基于属性攻击图的动态威胁跟踪与量化分析技术研究

杨英杰 冷 强* 潘瑞萱 胡 浩

(信息工程大学 郑州 450001)

摘 要：网络多告警信息融合处理是有效实施网络动态威胁分析的主要手段之一。基于此该文提出一种利用网络系统多告警信息进行动态威胁跟踪与量化分析的机制。该机制首先利用攻击图理论构建系统动态威胁属性攻击图；其次基于权限提升原则设计了前件推断算法(APA)、后件预测算法(CPA)和综合告警信息推断算法(CAIIA)进行多告警信息的融合与威胁分析，生成网络动态威胁跟踪图进行威胁变化态势的可视化展示。最后通过实验验证了该机制和算法的有效性。

关键词：多告警信息；网络动态威胁分析；属性攻击图；权限提升

中图分类号：TP393 **文献标识码**：A **文章编号**：1009-5896(2019)09-2172-08

DOI: 10.11999/JEIT181117

Research on Dynamic Threat Tracking and Quantitative Analysis Technology Based on Attribute Attack Graph

YANG Yingjie LENG Qiang PAN Ruixuan HU Hao

(*Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: Network multi-alarm information fusion processing is one of the most important methods to implement effectively network dynamic threat analysis. Focusing on this, a mechanism for dynamic threat tracking and quantitative analysis by using network system multi-alarm information is proposed. Firstly, the attack graph theory is used to construct the system dynamic threat attribute attack graph. Secondly, based on the privilege escalation principle, Antecedent Predictive Algorithm(APA), the Consequent Predictive Algorithm(CPA) and the Comprehensive Alarm Information Inference Algorithm(CAIIA) are designed to integrate the multi-alarm information fusion and do threat analysis. Then, the network dynamic threat tracking graph is generated to visualize the threat change situation. Finally, the effectiveness of the mechanism and algorithm is validates through experiments.

Key words: Multiple alarm information; Network dynamic threat analysis; Attribute attack graph; Privilege escalation

1 引言

网络信息系统固有的脆弱性使其不可避免地面临外在威胁的影响，针对外在动态、变化的威胁开展有效分析对于实施针对性的防御决策具有重要支撑作用。随着信息网络规模的不断扩大，仅仅割裂式地针对单一或部分主机、服务器等开展威胁信息采集与分析，已无法满足信息网络动态威胁分析的需求，因此必须融合信息网络整体威胁信息，才能有效实施信息网络动态威胁态势分析。

现有的网络威胁信息主要体现在报警日志、入侵检测系统(Intrusion Detection Systems, IDS)、异常行为检测、网络预警等告警信息，因此如何融合处理网络告警信息是研究网络动态威胁的关键。目前研究人员在该领域开展了大量的研究并取得了一定的研究成果。文献[1]提出了基于信息融合的网络安全态势评估模型，引入改进的D-S证据理论融合态势要素和节点态势计算网络安全态势；文献[2]研究了从告警数据中发现多步攻击模式的方法，通过定义告警间的相似度函数来构建攻击活动序列集。但是在直接融合处理网络告警信息需要对网络

收稿日期：2018-12-04；改回日期：2019-04-05；网络出版：2019-04-22
*通信作者： 冷强 lqsly1993@163.com
基金项目：国家“863”高技术研究发展计划基金(2015AA016006)，国家重点研发计划(2016YFF0204003)，国家自然科学基金(61471344)

Foundation Items: The National “863” High Technology Research and Development Program of China (2015AA016006), The National Key Research and Development Program of China (2016YFF0204003), The National Natural Science Foundation of China (61471344)

系统中的多节点进行关联分析研究，因此在近年来，利用攻击图理论融合处理网络多告警信息的研究方法成为了研究网络威胁的主流方法。

攻击图[3,4]是研究网络动态威胁转移的主要方法；文献[5–11]在攻击图模型构建技术和威胁转移概率度量方法等方面开展了研究，为研究网络威胁转移与攻击行为预测做出了一定的贡献。在此基础上，文献[12]首次提出基于序列图的攻击图结构融合处理告警信息，并采用宽度优先搜索(Breadth First Search, BFS)算法树遍历前件节点和后件节点；文献[13,14]提出了一种分布式IDS关联系统，融合告警信息，存在的问题是并未考虑攻击图中环路问题；文献[15]提出了一种基于攻击图的混合告警关联模型，能够关联攻击图已知的告警，但是没有解决后件漏报的问题；文献[16]基于威胁状态转移图发掘威胁事件的时空关联关系，获得当前有效威胁及网络实时状态，从而量化评估安全威胁；文献[17]基于前后件推断的方法，解决攻击图中的告警漏报和减少误报的问题；文献[18]根据因果知识网络，首先通过告警识别已经发生的攻击行为，然后预测攻击路径。文献[19]在不同的比例因子信息熵中使用均方差(Mean Squared Error, MSE)，然后选择适当的比例信息以处理告警时间序列数据，最后使用隐马尔可夫模型训练网络参数，预测未来网络安全状况。但是上述研究利用的是状态攻击图处理多告警信息，首先状态攻击图存在状态爆炸的问题[8]；且利用攻击图研究网络告警信息存在未考虑攻击图中节点间的服务存取访问关系对网络威胁转移的影响。

