骤 3 中的攻击序列的先验概率以及攻击序列与节点序列的似然度计算方法如下:

1) 攻击序列的先验概率计算方法

攻击序列由因果知识网络中的状态型节点 s 和攻击行为节点 v 交错排列而成,即 $Attackseq_i=s_i^1\rightarrow v_i^1\rightarrow s_i^2\rightarrow v_i^2\rightarrow\cdots$,则攻击序列的先验概率 $P(Attackseq_i)$ 指此攻击序列所展示的攻击行为发生的可能性,由于攻击序列中节点之间是因果串联关系,固可用攻击序列中所有相邻的一步转移概率的乘积表示:

$$P(Attackseq_i)=p(s_i^1\rightarrow v_i^1)\times p(v_i^1\rightarrow s_i^2)\times p(s_i^2\rightarrow v_i^2)\times p(v_i^2\rightarrow s_i^3)\times\cdots, \tag{6}$$

其中一步转移概率由 2.2 节和 2.3 节挖掘得到的因果知识 K 提供.

2) 攻击序列与节点序列间的似然度计算方法

攻击序列与节点序列间的似然度本质是指特定攻击场景下产生此告警的可能性,借助本文的因果知识网络,攻击场景可用因果知识网络中的攻击序列表示,而告警则可转化为节点序列,于是两者间的似然度可用序列间差异来表示. 为了进一步量化似然度,本文引出序列长度和序列间距 2 个定义.

定义 7. 序列长度 L. 用于表征因果知识网络中的攻击序列的长度,用攻击序列中节点的总数量度量. 如图 4 所示的因果知识网络中,攻击序列 $s_1\rightarrow v_2\rightarrow s_3\rightarrow v_6\rightarrow s_6\rightarrow v_{10}\rightarrow s_9$ 的序列长度 $L=7$.

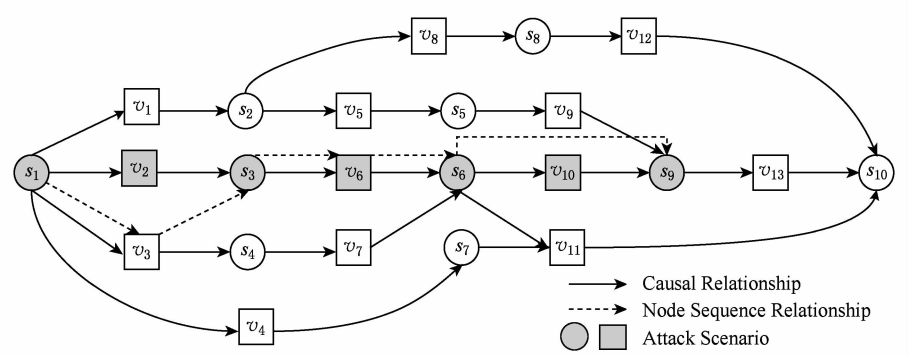

Fig. 4　Another example of causal knowledge network

图 4　因果知识网络示例 2

定义 8. 序列间距 D. 用于表征节点序列与攻击序列之间的差异,用 2 序列间的差异节点与攻击序列之间的距离和表示. 其中,每个差异节点与攻击序列之间的距离等同于此差异节点到攻击序列中所有节点距离的绝对值的最小值,即转化为节点之间的距离,计算方法如 2.1 节中图 2 所示. 如图 4 所示的因果知识网络中,若节点序列 $Nodeseq_i^T$ 为 $s_1\rightarrow v_3\rightarrow s_3\rightarrow v_6\rightarrow s_6\rightarrow s_9$,攻击序列 $Attackseq_i^T$ 为 $s_1\rightarrow v_2\rightarrow s_3\rightarrow v_6\rightarrow s_6\rightarrow v_{10}\rightarrow s_9$,则这 2 个序列间的差异节点为 v_2,v_3,v_{10},序列间距 $D=d(a_2,attack_i^T)+d(v_3,attack_i^T)+d(v_{10},attack_i^T)=|d(v_2,s_1)|+|d(v_3,s_1)|+|d(v_{10},s_6)|=|d(v_2,s_3)|+|d(v_3,s_3)|+|d(v_{10},s_9)|=1+1+1=3$.

不妨设 $P(Nodeseq\mid Attackseq)$ 为攻击序列 $Attackseq$ 与节点序列 $Nodeseq$ 的似然,则得出以下定理.

定理 2. 假设 $P(Nodeseq\mid Attackseq)$ 与 $D(Nodeseq,Attackseq)$ 成反比,即攻击序列与节点序列间距越大,二者似然度越小,反之越大. 则能够得出:

$$P(Nodeseq\mid Attackseq)=\frac{L(Attackseq)-D(Nodeseq,Attackseq)}{L(Attackseq)}. \tag{7}$$

证明. 由网络攻击实际知,当 $Nodeseq=\varnothing$ 时,实际意义为当发生多步攻击活动 $Attackseq$ 时,获取的告警集为空,由目前的网络安全设备效率来讲,这种情况的可能性很小,即 $P(\varnothing\mid Attackseq)=0$;当 $Nodeseq=Attackseq$ 时,实际意义为当发生多步攻击活动 $Attackseq$ 时,获取了每一步攻击活动的告警,发生这种情况的可能性很大,即 $P(Nodeseq\mid Attackseq)=1$. 由此可知,当 $Nodeseq=\varnothing$ 时,$D(Nodeseq,Attackseq)=L(Attackseq)$,$P(\varnothing\mid Attackseq)=0$;当 $Nodeseq=Attackseq$,$D(Nodeseq,Attackseq)=0$,$P(Attackseq\mid Attackseq)=1$. 又由于 $P(Nodeseq\mid Attackseq)$ 与 $D(Nodeseq,Attackseq)$ 成反比,由 2 点式直线方程可知:

$$\frac{P(Nodeseq\mid Attackseq)-1}{D(Nodeseq,Attackseq)}=\frac{P(Nodeseq\mid Attackseq)-0}{D(Nodeseq,Attackseq)-L(Attackseq)}, \tag{8}$$

化简得:

$$P(Nodeseq|Attackseq)=\frac{L(Attackseq)-D(Nodeseq,Attackseq)}{L(Attackseq)}. \quad (9)$$

证毕.

