# 基于属性攻击图的网络动态威胁分析技术研究

杨英杰 冷 强* 常德显 潘瑞萱 胡 浩

(信息工程大学 郑州 450001)

**摘 要**：该文首先利用属性攻击图理论构建了网络动态威胁分析属性攻击图(DT-AAG)模型，该模型在全面刻画系统漏洞和网络服务导致的威胁转移关系的基础上，结合通用漏洞评分标准(CVSS)和贝叶斯概率转移计算方法设计了威胁转移概率度量算法；其次基于构建的DT-AAG模型，利用威胁与漏洞、服务间的关联关系，设计了动态威胁属性攻击图生成算法(DT-AAG-A)，并针对生成的属性攻击图存在的威胁传递环路问题，设计了环路消解机制；最后通过实验验证了该模型和算法的有效性。

**关键词**：属性攻击图；威胁转移；通用漏洞评分标准；传递环路

**中图分类号**：TP393 **文献标识码**：A **文章编号**：1009-5896(2019)08-1838-09

**DOI**: 10.11999/JEIT181025

# Research on Network Dynamic Threat Analysis Technology Based on Attribute Attack Graph

YANG Yingjie LENG Qiang CHANG Dexian PAN Ruixuan HU Hao

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

**Abstract**: Firstly, a network Dynamic Threat Attribute Attack Graph (DT-AAG) analysis model is constructed by using Attribute Attack Graph theory. On the basis of the comprehensive description of system vulnerability and network service-induced threat transfer relationship, a threat transfer probability measurement algorithm is designed in combination with Common Vulerability Scoring System (CVSS) vulnerability evaluation criteria and Bayesian probability transfer method. Secondly, based on the model, a Dynamic Threat Attribute Attack Graph generation Algorithm (DT-AAG-A) is designed by using the relationship between the threat and the vulnerability as well as the service. What's more, to solve the problem that threat transfer loop existing in the generated attribute attack graph, the loop digestion mechanism is designed. Finally, the effectiveness of the proposed model and algorithm is verified by experiments.

**Key words**: Attribute Attack Graph (AAG); Threat to transfer; Common Vulerability Scoring System (CVSS) scoring standard; Transfer loop

## 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。目前，在利用攻击图进行威胁动态分析方面人们已开展了大量的研究工作。文献[1,2]首次提出攻击图概念，并应用于网络威胁分析；文献[3–15]分别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；2017年叶子维[16]等人深入分析了攻击图在网络威胁中的应用模式，并总结了攻击图在网络威胁分析中的优势和存在的问题。由此可见，攻击图是开展网络威胁动态分析广泛采用的重要方法。

根据构建方式攻击图可分为状态攻击图和属性攻击图，其中由于状态攻击图存在状态空间爆炸问题，因此近年来通常采用属性攻击图进行威胁风险分析研究。属性攻击图[8–11,16]将网络中的安全要素作为独立的属性节点，每个主机上的同一漏洞仅对应图中的一个属性节点，有向边表示节点间的关联关系。在属性攻击图模型构建中，节点间威胁转移概率的度量是建模要解决的重要问题之一。

收稿日期：2018-11-07；改回日期：2019-03-25；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(2015AA016006)，国家重点研发计划课题(2016YFF0204003)，国家自然科学基金(61471344)

Foundation Items: The National 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)

目前在威胁转移概率度量方法研究中，主要是根据网络节点漏洞的时间、重要性、环境等因素量化分析威胁转移概率，例如文献[12]提出了基于攻击者攻击能力增长的网络安全分析模型，给出攻击路径，并结合威胁转移概率分析了网络的安全性。文献[13]通过改进通用漏洞评分标准(Common Vulerability Scoring System, CVSS)，增加了攻击频率对网络风险值的影响，得到攻击频率越高，漏洞风险值越大的研究结果。文献[14]研究了漏洞的生命周期，并且提出基于马尔科夫链给出漏洞生命周期的计算方法，得到漏洞在不同的生命周期具有不同风险值的结论。虽然在属性攻击图模型构建方面人们已取得了很大成果，但是仍然存在一些不足，例如现有属性攻击图模型在威胁转移关系刻画方面，只能描述系统漏洞导致的威胁转移，对于网络业务应用之间存取访问关系导致的威胁转移并未刻画，从而在威胁转移概率度量方面也存在一定偏差。