基于上述分析，本文首先给出了基于攻击图理论的动态威胁跟踪分析机制；其次设计了动态威胁跟踪分析机制中的前件推断算法(Antecedent Predictive Algorithm, APA)、后件预测算法(Consequent Predictive Algorithm, CPA)和综合告警信息推断算法(Comprehensive Alarm Information Inference Algorithm, CAIIA)；最后通过仿真实验验证了动态威胁跟踪分析机制和算法的有效性。

2　动态威胁跟踪分析机制

在网络动态威胁分析中需要对系统的告警信息进行有效的融合处理，本文所提融合处理机制(详见图1)是首先利用攻击图理论构建系统动态威胁属性攻击图模型(见定义1)，并结合具体网络系统配置信息、漏洞信息，以及网络节点间服务的存取访问关系等生成攻击图；接着利用权限提升原则，设计APA, CPA和CAIIA(详见第3节)进行告警信息的融合；最后通过定义推断强度(见定义2)量化系统威胁，得到网络的动态威胁跟踪图描述网络系统威胁的动态变化态势。其中H表示网络系统中的主机或服务器设备。

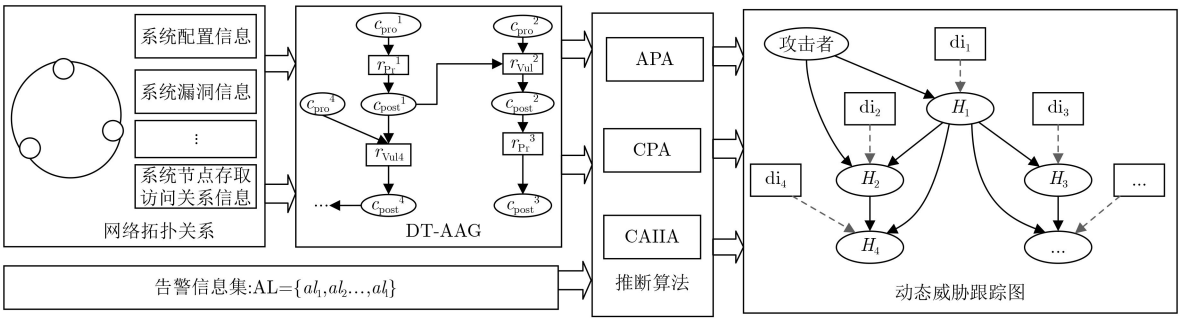

图 1 动态威胁跟踪机制图

(1) 属性攻击图模型定义

属性攻击图模型是进行动态威胁分析的理论基础，具体定义如下：

定义1　动态威胁属性攻击图(Dynamic Threat Attribute Attack Graph, DT-AAG)模型由4元组$\mathrm{DT-AAG}=(C,R,E,p)$表示，其中$C$表示威胁转移条件属性集，$R$表示威胁转移条件属性间的关系集，$E$表示连接条件属性和关系的边集，$p$表示威胁转移概率。

(a) 威胁转移条件属性集C

$C=C_{\mathrm{Pro}}\cup C_{\mathrm{Post}}$，其中，$C_{\mathrm{Pro}}$是前置条件，即攻击者利用系统漏洞或者协议的前提条件，其中包括身份认证、攻击可达性、服务存在漏洞等；当攻击者利用协议提升权限时，前提条件一般是协议认证有效性、身份认证等；C_{Post}是后置条件，即攻击者利用前提条件攻击系统漏洞或者根据协议获得的权限。前置条件和后置条件用节点IP表示。

(b) 威胁转移条件属性间的关系集R

$R=\{r_{\mathrm{Vul}},r_{\mathrm{Pr}}\}$为通过漏洞或协议关联主机或服务的节点集，4元组$r_{\mathrm{Vul}}=(\mathrm{IP}_{\mathrm{Pro}},\mathrm{IP}_{\mathrm{Post}},\mathrm{Vul},0)$和$r_{\mathrm{Pr}}=(\mathrm{IP}_{\mathrm{Pro}},\mathrm{IP}_{\mathrm{Post}},0,\mathrm{Pr})$表示漏洞和协议节点。其中$\mathrm{IP}_{\mathrm{Pro}}$表示通过攻击漏洞或者利用协议获得权限

的源IP; $\mathrm{IP}_{\mathrm{Post}}$表示通过攻击漏洞或者利用协议获得权限的目标IP; Vul表示攻击者提升权限利用的漏洞；Pr表示攻击者提升权限的协议。为了更加全面地描述系统安全，给定数据存取访问关系为协议Pr(Protocol)。攻击者可以利用Pr，提升自身在系统中的权限。