$P(Nodeseq|Attackseq)$ 与 $D(Nodeseq,Attackseq)$ 的关系如图 5 所示:

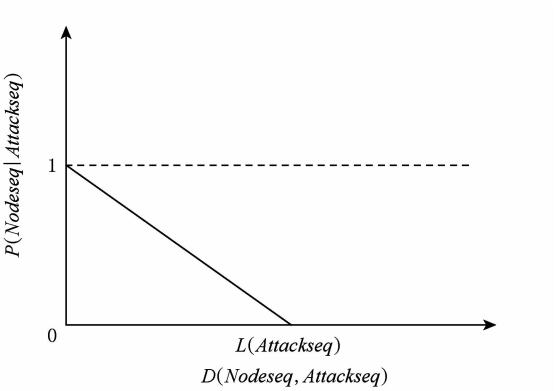

Fig. 5 The relationship between $P(Nodeseq|Attackseq)$ and $D(Nodeseq,Attackseq)$

图 5 $P(Nodeseq|Attackseq)$ 与 $D(Nodeseq,Attackseq)$ 的关系

由定理 2,依据候选攻击序列与节点序列的序列间距以及攻击序列的长度即可计算出攻击序列与节点序列的似然度.

3 实验与分析

3.1 基于公开数据集的实验分析

目前,能够用于攻击场景构建的公开数据集较少.1998 年美国国防部为了加强网络安全技术,实施了 DARPA 项目,此项目生成的数据集成为目前公认的可用于攻击场景构建的数据集. DARPA 实施了 2 个攻击过程:LLDOS1.0 和 LLDOS2.0.由于 LLDOS1.0 和 LLDOS2.0 这 2 个攻击场景的攻击目标一致,都是对目标主机 131.84.1.31 实施 DDOS 攻击,且它们的攻击过程基本相似,均是利用 Sadmind 漏洞实施的 DDOS 攻击过程.而区别在于 LLDOS2.0 比 LLDOS1.0 更难被检测,其中的一些攻击过程与正常的网络行为相似,检测系统并没有产生相应的告警,相当于"漏报"的情况.而由于官方公布的数据集中没有明确指出目标网络的漏洞知识,鉴于此,依据大量学者[23-24]的研究,再加上对 LLDOS1.0 攻击过程中产生告警的分析,构建此网络的因果知识网络,在此基础上利用因果知识网络对 LLDOS2.0 的攻击场景进行构建.深入分析知,网络中的漏洞信息、攻击方法和告警类型对应关系如表 1 所示.构建的 LLDOS 因果关系网络如图 6 所示.

Table 1 Corresponding Relation of Vulnerability Information, Attack Method and Alarm Type in the Network

表 1 网络中的漏洞信息、攻击方法和告警类型的对应关系

Vulnerability Information	Attack Method	Alarm Type
ICMP Incorrectly Configured	IPSweep	ICMP PING
SunRPC Incorrectly Configured	Sadmind Ping	RPC Sadmind UDP PING
Sadmind Buffer Overflow	Sadmind Exploit	RPC Sadmind UDP Overflow Attempt
RCP Incorrectly Configured	Daemon Installed	RSEVICES Rsh Root
SYN Flood	DDOS	BADTRAFFIC Loopback Traffic
HINFO Query Incorrectly Configured	DNS Query	NULL

由于 LLDOS 每一步利用的原子攻击均比较简单,其前提条件和后果均可由所利用的攻击手段得出,例如 IPSweep 攻击的前提条件为源主机能够访问目标主机,且目标主机存在 ICMP Incorrectly Configured 漏洞,攻击的后果则为探测到目标主机的信息;Sadmind Exploit 攻击的前提条件为具有目标主机的普通权限,且目标主机存在 Sadmind Buffer Overflow 漏洞,攻击的后果则为获得目标主机的 ROOT 权限.因此,为了便于描述,不再具体给出每一个原子攻击的前提后果条件.具体地,因果关系网络中原子攻击行为节点对应的攻击手段如表 2 所示;因果关系网络中状态节点对应的 IP 地址如表 3

Table 2 The Attack Means Corresponding Atomic Attack Behavior Node

表 2 原子攻击行为节点对应的攻击手段

Atomic Attack Behavior Node	Attack Means
v_3	IPSweep
$v_2, v_4, v_6, v_8, v_{18}, v_{20}, v_{22}, v_{24}, v_{26}, v_{28}$	Sadmind Ping
$v_9, v_{12}, v_{15}, v_{19}, v_{21}, v_{23}, v_{25}, v_{27}, v_{29}$	Sadmind Exploit
v_{10}, v_{13}, v_{16}	Daemon Installed
v_{11}, v_{14}, v_{17}	DDOS
v_1, v_5, v_7	DNS Query