属性攻击图模型的构建为威胁分析提供了理论基础，然而针对具体网络实施威胁分析时，还须结合现实网络环境生成攻击图模式库。目前提出的攻击图模式生成算法生成的攻击图普遍存在威胁传递环路问题，其在威胁分析中会产生干扰。针对该问题，文献[15]通过限制攻击图中的路径长度来解决威胁传递环路问题，但是其只能针对单一网络节点内存在的环路进行消解。

基于上述分析，本文在研究网络攻击行为与系统漏洞、网络服务之间相互影响关系的基础上，首先基于属性攻击图理论构建了网络动态威胁风险分析模型；其次结合CVSS评分标准和贝叶斯概率转移计算方法设计了威胁转移概率度量算法；然后针对攻击图模式中存在的多节点间威胁传递环路问题，依据权限递增原则提出了威胁传递环路消解方法；最后通过实验对所提出的模型和算法进行了有效性验证。

## 2　网络动态威胁分析模型

### 2.1　属性攻击图模型定义

攻击行为建模是实施网络动态威胁分析的理论基础。为避免状态爆炸问题，本文在动态威胁分析模型构建中将采用属性攻击图理论。目前提出的属性攻击图威胁分析模型仅考虑了系统漏洞引起的威胁转移，但是现实中网络节点间的业务应用存取访问关系同样会造成威胁的转移，因此在动态威胁分析模型构建时融入存取访问关系导致的威胁转移的刻画，具体模型定义如下：

**定义 1**　动态威胁属性攻击图(Dynamic Threat Attribute Attack Graph, DT-AAG)模型可描述为一个4元组：

$$\text{DT-AAG} = (C, R, E, p) \tag{1}$$

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。

(1) 威胁转移条件属性集$C$

$$C = C_{\text{Pro}} \cup C_{\text{Post}} \tag{2}$$

其中

$$C_{\text{Pro}} = (\text{ID}, \text{IP}_{\text{Pro}}, \text{IP}_{\text{Post}}, \text{Port}, \text{Vul}, \text{Pr}) \tag{3}$$

ID表示前置条件中攻击者的权限，且$\text{ID} \in [0,1]$。当ID=0时表示攻击者不具有该节点任何权限，当$\text{ID} \in (0,1)$时表示攻击者具有该节点部分权限，当ID=1时表示攻击者具有该节点全部权限；$\text{IP}_{\text{Pro}}$表示攻击的源IP; $\text{IP}_{\text{Post}}$表示攻击的目标IP; Port表示节点间连接的端口；Vul表示实施攻击的漏洞；Pr表示能够提升攻击者权限的服务访问关系，服务访问关系具体体现为协议。

$$C_{\text{Post}} = \left(\text{ID}', \text{IP}', \text{Port}', \text{Vul}', \text{Pr}'\right) \tag{4}$$

$\text{ID}'$表示攻击者实施攻击后获得的权限；$\text{IP}'$表示获得权限节点的IP地址；$\text{Port}'$表示攻击利用的端口；$\text{Vul}'$表示实施攻击的漏洞；$\text{Pr}'$表示可提升权限的协议。

(2) 威胁转移条件属性间的关系集$R$

$R = \{r_{\text{Vul}}, r_{\text{Pr}}\}$是通过系统漏洞或协议关联主机或服务的关系节点集，其中$r_{\text{Vul}} = (\text{IP}_{\text{Pro}}, \text{IP}_{\text{Post}}, \text{Vul}, 0)$和$r_{\text{Pr}} = (\text{IP}_{\text{Pro}}, \text{IP}_{\text{Post}}, 0, \text{Pr})$分别表示漏洞节点和协议节点。

(3) 连接条件属性和关系的边集$E$

$$\begin{aligned} E &= \{C_{\text{Pro}} \cdot R\} \cup \{R \cdot C_{\text{Post}}\} \\ &= \{C_{\text{Pro}} \cdot r_{\text{Vul}}\} \cup \{r_{\text{Vul}} \cdot C_{\text{Post}}\} \\ &\quad \cup \{C_{\text{Pro}} \cdot r_{\text{Pr}}\} \cup \{r_{\text{Pr}} \cdot C_{\text{Post}}\} \end{aligned} \tag{5}$$

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

(4) 威胁转移概率$p$

威胁转移概率$p$是指攻击者利用系统漏洞或服务访问关系提升权限达到的威胁转移成功率，其进一步可划分为单步威胁转移概率和综合威胁转移概率，单步威胁转移概率是指攻击者根据$C_{\text{Pro}}$利用系统漏洞Vul或服务访问关系Pr实施单次威胁转移的成功率；综合威胁转移概率是指包含多步威胁转移序列造成的威胁转移的成功率。