(c) 连接条件属性和关系的边集E

$E=\{C_{\mathrm{Pro}}\times R\}\cup\{R\times C_{\mathrm{Post}}\}=\{C_{\mathrm{Pro}}\times r_{\mathrm{Vul}}\}\cup\{r_{\mathrm{Vul}}\times C_{\mathrm{Post}}\}\cup\{C_{\mathrm{Pro}}\times r_{\mathrm{Pr}}\}\cup\{r_{\mathrm{Pr}}\times C_{\mathrm{Post}}\}$，其中$C_{\mathrm{Pro}}\times r_{\mathrm{Vul}}$表示前置条件指向漏洞节点的边，$r_{\mathrm{Vul}}\times C_{\mathrm{Post}}$表示漏洞节点指向后置条件的边，$C_{\mathrm{Pro}}\times r_{\mathrm{Pr}}$表示前置条件指向协议的边，$r_{\mathrm{Pr}}\times C_{\mathrm{Post}}$表示协议指向后置条件的边。

(d) 威胁转移概率p

p为威胁转移概率，即攻击者利用前提条件攻击系统中漏洞的成功概率，或者为攻击者利用系统中的协议提升权限的概率。其中攻击者根据C_{Pro}对系统中存在的Vul实施单次转移概率叫做单个漏洞转移概率。当攻击者通过业务应用中的访问协议提升攻击者在系统中的权限时，$p=1$。由于在网络系统中，攻击者利用业务应用背景的数据存取访问关系攻击系统时，不需要攻击系统中的漏洞，因此，转移概率为1。

(2) 告警信息格式

告警信息是进行动态威胁分析的数据基础，为了便于告警信息的融合处理，给出如下格式规范：al = (time, IPpro, IPpost, class)。其中，al表示告警信息元素，time表示告警产生的时间，IPpro表示产生告警的源IP, IPpost表示产生告警的目标IP，class表示产生告警的漏洞类型。本文定义AL为告警信息集合，即$\mathrm{al}\in\mathrm{AL}$。

(3) 节点权限

因为攻击者攻击网络系统是自身在系统中提升权限的过程，在此定义W_{IP_i}表示网络节点IP_i在系统中的权限，权限大小与攻击者攻击目标存在紧密的关联关系，如图2所示，攻击者在攻击过程中，如果攻击者的攻击目标为节点c，节点a,b,c的权限大小关系为：$W_a<W_b<W_c$；如果攻击者的攻击目标为节点b，那么节点c不在攻击者的攻击范围之内，因此节点a,b与节点c的权限无大小关系，权限关系为：$W_a<W_b$。

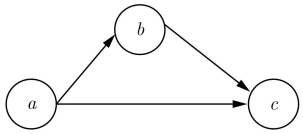

图 2 拓扑实例图

(4) 推断强度定义

动态威胁跟踪分析的目的是实时给出各个网络节点的推断强度，以展示整个威胁动态变化态势。在此推断强度定义如下：

定义2 推断强度DI(Deducetion Intensity), $\mathrm{di}\in\mathrm{DI}$表示从已告警节点推断出未告警节点的威胁转移概率，其中di的取值范围为$[0,1]$。

3 告警信息推断算法

在动态威胁跟踪分析机制中，告警信息的融合处理是关键，针对此问题本文设计了前件推断算法、后件预测算法和综合告警信息推断算法，其中前件推断算法和后件预测算法是分别对已告警节点的前件节点和后件节点进行推断强度的量化确定；综合告警信息推断算法是基于多告警信息，利用前件推断算法和后件预测算法进行网络整体威胁变化态势的量化确定。

3.1 前件推断算法

鉴于攻击者在攻击网络系统时，是一个权限提升的过程，虽然更侧重于对攻击者后续攻击行为的关注，但是对前件节点进行推断分析也至关重要。但是为了减少不必要的推断计算，本文对前件节点只推断一步。下面分析在前件推断过程中存在的两种情况：

(1) 攻击者是利用系统中的节点对告警节点进行攻击获得权限的情况；

(2) 攻击者是由外网直接攻击告警节点获得告警节点权限的情况。

第1种情况表示攻击者利用网络系统中的节点权限攻击产生告警的节点，意味着攻击者获得了告警节点的前件节点的权限，因此推断到告警节点的前一个节点，且确定该前件节点推断强度为1。当该前件节点不止告警节点一个后件节点时，需要对该前件节点的未告警的后件节点进行推断；当该前件节点只有告警节点一个后件节点时，停止推断。

第2种情况表示攻击者是通过网络系统外的节点对系统中产生告警节点进行攻击，因此推断到告警节点前一个节点，且确定该前件节点推断强度为0。

下面利用一个简单的前件推断图解释说明两种情况，如图3。

当节点b产生告警信息$\mathrm{al}_b=(\mathrm{time}_b,\mathrm{IPpro}_b,\mathrm{IPpost}_b,\mathrm{class}_b)$时，判断$\mathrm{IPpro}_b=\mathrm{IP}_a$是否成立，如果不成立，则推断节点$b$的前件节点$a$的推断强度为0，即$\mathrm{di}_a=0$；如果成立，则$\mathrm{di}_a=1$。