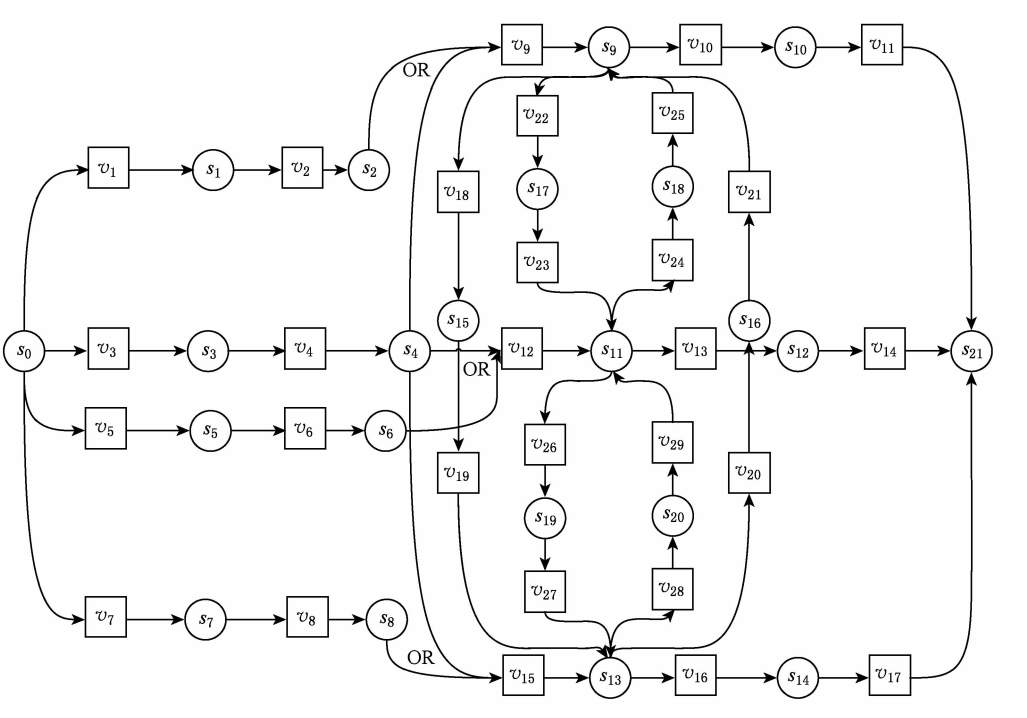

Fig. 6　Causal relationship network of LLDOS

图 6　LLDOS 因果关系网络

Table 3　The IP Address Corresponding to the Status Node

表 3　状态节点对应的 IP 地址

Status Node	IP Address
s_0	202.77.162.213
s_1,s_2,s_9,s_{10},s_{16},s_{18},	172.16.112.10
s_5,s_6,s_{11},s_{12},s_{17},s_{20},	172.16.115.20
s_7,s_8,s_{13},s_{14},s_{15},s_{19}	172.16.112.50
s_{21}	131.84.1.31
s_3	(172.16.112/,172.16.113/,172.16.114/)
s_4	(172.16.112.10,172.16.115.20,172.16.112.50)

所示. LLDOS1.0 的攻击场景如图 7 所示,深色节点表现了整个攻击过程.

通过分析 LLDOS2.0 中告警,推理的 LLDOS2.0 的攻击场景如图 8 所示. 图 8 中黑色实心小圆表示此节点检测到了告警,由于 LLDOS2.0 的攻击手段比 LLDOS1.0 隐蔽,使得攻击过程中存在告警漏报现象. 结合因果关系网络,可知对应 v_5,s_5,v_{16},s_{14} 的告警出现漏报,整个攻击过程如图 8 中深色节点所展现. 攻击者先采用正常的 DNS Query,查询到 DNS 服务器 172.16.115.20,并利用该主机中 Sadmind 漏洞获得 ROOT 权限,再以该主机为跳板控制主机 172.16.112.50,最后通过 172.16.115.20 和 172.16.112.50 对目标主机实施 DDOS 攻击.

由上述实验可知,尽管官方公布的数据中不含历史告警库,无法从中挖掘出因果知识,但是依据本文方法构建出因果关系网络,并在此基础上利用定性的告警映射关联,能够构建出 LLDOS2.0 的攻击场景.

3.2　真实网络环境中的实验分析

为了进一步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 9 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 Email 服务器. 子网 1 由 3 台主机构成. 子网 2 由 1 台工作站和 1 台文件服务器组成. 子网 3 包括 1 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