图1给出了一个典型的DT-AAG攻击图事例，椭圆表示属性攻击图中的条件属性，矩形表示威胁转移的关系。攻击者具有网络节点119.188.162.1的

$c_{\text{Pro1}}$和$c_{\text{Pro2}}$，网络节点119.188.162.1与网络节点119.188.162.2通过端口80进行连接，攻击者通过攻击网络节点119.188.162.2的SSH漏洞，获得网络节点119.188.162.2的$c_{\text{Post1}}$。然后攻击者利用网络节点119.188.162.2与网络节点119.188.162.3的ftp协议，获得网络节点119.188.162.3的$c_{\text{Post2}}$。其中虚线框内表示同一个节点的相同权限，且攻击者前一步获得的$c_{\text{Post1}}$变为下一步攻击的$c_{\text{Pro3}}$。

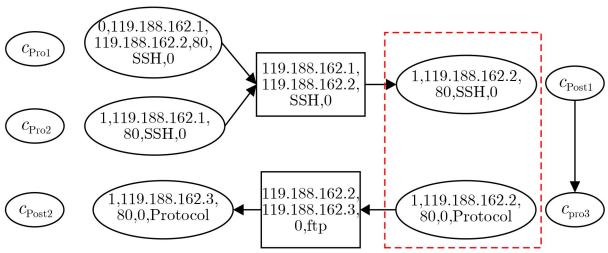


图 1 DT-AAG攻击示意图

### 2.2 威胁转移概率$p$度量方法

威胁转移概率的量化是动态威胁分析模型构建需要解决的关键问题之一。由2.1节可知，威胁转移概率可划分为单步威胁转移概率和多步威胁转移概率。由于网络服务存取关系带来的威胁转移没有攻击权限约束条件，因此本文在单步转移概率度量中默认服务访问关系引起的转移概率值为100%。

(1) 单步威胁转移概率度量

在单步威胁转移概率度量方面，本文采纳了CVSS[17]评分标准中给出的漏洞可利用性得分ExpSco和漏洞威胁影响得分ImpSco进行威胁转移概率的量化方法。

$$\text{ExpSco} = 20 \cdot \text{AV} \cdot \text{AC} \cdot \text{AU} \tag{6}$$

$$\text{ImpSco} = 10.41 \cdot (1 - (1 - \text{C}) \cdot (1 - \text{I}) \cdot (1 - \text{A})) \tag{7}$$

其中，AV表示攻击路径，AC表示攻击复杂度，AU表示身份认证，C表示机密性，I表示完整性，A表示可用性。根据CVE[18]和NVD[19]数据库可查询到CVSS评分标准中需要的漏洞等级评分。

漏洞风险等级Risklevel的计算方法见式(8)，其取值范围为$[0, 10]$[17]。漏洞的攻击成功概率$p$与Risklevel的函数关系见式(9)。

$$\text{Risklevel} = \text{ExpSco} + \text{ImpSco} \tag{8}$$

$$p = \lambda \cdot \text{Risklevel} \tag{9}$$

其中，$\lambda$为漏洞攻击成功概率系数，取值为0.1，以保证漏洞攻击成功概率$p$的取值范围控制在$[0, 1]$。

(2) 综合威胁转移概率度量

因为前后攻击行为成功概率间不存在明确的关联性，所以可利用贝叶斯概率转移计算方法进行综合威胁转移概率的度量。当攻击者攻击网络系统中的漏洞$k$时，且攻击漏洞$k$需要依次攻击$r^1_{\text{Vul}}, r^2_{\text{Vul}}, \cdots, r^i_{\text{Vu}}$漏洞和利用$r^{i+1}_{\text{Pr}}, r^{i+2}_{\text{Pr}}, \cdots, r^{k-1}_{\text{Pr}}$存取访问关系获得相应的权限，则漏洞$k$的多步威胁转移概率计算公式为

$$P_k = p_k \cdot \prod_{h=1}^{i} p_h \prod_{j=i+1}^{k-1} p_j = p_k \cdot \prod_{h=1}^{i} p_h \tag{10}$$