当$\mathrm{di}_a=1$，则继续预测节点a的其余后件节点c。

前件推断算法具体如表1。

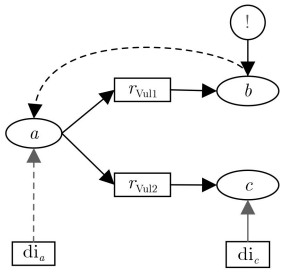

图 3 前件推断图

表 1　前件推断算法

算法1：前件推断算法(APA)
输入：DT − AAG, al_l
输出：DI
(1) $al_l = (time_l, IPpro_l, IPpost_l, class_l)$;
(2) if $IPpost_l = IP'_l$, set $di_l = 1$;
//根据IP地址确定攻击图中产生告警信息的节点;
(3) set l–1, l, l+1,···, l+m;
//按照攻击图中关于节点l 的路径的节点权限排序;
(4) if $IPpro_l = IP'_{l-1}$, set $di_{l-1} = 1$;
//如果该告警信息的源IP在系统中，表示攻击者已经获得该节点的前件节点的权限;
(5) { if not only $c_{l-1} \rightarrow c_l$;
//节点l–1的后置条件包含不止节点l;
(6) { set $l'-1, l', l'+1, \cdots, l'+n(n \le m-1)$;
//设置节点l-1的后件节点中非包含l节点路径的其余节点的顺序;
(7) $di_{l'-1} = di_{l-1} = 1$;
(8) DO { CPA($l'-1$); // 对节点$l'-1$执行后件预测算法;
(9) }}}
(10) else
(11) set $di_{l-1} = 0$;
//该告警节点与其所处攻击图中的前件节点无关，因此设置其前件节点推断强度为0;
(12) return DI

3.2　后件预测算法

利用系统告警信息预测攻击者的后续攻击行为，是研究网络动态威胁的关键，因此与前件推断算法不同，在后件预测算法中对告警节点的后件节点进行多步预测，以确定未告警节点的推断强度。下面利用一个简单的后件预测图解释说明，如图4。

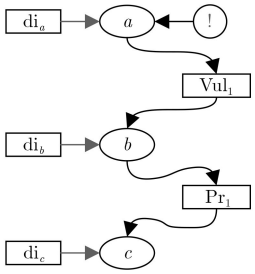

图 4 后件预测实例图

当节点a产生告警，根据节点a在属性攻击图中的位置，截取其中一条路径，利用节点间关联关系预测后件。其中攻击者在获得节点a的权限后，通过攻击Vul_1可以获得节点b的权限；攻击者在获得节点b的权限后，可以利用节点b与节点c之间的协议关系获得节点c的权限。

当$di_a = 1$，攻击者攻击Vul_1的成功概率为p_1，那么节点b的预测强度为：$di_b = p_1$；同理，节点c的预测强度为：$di_c = p_1 \times Pr_1$，由定义1可知：$Pr_1 = 1$，则$di_c = p_1$。

为了减少不必要的计算开支，设置阈值λ，当$di_i \ge \lambda$，且$di_{i+1} < \lambda$时，停止推断节点i+1的后件节点i+2。其中di_{i+1}表示节点i+1的推断强度，di_i表示节点i的推断强度，并且节点i+1是节点i的后件节点；λ为设置的一个推断强度阈值，表示该节点在具有λ的推断强度时，对系统的威胁程度较低，不需要继续推断下一节点。$\lambda \in [0,1)$，λ的设定与系统的安全需求有关，当网络系统的安全需求较高时，λ值较低；当网络系统安全需求较低时，λ值较高。

与文献[17]不同的是，本文没有设定推断层数，而是以推断强度为标准描述网络节点的威胁状态，且每一个告警节点的推断层数可以不同。

文献[17]确定推断层数，存在两个问题：

(1) 当攻击者触发某些节点的告警时，可能攻击者不会攻击该节点相邻的其他节点，但是文献[17]确定推断层数使得算法必须要推断相邻的节点，增加了误报；

(2) 当攻击者触发某个节点的告警，恰好该节点相邻的节点与攻击者相邻的攻击目标相关联，则攻击者会攻击该节点相邻的节点，限制推断层数将会漏掉对重要节点的推断。

因此，本文结合攻击转移概率确定推断强度，推断相应的节点，减少不必要的计算开支，提高推断准确度。

后件预测算法具体如表2。

3.3　综合告警信息推断算法

上面给出了单个告警信息的前件推断算法和后件预测算法推断告警节点相邻的节点，在实际的网络环境中，有组织的协同攻击行为越来越多，为了更好地分析多攻击行为，下面融合处理多告警信息，完成对系统威胁态势的分析。

在网络系统面临多个告警信息时，其中每个告警信息遵循单个告警信息的前件推断算法和后件预测算法。然后将每个告警信息的推断强度相结合，得到多告警信息融合处理后的整体威胁态势，如图5。