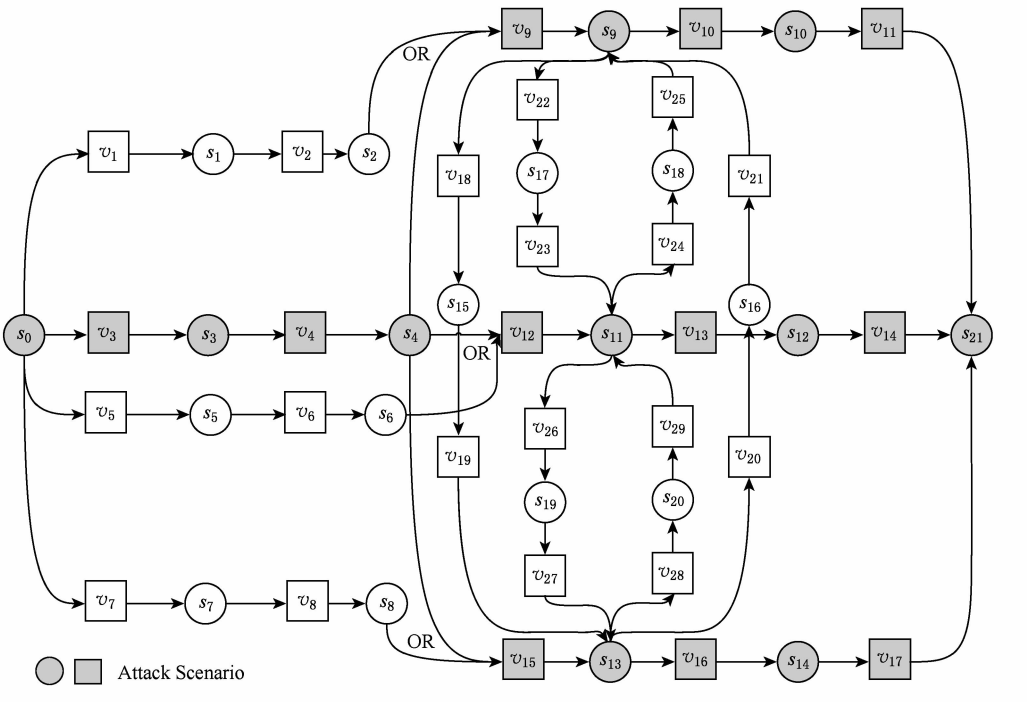

Fig. 7 Attack Scenario of LLDOS1.0

图 7 LLDOS1.0 的攻击场景

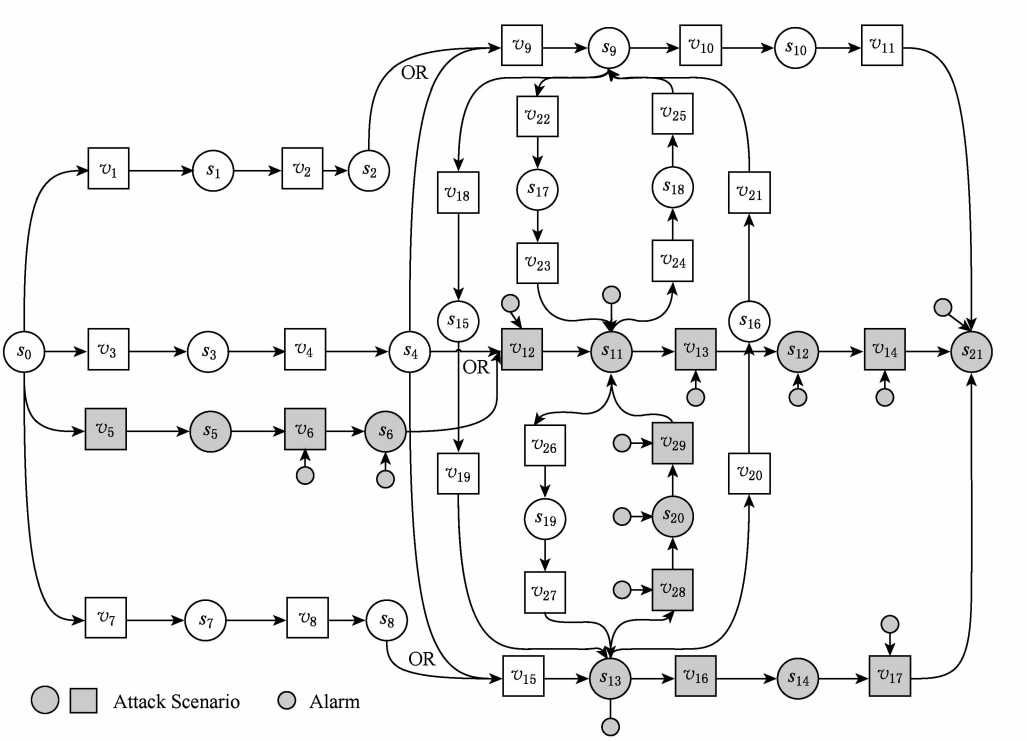

Fig. 8 Attack Scenario of LLDOS2.0

图 8 LLDOS2.0 的攻击场景

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 和子网 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 4 所示.依据漏洞信息和 CVSS 分析得出的攻击行为信息如表 5 所示.

根据图 9 和表 5,确定因果知识网络基本结构如图 10 所示,从初始状态 s_1 到目标状态 s_9 共有 6 条不同的攻击路径,分别是 $path1: s_1 \rightarrow v_1 \rightarrow s_2 \rightarrow v_5 \rightarrow s_8 \rightarrow v_{13} \rightarrow s_9$; $path2: s_1 \rightarrow v_1 \rightarrow s_2 \rightarrow v_3 \rightarrow s_4 \rightarrow v_6 \rightarrow s_6 \rightarrow v_{11} \rightarrow s_8 \rightarrow v_{13} \rightarrow s_9$; $path3: s_1 \rightarrow v_1 \rightarrow s_2 \rightarrow v_4 \rightarrow s_5 \rightarrow v_7 \rightarrow s_6 \rightarrow v_{11} \rightarrow s_8 \rightarrow v_{13} \rightarrow s_9$; $path4: s_1 \rightarrow v_1 \rightarrow s_2 \rightarrow v_4 \rightarrow s_5 \rightarrow v_8 \rightarrow s_7 \rightarrow v_{12} \rightarrow s_8 \rightarrow v_{13} \rightarrow s_9$; $path5: s_1 \rightarrow v_1 \rightarrow s_2 \rightarrow v_4 \rightarrow s_5 \rightarrow v_{10} \rightarrow s_8 \rightarrow v_{13} \rightarrow s_9$; $path6: s_1 \rightarrow v_2 \rightarrow s_3 \rightarrow v_1 \rightarrow s_2 \rightarrow v_4 \rightarrow s_5 \rightarrow v_9 \rightarrow s_9$.