其中，$P_k$表示在多步攻击中，漏洞$k$被攻击成功概率，$p_k$表示漏洞$k$的单个漏洞被攻击成功概率，$p_1, p_2, \cdots, p_{k-1}$表示漏洞$r^1_{\text{Vul}}, r^2_{\text{Vul}}, \cdots, r^i_{\text{Vu}}$被攻击成功概率和协议$r^{i+1}_{\text{Pr}}, r^{i+2}_{\text{Pr}}, \cdots, r^{k-1}_{\text{Pr}}$的威胁转移概率，如图2所示。由于协议的威胁转移概率为100%，因此可将公式表示为

$$P_k = p_k \cdot \prod_{h=1}^{i} p_h \tag{11}$$

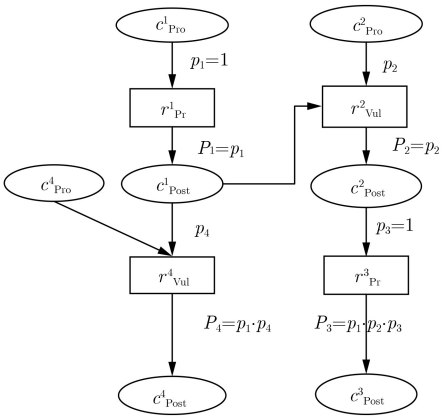


图 2 多步攻击威胁转移概率图

## 3 基于DT-AAG的攻击图生成方法

在攻击图生成方法研究方面，首先需要给出动态威胁属性攻击图模式(DT-AAG Pattern，DT_AAG_P)的表示方法。根据定义1可给出前置条件和后置条件的关联关系判定条件为

$$\left.\begin{aligned} \exists c^i_{\text{Pro}} &= \left(\text{ID}^i, \text{IP}^i_{\text{Pro}}, \text{IP}^i_{\text{Post}}, \text{Port}^i, \text{Vul}^i, \text{Pr}^i\right) \\ c^j_{\text{Post}} &= \left(\text{ID}^j, \text{IP}^j, \text{Port}^j, \text{Vul}^j, \text{Pr}^j\right) \end{aligned}\right\} \tag{12}$$

当$\text{ID}^i = 0$，$\text{ID}^j \in (0, 1]$，$\text{IP}^i_{\text{Post}} = \text{IP}^j$，$\text{Port}^i = \text{Port}^j$，$\text{Vul}^i = \text{Vul}^j$，$\text{Pr}^i = \text{Pr}^j$，则$c^j_{\text{Post}}$为$c^i_{\text{Pro}}$的后置条件。

根据推理结合网络系统中漏洞和协议信息给出相应的前置条件和后置条件，然后连接漏洞、协议与条件，生成属性攻击图模式(DT-AAG-P)。

图3表示的攻击图模式在属性攻击图模式库

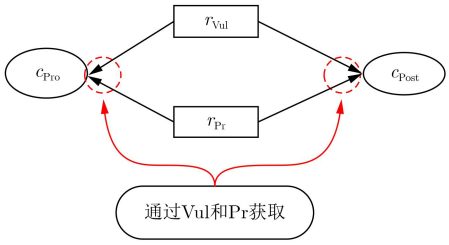


图 3 模式构建图

(DT-AAG-P Library, DT-AAG-PL)中的格式可表示为$C^i_{\text{Pro}} \rightarrow R \rightarrow C^j_{\text{Post}}$。

在实际攻击中攻击者的权限变化通常遵循不断提升的规律，即整个攻击过程中符合权限增长原则。本文依据权限增长原则设计了一种具有威胁传递环路消解能力的DT-AAG生成算法。下面首先给出网络节点权限定义。

**定义 2**　$W_{\text{IP}^i}$表示攻击者攻击到网络节点$\text{IP}^i$时具有的权限。当$\exists W_{\text{IP}^i} < W_{\text{IP}^j}$时，表示攻击者攻击到网络节点$\text{IP}^i$时具有的权限小于攻击到网络节点$\text{IP}^j$的权限。

下面根据网络节点间权限排序和网络节点中权限排序给出消解环路[15]的方法。

(1) 网络节点间权限排序环路消解方法：在扫描系统中配置信息时，获得系统中节点的权限排序，得到$W_{\text{IP}^1} > W_{\text{IP}^2} > \cdots > W_{\text{IP}^n}$。当$W_{\text{IP}^i} > W_{\text{IP}^j}$，攻击者通过$c^i_{\text{Pro}} = (\text{ID}^i, \text{IP}^i, \text{IP}^j, \text{Port}^i, \text{Vul}^i, \text{Pr}^i)$攻击漏洞$\text{Vul}^i$或者利用协议$\text{Pr}^i$获得$\text{IP}^j$的权限时，则是从高权限网络节点到低权限网络节点的攻击过程，因此，不存在该攻击行为；