表 2 后件预测算法

算法2：后件预测算法(CPA)
输入：DT − AAG, al_l
输出：DI
(1) $\mathrm{al}_l=(\mathrm{time}_l,\mathrm{IPpro}_l,\mathrm{IPpost}_l,\mathrm{class}_l)$；
(2) if $\mathrm{IPpost}_l=\mathrm{IP}'_l$, set $\mathrm{di}_l=1$；
(3) set l–1, l, l+1,…, l+m；
(4) for(i=1, $\mathrm{di}_{l+i}\geq\lambda\&\&i\leq m$, i++)
(5) $\{\mathrm{di}_{l+i}=\prod_{j=1}^{i}p_{l+j}\times\mathrm{di}_l;\ \}$
(6) when $\mathrm{DI}_{l+i}=\{\mathrm{di}^1_{l+i},\mathrm{di}^2_{l+i},\cdots,\mathrm{di}^n_{l+i}\}$；
//从节点l到节点l+i有n条路径，DI_{l+i}的元素都是由al_l推断；
(7) DO {
(8) $\mathrm{di}_{l+i}=\max(\mathrm{di}^1_{l+i},\mathrm{di}^2_{l+i},\cdots,\mathrm{di}^n_{l+i})$; }
//取单个告警不同路径中推断强度最大的值；
(9) Return DI

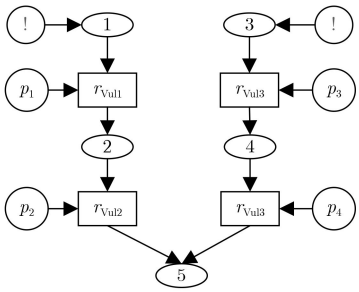

图 5 多告警信息实例图

当处理网络告警信息时，存在告警$\mathrm{al}_1=(\mathrm{time}_1,\mathrm{IPpro}_1,\mathrm{IPpost}_1,\mathrm{class}_1)$ 和$\mathrm{al}_3=(\mathrm{time}_3,\mathrm{IPpro}_3,\mathrm{IPpost}_3,\mathrm{class}_3)$，根告警信息推断算法可知，$\mathrm{di}_1=\mathrm{di}_3=1$。可知$\mathrm{di}_2=p_1$，$\mathrm{di}_4=p_3$。表3给出综合告警信息推断算法。

根据CAIIA得到图5中节点5的综合推断强度：$\mathrm{di}_5=\min(p_1\times p_2+p_3\times p_4,1)$。

4 实验

4.1 实验分析

为了验证本文威胁动态跟踪分析机制和算法的有效性，构建了网络实验环境如图6所示，具体包含3个主机和2个服务器，以及2个防火墙和2个IDS。

首先通过对系统主机服务器进行漏洞扫描和结合网络系统的业务访问关系，查询CVE[20]数据库漏洞信息，并在NVD[21]数据库查询到风险等级评分，结合CVSS[22]评分标准，得到系统节点间的威胁转移概率。

得到网络系统信息如表4和表5所示：

表 3 综合告警信息推断算法

算法3：综合告警信息推断算法(CAIIA)
输入：DT − AAG, AL
输出：DI
(1) AL $\neq\varnothing$; //告警信息不为空；
(2) $\mathrm{al}_i\in$ AL；
(3) for each
(4) $\mathrm{al}_i=(\mathrm{time}_i,\mathrm{IPpro}_i,\mathrm{IPpost}_i,\mathrm{class}_i)$；
(5) if $\mathrm{IPpost}_i=\mathrm{IP}'_i$, set $\mathrm{di}_i=1$；
(6) DO { APA(i); // 对节点i执行前件推断算法；
(7) CPA(i) //对节点i执行后件预测算法 }
(8) if $\mathrm{IP}_j\notin\bigcup_{\mathrm{al}_i\in\mathrm{AL}}\mathrm{IPpost}_i$；
(9) { $\mathrm{di}_j=\sum_{\mathrm{al}_k\in\mathrm{AL}}\mathrm{di}_k$；
//计算产生告警节点推断未产生告警的节点的推断强度；
(10) if $\mathrm{di}_j>1$, let $\mathrm{di}_j=1$； }
//表示将推强度大于1的值确定为1；
(11) else
(12) set $\mathrm{di}_i=1$；
(13) return DI

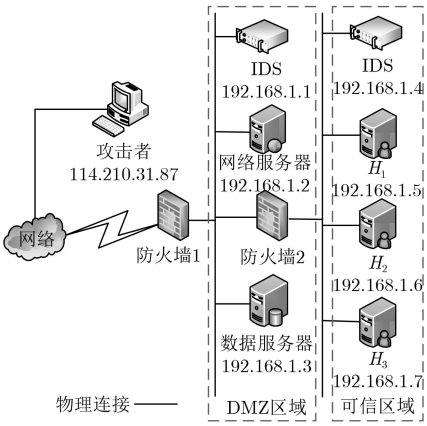

图 6 实验图

表 4 系统漏洞、协议关系表

Host/Server	Protocol/Vulnerability	Port
Web	Protocol with H_1&H_2 /IIS	445&80
Data	Apache	80
H_1	Protocol with Web /HIDP	445
H_2	Protocol with Web/GUN Wget	80
H_3	NDproxy	445