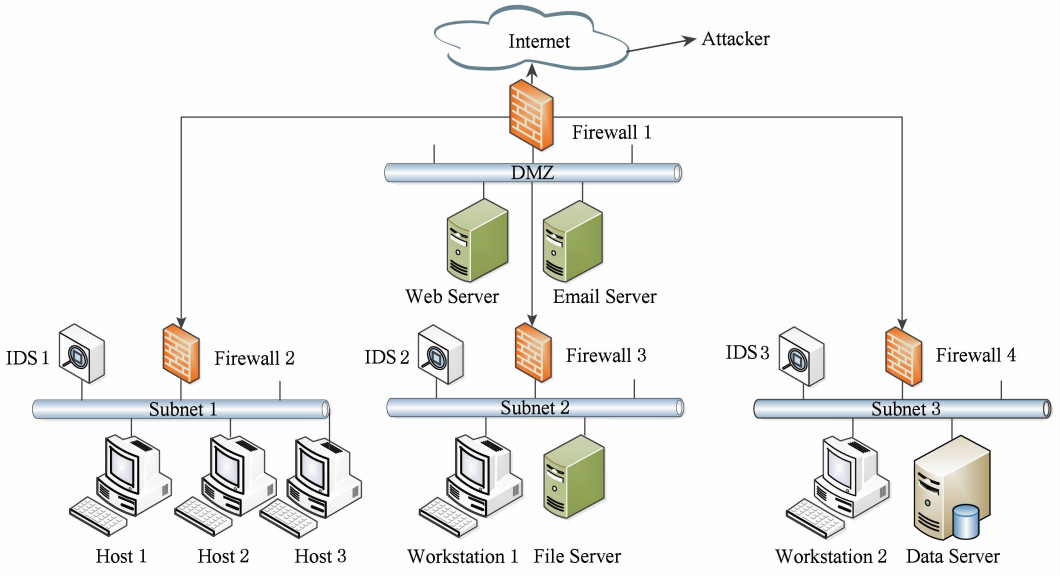

Fig. 9　Experimental network topology

图 9　实验网络拓扑图

Table 4　The Information of Hosts and Vulnerabilities

表 4　各主机信息及其所含漏洞信息

Host Name Number	Host Information	Vulnerabilities Number	CVE Number	Vulnerabilities Describe	Attack Number
$H1$	Web server,apache	$V1$	CVE-2013-2249	Unspecified Remote Security Vulnerability	v_1
$H2$	Host 1,Microsoft Windows XP SP2	$V2$	CVE-2013-3940	Graph Device Interface Integer Overflow	v_6,v_7
		$V3$	CVE-2013-5065	Local System Exploit	v_{11}
		$V4$	CVE-2012-0002	Microsoft Remote Code Execution	v_{12}
		$V5$	CVE-2013-1727	Mozilla Firefox Bypass Exploit	v_5
		$V6$	CVE-2007-6473	Heap-based Buffer Overflow	v_{10}
$H3$	Host 2,Microsoft Windows 7 SP2	$V7$	CVE-2011-0638	USB Warning Weakness Program Execution	v_2
$H4$	Host 3,Red Hat	$V8$ $V9$	CVE-2014-6271 CVE-2012-6137	GNU Bash Remote Code Execution SSL Certificate Validation Security Bypass	v_{13} v_9
$H5$	File server, Windows2000,HFS	$V10$	CVE-2014-6287	HFS Code Inject	v_3
$H6$	Workstation 2, Windows2000,Funk Proxy v3.0	$V11$	CVE-2002-0065	Funk Proxy Weak Password Store	v_8
$H7$	Data server,Windows server 2003	$V12$	CVE-2004-0119	Remote Buffer Overflow	v_4

Table 5 The Information of Attack Behaviors

表 5 攻击行为信息

Attack Number	Prerequisite and Number	Consequent and Number	Vulnerability Exploited
v_1	Access to Internet→s_1	($H1$,ROOT)→s_2	CVE-2013-2249
v_2	Access to Internet→s_1	($H3$,ROOT)→s_3	CVE-2011-0638
v_3	($H1$,ROOT)→s_2	($H5$,ROOT)→s_4	CVE-2014-6287
v_4	($H1$,ROOT)→s_2	($H7$,ROOT)→s_5	CVE-2004-0119
v_5	($H1$,ROOT)→s_2	($H2$,ROOT)→s_8	CVE-2013-1727
v_6	($H5$,ROOT)→s_4	($H2$,USER)→s_6	CVE-2013-3940
v_7	($H7$,ROOT)→s_5	($H2$,USER)→s_6	CVE-2013-3940
v_8	($H7$,ROOT)→s_5	($H6$,ROOT)→s_7	CVE-2002-0065
v_9	($H1$,ROOT)→s_2;($H3$,ROOT)→s_3	($H4$,ROOT)→s_9	CVE-2012-6137
v_{10}	($H7$,ROOT)→s_5	($H2$,ROOT)→s_8	CVE-2007-6473
v_{11}	($H2$,USER)→s_6	($H2$,ROOT)→s_8	CVE-2013-5065
v_{12}	($H6$,ROOT)→s_7	($H2$,ROOT)→s_8	CVE-2012-0002
v_{13}	($H2$,ROOT)→s_8	($H4$,ROOT)→s_9	CVE-2014-6271

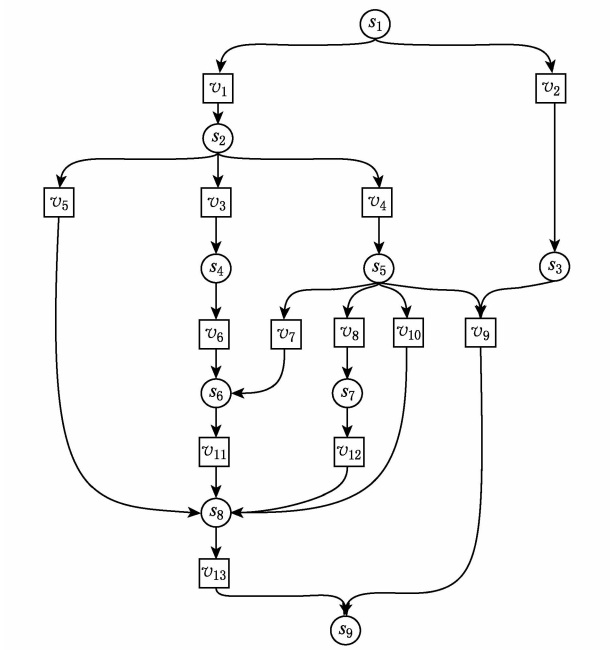

Fig. 10 The causal knowledge network structure of experiment

图 10 实验得出的因果知识网络结构

依据此网络产生的告警集,利用本文提出的因果知识挖掘方法得到的通过显著性检验(取显著性水平 $\alpha=0.05$)的因果知识为 $\boldsymbol{K}=\{\boldsymbol{K}_1,\boldsymbol{K}_2,\boldsymbol{K}_3,\boldsymbol{K}_4\}$,具体地:

$$\boldsymbol{K}_1=\begin{pmatrix}0.845 & 0.155 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0.284 & 0.572 & 0.144 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1.0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0.238 & 0.301 & 0.286 & 0.175 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\end{pmatrix},$$

$$\boldsymbol{K}_2=\begin{pmatrix}0&1&0&0&0&0&0&0&0\\0&0&1&0&0&0&0&0&0\\0&0&0&1&0&0&0&0&0\\0&0&0&0&1&0&0&0&0\\0&0&0&0&0&0&0&1&0\\0&0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0&0\\0&0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0&1\end{pmatrix},$$

$$\boldsymbol{K}_3=\begin{pmatrix}0&0.713&0.106&0.054&0&0.078&0.043&0&0.006\\0&0&0.056&0.207&0.484&0&0.057&0.129&0.067\\0&0.003&0.024&0&0.012&0&0&0.007&0.954\\0&0&0.005&0&0.004&0.973&0.007&0&0.011\\0&0.004&0.044&0.014&0&0.217&0.309&0.163&0.249\\0&0&0&0&0&0.051&0&0.921&0.028\\0&0&0&0.014&0&0.027&0&0.946&0.013\\0&0&0&0&0.006&0&0.017&0&0.977\\0&0&0&0&0&0&0&0&0\end{pmatrix},$$