(2) 网络节点内权限排序环路消解方法：当攻击者利用前置条件$c^i_{\text{Pro}} = (\text{ID}^i, \text{IP}^i_{\text{Pro}}, \text{IP}^i_{\text{Post}}, \text{Port}^i, \text{Vul}^i, \text{Pr}^i)$通过攻击某个网络节点中的$\text{Vul}^i$或者利用$\text{Pr}^i$获得后置条件$c^j_{\text{Post}} = (\text{ID}^j, \text{IP}^j, \text{Port}^j, \text{Vul}^j, \text{Pr}^j)$时，且$\text{ID}^i > \text{ID}^j$，则不存在该攻击行为。

利用系统中网络节点的信息，结合DT-AAG-PL中元素的后置条件和前置条件，得到系统DT-AAG。下面给出(DT-AAG Algorithm) DT-AAG-A生成算法，如表1所示。

上述算法结合模式库中元素信息，形成系统的动态威胁属性攻击图。图4是DT-AAG-A中DT-AAG-PL元素结合的两步过程图。

图4(a)中$c^i_{\text{Pro}} \rightarrow r^1_{\text{Vul}} \rightarrow c^j_{\text{Post}}$与$c^j_{\text{Pro}} \rightarrow r^2_{\text{Vul}} \rightarrow c^m_{\text{Post}}$的$c^j_{\text{Pro}}$与$c^j_{\text{Post}}$具有相同的ID，且$\text{IP}^j = \text{IP}^j_{\text{Post}}$，过程为从图4(a)到图4(b)；然后将图4(b)放入DT-AAG中，再从DT-AAG-PL中任取一个元素，如图4(c)，当$c^m_{\text{Pro}}$与$c^m_{\text{Post}}$中具有相同的ID，且$\text{IP}^m = \text{IP}^m_{\text{Post}}$，合并图4(c)与图4(b)得到图4(d)；

**表 1　DT-AAG-A生成算法**

**输入**：DT-AAG-PL
**输出**：DT-AAG
(1) DT-AAG-PL$\neq \varnothing$; /* DT-AAG-PL数据库不为空 */
(2) DT-AAG=$\varnothing$; /* 设置DT-AAG初始值为空 */
(3) $t, i \in$DT-AAG-PL
(4) For each $t = [\text{ID}_t, \text{IPpreCon}_t, \text{IPpostCon}_t]$
(5) DO { /* 任取DT-AAG-PL中一个元素 */
(6) SearchIDIPpre (DT-AAG-PL) }
(7) For rest $j \in$DT-AAG-PL DO {
/* 搜索匹配DT-AAG-PL中剩余元素*/
(8) SearchIDIPpre (DT-AAG-PL, DT－AAG);
/* 范围为DT-AAG-PL 和DT－AAG */ }
(9)　If DT-AAG-PL= $\varnothing${
/* 当DT-AAG-PL中所有元素都被移动 */
(10) Return DT-AAG;　}
(11) SearchIDIPpre (DT-AAG-PL) {
(12)　If $\text{ID}_t = \text{ID}_i$&&$\text{IPpostCon}_t = \text{IPpostCon}_i$;
/* 根据ID和IP搜索匹配 */
(13)　　{$a = t \rightarrow i$; Put $a$ to DT－AAG;　}
/* 将匹配到的元素移到DT－AAG */
(14)　else
(15)　　{$a = t$; Put $a$ to DT－AAG;　}
/* 将未匹配的元素移到DT－AAG中 */ }

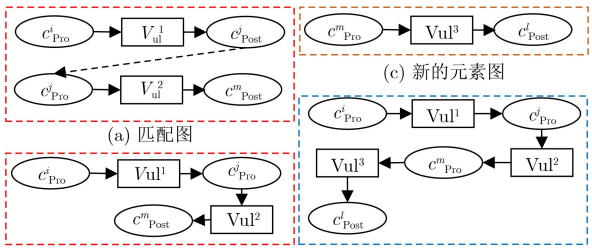


图 4 DT-AAG-A过程图

然后将图4(d)存入DT-AAG中；依次遍历DT-AAG-PL中的所有元素，最后得到DT-AAG。

## 4　实验

### 4.1　DT-AAG实验

为了确定DT－AAG威胁转移概率和验证环路消解算法的有效性，在一个经典的网络环境中开展实验，实验环境如图5所示。

攻击者的初始权限是user1。user2, user3和user4是系统中的普通用户，能够通过端口连接系统中的服务器，具体协议访问信息和相关漏洞信息如表2和表3。