其次对系统中权限关系进行排序，得到节点间权限关系：$W_{\mathrm{Web}}<W_{\mathrm{Data}}<W_{H_1}<W_{H_2}<W_{H_3}$然后根据系统中主机和服务器开放的端口和存在的漏洞结合属性攻击图模型，构建系统属性攻击图，根

表 5　漏洞信息表

Vul.	CVE Num.	Vul. Risklevel
IIS	CVE-2015-7597	7.8
Apache	CVE-2018-8015	7.5
HIDP	CVE-2018-8169	7.0
GUN Wget	CVE-2016-4971	8.8
NDproxy	CVE-2013-5065	7.2

据实验环境可知，攻击者通过攻击DMZ区域的服务器节点，然后攻击可信区域的服务器节点。得到网络系统属性攻击图如图7。

最后实时分析AL = $\{al_1, al_2\}$，其中$al_1 = (time_1, 213.92.100.63, 192.168.1.3, Apache)$，$al_2 = (time_2, 192.168.1.2, 192.168.1.3, Apache)$，且$time_1 < time_2$（表示$time_1$在$time_2$之前），设置参数$\lambda = 0.5$。首先在$time_1$时刻实时分析告警$al_1$，对$al_1$执行CAIIA得到如图8的威胁状态图。

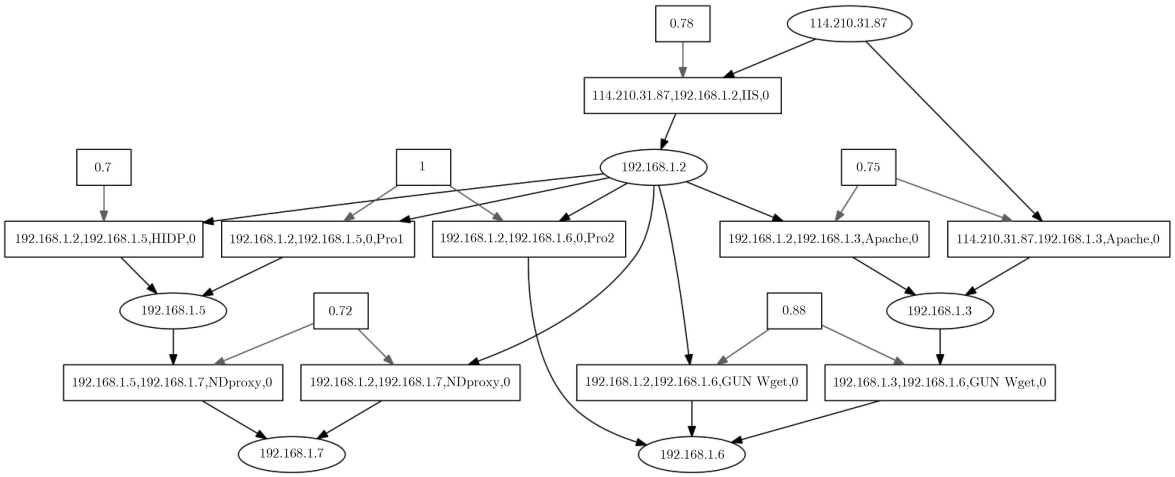

图 7 网络属性攻击图

由图8可知，攻击者可能对节点192.168.1.6进行下一步的攻击，因此在$time_1$时刻需要着重考虑对节点192.168.1.6采取防御措施。

然后在$time_2$时刻实时分析al_2，得到如图9的威胁状态图：

通过对al_2执行CAIIA，得到图9的系统威胁状态图，可知，系统中除了节点192.168.1.7推断强度小于1，其余节点推断强度都为1，需要立即采取针对性的防御措施保护系统安全。

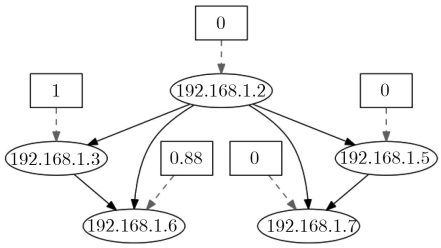

图 8 $time_1$威胁状态图

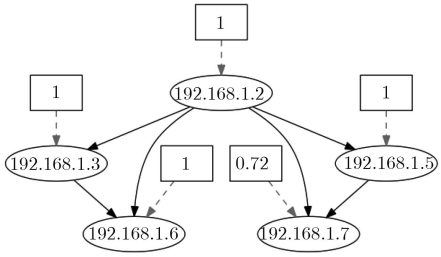

图 9 $time_2$威胁状态图

4.2　关联分析

为了对比分析本文的CAIIA和文献[17]对系统威胁转移的分析能力。下面利用文献[17]的融合处理告警信息方法，分析图6的实验环境。

为了更好对比本文算法和文献[17]，下面运用本文的节点表示方法对文献[17]的告警信息融合算法进行分析研究。根据文献[17]的算法，与文献[17]中实验相同，设置推断层数为3，然后在$time_1$时刻对告警al_1实时分析，得到如图10：