$$\boldsymbol{K}_4=\begin{pmatrix}0&0&0.193&0.547&0.131&0&0.051&0.043&0.006&0.001&0.025&0&0.003\\0&0&0&0.011&0.004&0.008&0&0.004&0.941&0.008&0.008&0.016&0\\0&0&0&0&0&0.964&0.006&0.003&0.009&0.009&0&0&0.009\\0&0&0.004&0&0&0.009&0.211&0.314&0.194&0.143&0.112&0.019&0.003\\0&0&0&0&0&0&0&0.006&0&0&0&0.006&0.988\\0&0&0&0&0.012&0&0.013&0.021&0&0&0.935&0.019&0\\0&0&0&0&0.064&0.005&0&0.063&0&0&0.868&0&0\\0&0&0&0&0&0&0&0.005&0.042&0.007&0.007&0.877&0.062\\0&0&0&0&0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0.029&0.002&0.012&0.016&0.008&0.933\\0&0&0&0&0&0&0&0&0&0&0&0.040&0.960\\0&0&0&0&0&0&0&0&0&0.015&0&0.003&0.982\\0&0&0&0&0&0&0&0&0&0&0&0&0\end{pmatrix}.$$

实验模拟了 3 个不同的攻击场景,用于验证告警冗余及缺失时攻击场景构建的准确性.具体实验结果如表 6 所示.

实验 1 对于告警缺失的情况进行了模拟,模拟的攻击序列为 $s_1\rightarrow v_1\rightarrow s_2\rightarrow v_3\rightarrow s_4\rightarrow v_6\rightarrow s_6\rightarrow v_{11}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$,而由告警映射形成的节点序列为 $s_1\rightarrow v_1\rightarrow v_3\rightarrow s_4\rightarrow v_6\rightarrow v_{11}\rightarrow v_{13}\rightarrow s_9$,即缺失了状态节点 s_2,s_6,s_8.结合因果知识网络选取了 2 个候选的攻击序列:$s_1\rightarrow v_1\rightarrow s_2\rightarrow v_3\rightarrow s_4\rightarrow v_6\rightarrow s_6\rightarrow v_{11}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$ 和 $s_1\rightarrow v_1\rightarrow s_2\rightarrow v_4\rightarrow s_5\rightarrow v_7\rightarrow s_6\rightarrow v_{11}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$.依据本文提出的基于最大后验假设估计的攻击场景定量重构方法,计算得出前者的概率为 $0.845\times 0.572\times(11-3)/11=0.351\,52$,后者的概率为 $0.845\times0.144\times0.238\times(11-5)/11=0.015\,796$,取二者概率最大的攻击序列,即可得出重构后的攻击序列为 $s_1\rightarrow v_1\rightarrow s_2\rightarrow v_3\rightarrow s_4\rightarrow v_6\rightarrow s_6\rightarrow v_{11}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$,与模拟的攻击序列一致,故攻击场景构建成功.实验 2 模拟了告警冗余的情况,模拟的攻击序列

为 $s_1\rightarrow v_1\rightarrow s_2\rightarrow v_5\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$，而由告警映射形成的节点序列为 $s_1\rightarrow v_2\rightarrow s_2\rightarrow v_5\rightarrow v_3\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$，即 v_3 为冗余的告警. 结合因果知识网络选取了 2 个候选的攻击序列：$s_5\rightarrow v_8\rightarrow s_7\rightarrow v_{12}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$ 和 $s_1\rightarrow v_1\rightarrow s_2\rightarrow v_3\rightarrow s_4\rightarrow v_6\rightarrow s_6\rightarrow v_{11}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$. 同样方法计算得出前者的概率为 0.845×0.284×(7−1)/7=0.2057，后者的概率为 0.845×0.572×(11−7)/11=0.17576，取二者概率最大的攻击序列，即可得出重构后的攻击序列为 $s_5\rightarrow v_8\rightarrow s_7\rightarrow v_{12}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$，与模拟的攻击序列一致，故攻击场景构建成功. 实验 3 模拟了告警冗余和告警缺失这种混合情况，模拟的攻击序列为 $s_1\rightarrow v_1\rightarrow s_2\rightarrow v_4\rightarrow s_5\rightarrow v_8\rightarrow s_7\rightarrow v_{12}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$，而由告警映射形成的节点序列为 $s_1\rightarrow v_1\rightarrow s_2\rightarrow s_5\rightarrow v_9\rightarrow v_8\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$，即缺失了告警 v_4、s_7 和 v_{12}，而 v_9 为冗余的告警，依据因果知识网络，选取了 3 个候选的攻击序列：$s_1\rightarrow v_1\rightarrow s_2\rightarrow v_4\rightarrow s_5\rightarrow v_8\rightarrow s_7\rightarrow v_{12}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$，$s_1\rightarrow v_1\rightarrow s_2\rightarrow v_4\rightarrow s_5\rightarrow v_7\rightarrow s_6\rightarrow v_{11}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$，$s_1\rightarrow v_1\rightarrow s_2\rightarrow v_4\rightarrow s_5\rightarrow v_2\rightarrow s_3\rightarrow v_9\rightarrow s_9$. 计算得出三者的概率分别为：0.845×0.144×0.301×(11−4)/11=0.2057=0.0233，0.845×0.144×0.238×(11−7)/11=0.0105，0.845×0144×0.155×0.175×(9−4)/9=0.0018，取 3 者概率最大的攻击序列，即可得出重构后的攻击序列为 $s_1\rightarrow v_1\rightarrow s_2\rightarrow v_4\rightarrow s_5\rightarrow v_8\rightarrow s_7\rightarrow v_{12}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$，与模拟的攻击序列一致，故攻击场景构建成功.