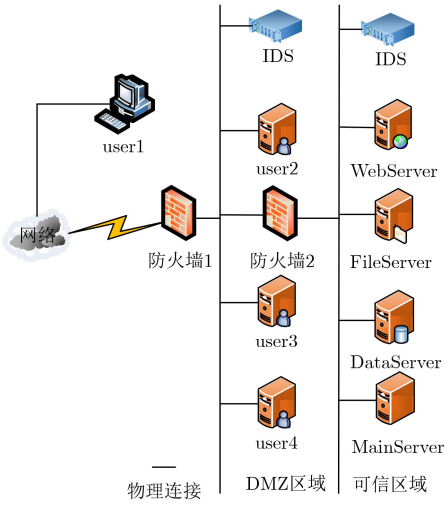


图 5 实验环境图

**表 2 主机与服务器存在的漏洞和协议信息表**

| Host/Server | Protocol/Vulnerability | Port |
|---|---|---|
| user1 | – | 80/445 |
| user2 | HIDP | 80 |
| user3 | GUN Wget | 80 |
| user4 | NDproxy | 445 |
| WebServer | IIS | 80 |
| FileServer | Protocol with user3/Apache | 80 |
| DataServer | Protocol with user4 | 445 |
| MainServer | Protocol with user2&user3&user4 | 80&445 |

**表 3 漏洞信息表**

| Vulnerability | ExpSco+ImpSco | CVE Num. |
|---|---|---|
| HIDP | 7.0 | CVE-2018-8169 |
| GUN Wget | 8.8 | CVE-2016-4971 |
| NDproxy | 7.2 | CVE-2013-5065 |
| IIS | 7.8 | CVE-2015-7597 |
| Apache | 7.5 | CVE-2018-8015 |

其中权限排序为：$W_{\text{user1}} < W_{\text{user2}} < W_{\text{user3}} < W_{\text{user4}} < W_{\text{WebServer}} < W_{\text{FileServer}} < W_{\text{DataServer}} < W_{\text{MainServer}}$。user1是攻击者使用的主机，在攻击过程中，权限值最低。

(1) 得到系统前置条件和后置条件

前置条件$C_{\text{Pro}}$：

(1,user1,user2,80,HIDP,0), (1,user1,user3,80,GUN Wget,0), (1,user1,user4,445,NDproxy,0), (0,user2,user3,80,GUN Wget,0), (0,user2,WebServer,80,IIS,0), (0,user2,FileServer,80,Apache,0), (0,user2,MainServer,80,0,Protocol), (0,user3,user2,80,HIDP,0), (0,user3,WebServer,80,IIS,0), (0,user3,FileServer,80,Apache,0), (0,user3,FileServer,80,0,Protocol), (0,user3,MainServer,80,0, Protocol), (0,user4,DataServer,445,0,Protocol), (0,user4,MainSer-ver, 445,0,Protocol)。

后置条件$C_{\text{Post}}$：

(1,user2,80,HIDP,0), (1,user3,80,GUN Wget,0), (1,user4,445,NDproxy,0), (1,WebServer,80,IIS,0), (1,FileServer,80,0,Protocol), (1,FileServer,80,Apache,0), (1,DataServer,445,0,Protocol), (1,MainServer,80,0,Protocol), (1,MainServer,445,0,Protocol)。

(2) 验证环路消解方法和分析协议路径

本文仅利用user2和user3解释权限增长原则对攻击图环路消解的效果，其余服务器之间的环路关系在生成攻击图之前已经删除相关节点。根据权限增长可知，$W_{\text{user2}} < W_{\text{user3}}$，(0,user3,user2,80,HIDP,0)为不可取前置条件。且条件(0,user3,FileServer,80,Apache,0)与(0,user3,FileServer,80,0,Protocol)在利用user3的用户身份攻击FileServer时，有两条攻击路径，一是通过攻击Apache漏洞获得FileServer权限，需要攻击漏洞；二是通过Protocol攻击FileServer时，攻击支出低。所以在攻击者具有user3的用户身份，攻击FileServer时，攻击者利用Protocol获得FileServer的权限的攻击行为发生的概率更大，但是在DT – AAG生成时，还是存在利用Apache漏洞获得FileServer权限的路径。该实验没有存在攻击者攻击某个漏洞获得的权限使得ID $\in (0,1)$的情况，因此实验没有分析节点内的环路。其中(1,FileServer,80,0,Protocol) = (1,FileServer,80, Apache,0)，因为两个后置条件获取的权限相同，只是获取的方式不同。