由于文献[17]的推断方法是单路径推断，因此在节点192.168.1.3同一条路径上的前件和后件的3层内都推断为1。

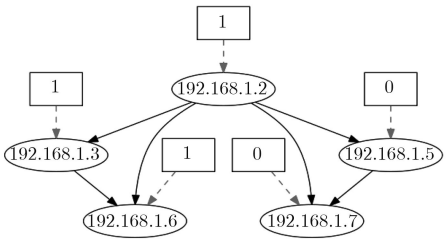

图 10 文献[17]$time_1$威胁状态图

然后在time_2时刻利用文献[17]方法实时分析al_2，得到图11的威胁状态图：

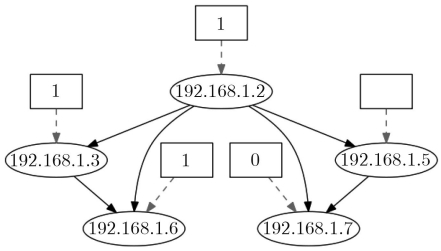

图 11 文献[17]time_2威胁状态图

由于文献[17]只考虑告警节点，没有考虑攻击的源节点被攻击成功的情况，因此与本文的结果不同；且文献[17]没有考虑节点间的存取访问关系对网络威胁转移的影响，在上述实验中由于产生告警节点192.168.1.3与其余节点没有存取访问关系，因此没有体现在实验图中。

本文在攻击路径、威胁转移概率、前后件推断、消解环路、实时分析、综合多路径、权限提升和存取访问关系等方面与文献[15]和文献[17]做了比较。如表6，本文与文献[17]相比较，利用威胁转移概率细化网络节点的推断强度；考虑多路径更准确地推断非告警节点；加入权限提升的因素提高预测后件的能力；分析存取访问关系完善攻击图和攻击路径，更加准确地分析告警节点对非告警节点的推断情况。本文与文献[15]相比较，对前件进行推断，多角度地对网络告警信息进行分析；消解攻击图中的攻击环路，从而构建实用的网络攻击图；实时分析网络告警信息，能够及时为管理人员提供网络威胁的状况。

表 6 关联分析

文献	攻击路径	威胁转移概率	前后件推断	消解环路	实时分析	综合多路径	权限提升	存取访问关系
文献[15]	√	√	×	×	×	×	×	×
文献[17]	√	×	√	√	√	×	×	×
本文	√	√	√	√	√	√	√	√

5 结束语

网络动态威胁分析至今仍然是网络安全领域研究的热点之一。本文提出了一种利用多告警信息进行网络动态威胁跟踪与量化分析的技术，设计了网络动态威胁机制；创新性地提出了利用威胁转移概率对推断强度进行度量的方法；其次结合了权限提升原则，并考虑了网络服务之间的协议，完善了攻击图；接着给出了前件推断算法、后件预测算法和综合告警算法；为动态威胁实时监测提供了一种新的手段。下一步还需在网络动态威胁分析的基础上，研究威胁对网络系统带来的风险，以及基于风险的防御决策。

参 考 文 献

[1] 韦勇. 网络安全态势评估模型研究[D]. [博士论文], 中国科学技术大学, 2009.
WEI Yong. Research on network security situational awareness model[D]. [Ph.D. dissertation], University of Science and Technology of China, 2009.

[2] 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. doi: 10.3969/j.issn.1000-436X.2011.05.009.
MEI Haibin, GONG Jian, and ZHANG Minghua. Research on discovering multi-step attack patterns based on clustering IDS alert sequences[J]. *Journal on Communications*, 2011, 32(5): 63–69. doi: 10.3969/j.issn.1000-436X.2011.05.009.

[3] PHILLIPS C and SWILER L P. A graph-based system for network-vulnerability analysis[C]. The 1998 Workshop on New Security Paradigms, Charlottesville, USA, 1998: 71–79. doi: 10.1145/310889.310919.

[4] SWILER L P, PHILLIPS C, ELLIS D, *et al*. Computer-attack graph generation tool[C]. The 2nd DARPA Information Survivability Conference and Exposition, Anaheim, USA, 2001: 307–321. doi: 10.1109/DISCEX.2001.932182.

[5] 王会梅, 鲜明, 王国玉. 基于扩展网络攻击图的网络攻击策略生成算法[J]. 电子与信息学报, 2011, 33(12): 3015–3021. doi: 10.3724/SP.J.1146.2011.00414.
WANG Huimei, XIAN Ming, and WANG Guoyu. A network attack decision-making algorithm based on the extended attack graph[J]. *Journal of Electronics & Information Technology*, 2011, 33(12): 3015–3021. doi: 10.3724/SP.J.1146.2011.00414.

[6] 苏婷婷, 潘晓中, 肖海燕, 等. 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. doi: 10.3724/SP.J.1146.2012.00261.
SU Tingting, PAN Xiaozhong, XIAO Haiyan, *et al*. Research on attack graph based on attributes adjacncy matrix[J]. *Journal of Electronics & Information Technology*, 2012, 34(7): 1744–1747. doi: 10.3724/SP.J.1146.2012.00261.