Table 6 Experimental Results of Three Different Simulated *Attackseq*

表 6 不同模拟攻击序列下的实验结果

Attackseq Number	Simulated *Attackseq*	*Nodeseq* Coming from Alarm Mapping	Candidate *Attackseq* and Their Probability
1	$s_1\rightarrow v_1\rightarrow s_2\rightarrow v_3\rightarrow s_4\rightarrow v_6\rightarrow s_6\rightarrow v_{11}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$	$s_1\rightarrow v_1\rightarrow v_3\rightarrow s_4\rightarrow v_6\rightarrow v_{11}\rightarrow v_{13}\rightarrow s_9$ (Missing: s_2, s_6, s_8)	$s_1\rightarrow v_1\rightarrow s_2\rightarrow v_3\rightarrow s_4\rightarrow v_6\rightarrow s_6\rightarrow v_{11}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$ (0.3515) $s_1\rightarrow v_1\rightarrow s_2\rightarrow v_4\rightarrow s_5\rightarrow v_7\rightarrow s_6\rightarrow v_{11}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$ (0.0158)
2	$s_1\rightarrow v_1\rightarrow s_2\rightarrow v_5\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$	$s_1\rightarrow v_2\rightarrow s_2\rightarrow v_5\rightarrow v_3\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$ (Adding: v_3)	$s_5\rightarrow v_8\rightarrow s_7\rightarrow v_{12}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$ (0.2057) $s_1\rightarrow v_1\rightarrow s_2\rightarrow v_3\rightarrow s_4\rightarrow v_6\rightarrow s_6\rightarrow v_{11}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$ (0.1758)
3	$s_1\rightarrow v_1\rightarrow s_2\rightarrow v_4\rightarrow s_5\rightarrow v_8\rightarrow s_7\rightarrow v_{12}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$	$s_1\rightarrow v_1\rightarrow s_2\rightarrow s_5\rightarrow v_9\rightarrow v_8\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$ (Missing: v_4, s_7, v_{12}; Adding: v_9)	$s_1\rightarrow v_2\rightarrow s_2\rightarrow v_4\rightarrow s_5\rightarrow v_8\rightarrow s_7\rightarrow v_{12}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$ (0.0233) $s_1\rightarrow v_1\rightarrow s_2\rightarrow v_4\rightarrow s_5\rightarrow v_7\rightarrow s_6\rightarrow v_{11}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$ (0.0105) $s_1\rightarrow v_2\rightarrow s_2\rightarrow v_4\rightarrow s_5\rightarrow v_{10}\rightarrow s_8\rightarrow v_{13}\rightarrow s_9$ (0.0155) $s_1\rightarrow v_1\rightarrow s_2\rightarrow v_4\rightarrow s_5\rightarrow v_2\rightarrow s_3\rightarrow v_9\rightarrow s_9$ (0.0018)

此外，与陈小军等人[12]的结果相比，在他们的第 2 个实验中，由于观测事件 o_6 的置信度为 1，而观测事件 o_7 和 o_9 的置信度小于 1，因此应用本文的方法可将文中求最可能的攻击路径的问题转化为已知节点序列 $v_7\rightarrow v_9$ 的条件下求最有可能的攻击场景. 由于攻击目标状态节点为 s_5，则候选的攻击序列为 $s_0\rightarrow v_6\rightarrow s_6\rightarrow v_7\rightarrow s_7\rightarrow v_8\rightarrow s_8\rightarrow v_9\rightarrow s_4\rightarrow v_5\rightarrow s_5$ 和 $s_0\rightarrow v_{10}\rightarrow s_7\rightarrow v_8\rightarrow s_8\rightarrow v_9\rightarrow s_4\rightarrow v_5\rightarrow s_5$. 计算可得前者的概率为 0.8×1×0.8×1×0.5×1×0.9×1×(11−8)/11=0.0785，后者的概率为 0.8×1×0.8×1×0.5×1×0.9×1×(9−8)/9=0.032，取二者概率最大的攻击序列，故应用本文方法构建的攻击场景为 $s_0\rightarrow v_6\rightarrow s_6\rightarrow v_7\rightarrow s_7\rightarrow v_8\rightarrow s_8\rightarrow v_9\rightarrow s_4\rightarrow v_5\rightarrow s_5$，与原文中结果保持一致，而由于陈小军的方法计算的是累积概率，导致其概率计算结果相对较大.

综上，本实验验证了本文提出的基于因果知识网络的攻击场景构建方法适用于解决告警缺失及冗余条件下攻击场景的构建问题.

4 结束语

目前，以高级持续性威胁(advanced persistent threat, APT)攻击为代表的多步攻击行为给网络安全造成了极大的威胁. 攻击场景构建能够通过告警数据重现攻击者的攻击过程，为攻击行为分析及预测提供了重要依据，是应对多步攻击威胁和实施网络安全主动防御的重要手段. 然而，在当前有关攻击场景构建的研究中，普遍缺乏对告警缺失及冗余的考虑，导致攻击场景构建不完整、不准确. 针对此问题，本文提出了基于因果知识网络的攻击场景构建方法. 首先选给出了因果知识网络的相关定义，并设计了获取因果知识网络的方法；然后在因果知识网络的基础上，利用概率推理分 2 步重构攻击场景. 实验结果表明，该方法能利用专家知识和数据挖掘相结合的优势，能够提高攻击场景构建的准确度，为网络管理员理解当前攻击行为态势提供了重要依据. 未来的工作包括考虑目标网络存在零日漏洞条件下攻击场景的重构问题.

参 考 文 献

[1] National Internet Emergency Center. 2015 Annual Report of Chinese Internet Security [M]. Beijing: Posts and Telecom Press, 2016: 26-87 (in Chinese)
(国家计算机网络应急技术处理协调中心. 2015 年中国互联网网络安全报告[M]. 北京: 人民邮电出版社, 2016: 26-87)

[2] Sadoddin R, Ghorbani A A. An incremental frequent structure mining framework for real-time alert correlation [J]. Computers & Security, 2009, 28(3/4): 153-173

[3] Wang Li, Ghorbani A, Li Yao. Automatic multi-step attack pattern discovering [J]. International Journal of Network Security, 2010, 10(2): 142-152

[4] Morin B, Debar H. Correlation of intrusion symptoms: An application of chronicles [C] //Proc of the 6th Int Symp on Recent Advances in Intrusion Detection. Berlin: Springer, 2003: 94-112