(3) 动态威胁属性攻击图模式库

(a) (1,user1,user2,80,HIDP,0)→(user1,user2,HIDP,0)→(1,user2,80,HIDP,0),

(b) (1,user1,user3,80,GUN Wget,0)→(user1,user3,GUN Wget,0)→(1,user3,80,GUN Wget,0),

(c) (1,user1,user4,445,NDproxy,0)→(user1,user4,NDproxy,0)→(1,user4,445,NDproxy,0),

(d) (0,user2,user3,80,GUN Wget,0)⊕(1,user2,80,HIDP,0)→(user2,user3,GUN Wget,0)→(1,user3,80,GUN Wget,0),

(e) (0,user2,WebServer,80,IIS,0)⊕(1,user2,80,HIDP,0)→(user2,WebServer,IIS,0)→(1,WebServer,80,IIS,0),

(f) (0,user2,FileServer,80,Apache,0)⊕(1,user2,

80,HIDP,0)→(user2,FileServer,Apache,0)→(1,FileServer,80,Apache,0),

(g) (0,user2,MainServer,80,0,Protocol)⊕(1,user2,80,HIDP,0)→(user2,MainServer,0,Protocol)→(1,MainServer,80,0,Protocol),

(h) (0,user3,user2,80,HIDP,0)⊕(1,user3,80,GUN Wget,0)→(user3,user2,HIDP,0)→(1,user2,80,HIDP,0),

(i) (0,user3,WebServer,80,IIS,0)⊕(1,user3,80,GUN Wget,0)→(user3,WebServer,IIS,0)→(1,WebServer,80,IIS,0),

(j) (0,user3,FileServer,80,Apache,0)⊕(1,user3,80,GUN Wget,0)→(user3,FileServer,Apache,0)→(1,FileServer,80,Apache,0),

(k) (0,user3,FileServer,80,0,Protocol)⊕(1,user3,80,GUN Wget,0)→(user3,FileServer,0,Protocol)→(1,FileServer,80,0,Protocol),

(l) (0,user3,MainServer,80,0,Protocol)⊕(1,user3,80,GUN Wget,0)→(user3,MainServer,0,Protocol)→(1,MainServer,80,0,Protocol),

(m) (0,user4,DataServer,445,0,Protocol)⊕(1,user4,445,NDproxy,0)→(user4,DataServer,0,Protocol)→(1,DataServer,445,0,Protocol),

(n) (0,user4,MainServer,445,0,Protocol)⊕(1,user4,445,NDproxy,0)→(user4,MainServer,0,Protocol)→(1,MainServer,445,0,Protocol)。

⊕表示需要两个条件同时满足；→表示条件与关联关系的连接。根据DT-AAG-PL中的元素信息，利用DT-AAG-A，得到DT-AAG如图6。

(4) 实验结果分析

图6中红色虚线指向的是同一个前置条件或后置条件。蓝色方框中表示攻击者在获得user2的主机权限攻击user3的模式库元素和攻击者获得user3的主机权限攻击user2的模式库元素，显然该DT-AAG存在环路，因此删掉DT-AAG-PL中不符合权限增长原则的元素$h$，实现消解DT-AAG中的环路的目的。

去掉元素$h$后，得到DT-AAG中每条攻击路径和威胁转移概率为表4所示。

首先根据表3中漏洞信息和式(8)、式(9)计算得到攻击单个漏洞的威胁转移概率；然后根据图6中攻击路径和式(10)计算每条路径的攻击成功概率；最后得到表4的转移概率。