[7] 黄永洪, 吴一凡, 杨豪璞, 等. 基于攻击图的APT脆弱节点评估方法[J]. 重庆邮电大学学报: 自然科学版, 2017, 29(4):

535–541. doi: 10.3979/j.issn.1673-825X.2017.04.017.
HUANG Yonghong, WU Yifan, YANG Haopu, *et al*. Graph-based vulnerability assessment for APT attack[J]. *Journal of Chongqing University of Posts and Telecommunications*: *Natural Science Edition*, 2017, 29(4): 535–541. doi: 10.3979/j.issn.1673-825X.2017.04.017.

[8] 叶子维, 郭渊博, 王宸东, 等. 攻击图技术应用研究综述[J]. 通信学报, 2017, 38(11): 121–132. doi: 10.11959/j.issn.1000-436x.2017213.
YE Ziwei, GUO Yuanbo, WANG Chendong, *et al*. Survey on application of attack graph technology[J]. *Journal on Communications*, 2017, 38(11): 121–132. doi: 10.11959/j.issn.1000-436x.2017213.

[9] HU Hao, LIU Yulin, ZHANG Hongqi, *et al*. Security metric methods for network multistep attacks using AMC and big data correlation analysis[J]. *Security and Communication Networks*, 2018, 2018: 5787102. doi: 10.1155/2018/5787102.

[10] WANG Huan, CHEN Zhanfang, ZHAO Jianping, *et al*. A vulnerability assessment method in industrial internet of things based on attack graph and maximum flow[J]. *IEEE Access*, 2018, 6: 8599–8609. doi: 10.1109/ACCESS.2018.2805690.

[11] 胡浩, 叶润国, 张红旗, 等. 面向漏洞生命周期的安全风险度量方法[J]. 软件学报, 2018, 29(5): 1213–1229. doi: 10.13328/j.cnki.jos.005507.
HU Hao, YE Runguo, ZHANG Hongqi, *et al*. Vulnerability life cycle oriented security risk metric method[J]. *Journal of Software*, 2018, 29(5): 1213–1229. doi: 10.13328/j.cnki.jos.005507.

[12] WANG Lingyu, LIU Anyi, and JAJODIA S. Using attack craphs for correlating, hypothesizing, and predicting intrusion alerts[J]. *Computer Communications*, 2006, 29(15): 2917–2933. doi: 10.1016/j.comcom.2006.04.001.

[13] ROSCHKE S, CHENG F, and MEINEL C. A New Alert Correlation Algorithm Based on Attack Graph[M]. HERRERO Á, CORCHADO E. Computational Intelligence in Security for Information Systems. Berlin, Germany: Springer, 2011: 58–67. doi: 10.1007/978-3-642-21323-6_8.

[14] ROSCHKE S, CHENG F, and MEINEL C. High-quality attack graph-based IDS correlation[J]. *Logic Journal of the IGPL*, 2013, 21(4): 571–591. doi: 10.1093/jigpal/jzs034.

[15] AHMADINEJAD S H, JALILI S, and ABADI M. A hybrid model for correlating alerts of known and unknown attack scenarios and updating attack graphs[J]. *Computer Networks*, 2011, 55(9): 2221–2240. doi: 10.1016/j.comnet.2011.03.005.

[16] 吕慧颖, 彭武, 王瑞梅, 等. 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. doi: 10.7544/issn1000-1239.2014.20120816.
Huiying, PENG Wu, WANG Ruimei, *et al*. 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. doi: 10.7544/issn1000-1239.2014.20120816.

[17] 刘威歆, 郑康锋, 武斌, 等. 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. doi: 10.11959/j.issn.1000-436x.2015193.
LIU Weixin, ZHENG Kangfeng, WU Bin, *et al*. Alert processing based on attack graph and multi-source analyzing[J]. *Journal on Communications*, 2015, 36(9): 135–144. doi: 10.11959/j.issn.1000-436x.2015193.

[18] 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. doi: 10.11959/j.issn.1000-436x.2016210.
WANG Shuo, TANG Guangming, KOU Guang, *et al*. Attack path prediction method based on causal knowledge net[J]. *Journal on Communications*, 2016, 37(10): 188–198. doi: 10.11959/j.issn.1000-436x.2016210.

[19] LIANG Wei, CHEN Zuo, YAN Xiaolong, *et al*. Multiscale entropy-based weighted hidden Markov network security situation prediction model[C]. 2017 IEEE International Congress on Internet Of Things (ICIOT), Honolulu, USA 2017: 97–104. doi: 10.1109/IEEE.ICIOT.2017.31.

[20] CVE. Common vulnerabilities and exposures[EB/OL]. http://cve.mitre.org/, 2018.

[21] NIST. National vulnerability database[EB/OL]. https://nvd.nist.gov/, 2018.

[22] CVSS v3.0: specification document[EB/OL].

杨英杰：男，1971年生，教授,研究方向为信息安全.
冷　强：男，1993年生，硕士生，研究方向为信息安全风险评估.
潘瑞萱：女，1995年生，硕士生，研究方向为SDN网络协议安全.
胡　浩：男，1989年生，讲师，研究方向为网络安全态势感知和图像秘密共享.