[5] Valeur F, Vigna G, Kruegel C, et al. Comprehensive approach to intrusion detection alert correlation [J]. IEEE Transactions on Dependable & Secure Computing, 2004, 1(3): 146-169

[6] Ning Peng, Cui Yun, Douglas S R, et al. Techniques and tools for analyzing intrusion alerts [J]. ACM Transactions on Information and System Security, 2004, 7(2): 274-318

[7] Jajodia S, Noel S, Kalapa P, et al. Cauldron: Mission-centric cyber situational awareness with defense in depth [C] //Proc of the 30th IEEE Conf on Military Communications. Piscataway, NJ: IEEE, 2011: 1339-1344

[8] Lü Huiying, Peng Wu, Wang Ruimei. 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 (in Chinese)
(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)

[9] Dewri R, Poolsappasit N, Ray I, et al. Optimal security hardening using multi-objective optimization on attack tree models of networks [C] //Proc of the 14th ACM Conf on Computer and Communications Security. New York: ACM, 2007: 204-213

[10] Ye Nong, Zhang Yebin, Borror C M. Robustness of the Markov-chain model for cyber-attack detection [J]. IEEE Transactions on Reliability, 2004, 53(1): 116-123

[11] Yu Dong, 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

[12] Chen Xiaojun, Fang Binxing, Tan Qingfeng, et al. Inferring attack intent of malicious insider based on probabilistic attack graph model [J]. Chinese Journal of Computers, 2014, 37(1): 62-72 (in Chinese)
(陈小军, 方滨兴, 谭庆丰, 等. 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)

[13] Wang Shuo, Tang Guangming, Kou Guang, et al. Attack path prediction method based on causal knowledge [J]. Journal on Communications, 2016, 37(10): 188-198 (in Chinese)
(王硕, 汤光明, 寇广, 等. 基于因果知识网络的攻击路径预测方法[J]. 通信学报, 2016, 37 (10): 188-198)

[14] Li Zhitang, Wang Li, Li Yao. Constructing attack scenarios through statistics and correlation of hi-alerts [J]. Journal of Computer Research and Development, 2006, 43(Suppl Ⅱ): 442-446 (in Chinese)
(李之棠, 王莉, 黎耀. 一种新的基于统计的攻击场景挖掘算法研究[J]. 计算机研究与发展, 2006, 43(增刊Ⅱ): 442-446)

[15] Wu Qingtao, Lu Kai, Li Lianmin. An improved attack scenarios reconstructing method based on causal correlation [J]. Microelectronics & Computer, 2009, 26(6): 121-124 (in Chinese)
(吴庆涛, 路凯, 李连民. 一种改进的基于因果关联的攻击场景重构方法[J]. 微电子学与计算机, 2009, 26(6): 121-124)

[16] Ma Linru, Yang Lin, Wang Jianxin. Using fuzzy clustering to reconstruct alert correlation graph of intrusion detection [J]. Journal on Communications, 2006, 27(9): 47-52 (in Chinese)
(马琳茹, 杨林, 王建新. 利用模糊聚类实现入侵检测告警关联图的重构[J]. 通信学报, 2006, 27(9): 47-52)

[17] Liu Jing, Gu Lize, Niu Xinxin. Network security events analyze method based on neural networks and genetic algorithm [J]. Journal of Beijing University of Posts and Telecommunications, 2015, 38(2): 50-54 (in Chinese)
(刘敬, 谷利泽, 钮心忻. 基于神经网络和遗传算法的网络安全事件分析方法[J]. 北京邮电大学学报, 2015, 38(2): 50-54)

[18] Liu Weixin, Zheng Kangfeng, Wu Bin. Alert processing based on attack graph and multi-source analyzing [J]. Journal on Communications, 2015, 36(9): 135-144 (in Chinese)
(刘威歆, 郑康锋, 武斌. 基于攻击图的多源告警关联分析方法[J]. 通信学报, 2015, 36(9): 135-144)

[19] Hu Liang, Xie Nannan, Nu Erbuli. A multi-stage attack scenario recognition algorithm based on intelligent planning [J]. Acta Electroniga Sinica, 2013, 41(9): 1753-1759 (in Chinese)
(胡亮, 解男男, 努尔布力. 基于智能规划的多步攻击场景识别算法[J]. 电子学报, 2013, 41(9): 1753-1759)

[20] Mei Haibin, Gong Jian, Zhang Minghua. Research on discovering multi-step attack patterns based on clustering IDS alert sequences [J]. Journal on Communications, 2011, 32(5): 63-69 (in Chinese)
(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)

[21] Feng Xuewei, Wang Dongxia, Huang Minhuan. A mining approach for causal knowledge in alert correlating based on the Markov [J]. Journal of Computer Research and Development, 2014, 51(11): 2493-2504 (in Chinese)
(冯学伟, 王东霞, 黄敏桓. 一种基于 Markov 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)

[22] Ammann P, Wijesekera D, Kaushik S. Scalable graph-based network vulnerability analysis [C] //Proc of the 9th ACM Conf on Computer and Communications Security. New York: ACM, 2002: 217-224

[23] Liu Xuejiao. Research on network vulnerability assessment and intrusion alert analysis technology [D]. Wuhan: Huazhong Normal University, 2011 (in Chinese)
(刘雪娇. 网络脆弱性评估及入侵报警分析技术研究[D]. 武汉: 华中师范大学, 2011)

[24] Zhu Lina, Zhang Zuochang. Research on hierarchical alerts correlation based on causality [J]. Application Research of Computers, 2016, 33(3): 848-859 (in Chinese)
(朱丽娜, 张作昌. 基于因果关系的分层报警关联研究[J]. 计算机应用研究, 2016, 33(3): 848-859)

Wang Shuo, born in 1991. PhD candidate in PLA Information Engineering University. His main research interests include network security and machine learning.

Tang Guangming, born in 1963. PhD, professor, PhD supervisor. Her main research interests include network and information security.

Wang Jianhua, born in 1962. Professor, PhD supervisor. His main research interests include information security and security management.

Sun Yifeng, born in 1976. PhD, associate professor, master supervisor. His main research interests include network security and machine learning.

Kou Guang, born in 1983. PhD, lecturer. His main research interests include network security and machine learning.