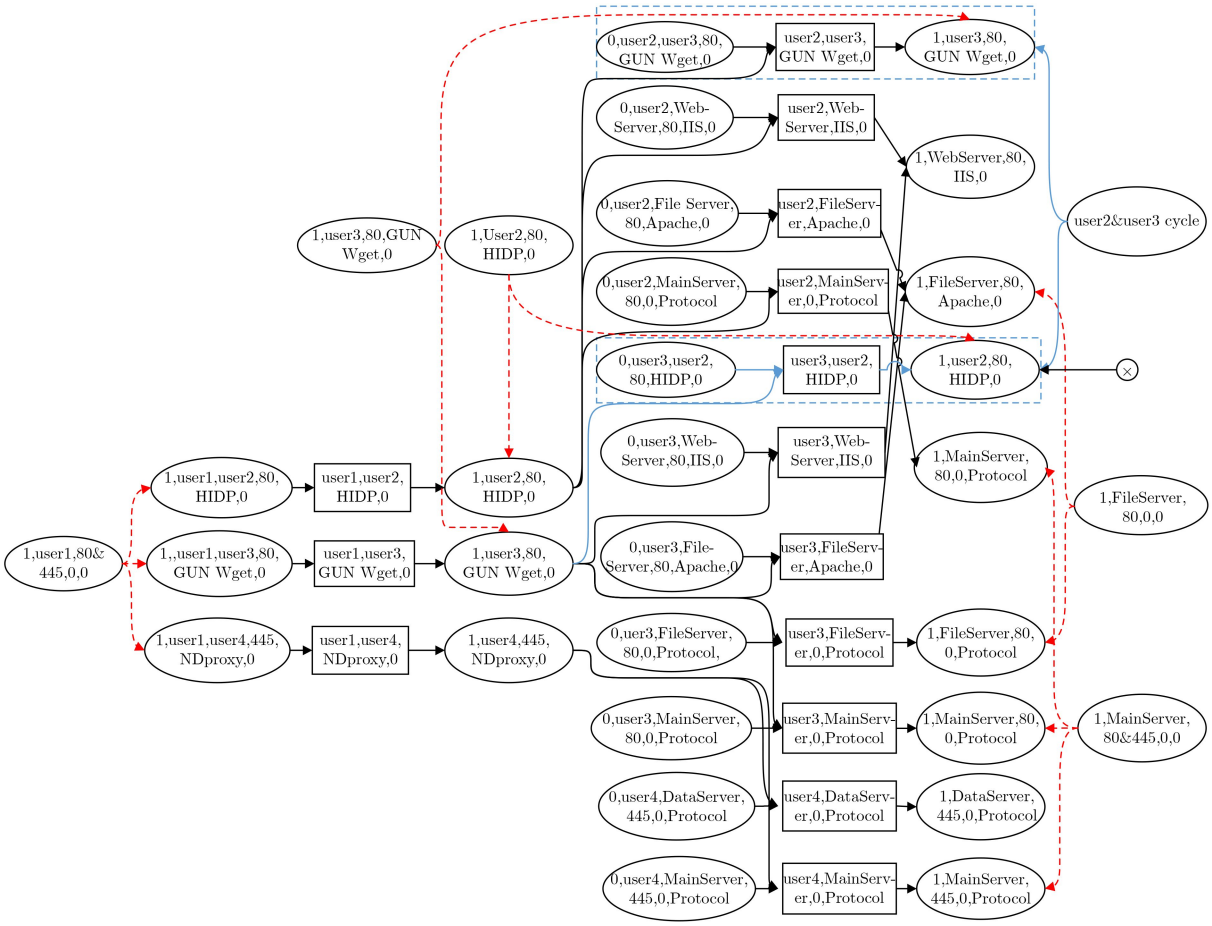


图 6 DT-AAG生成图

**表 4 攻击路径和威胁转移概率表**

| 攻击路径 | $a\rightarrow d\rightarrow i$ | $a\rightarrow d\rightarrow j$ | $a\rightarrow d\rightarrow k$ | $a\rightarrow d\rightarrow l$ | $a\rightarrow e$ | $a\rightarrow f$ | $a\rightarrow g$ | $b\rightarrow j$ | $b\rightarrow k$ | $b\rightarrow l$ | $c\rightarrow m$ | $c\rightarrow n$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 转移概率 | 0.38 | 0.30 | 0.49 | 0.49 | 0.44 | 0.34 | 0.56 | 0.53 | 0.88 | 0.88 | 0.58 | 0.58 |

由表4可知，路径$b\rightarrow k$和$b\rightarrow l$的威胁转移概率最大，原因是user3与FileServer, MainServer具有相关的数据存取访问关系Pr，且user3的漏洞风险值大，因此，为了降低系统服务器的风险，需要修复user3的漏洞，或者修改user3与FileServer, MainServer之间的存取访问关系。

### 4.2 关联分析

为了对比分析本文和文献[8]利用属性攻击图对系统安全状况描述的准确性，下面结合实验和文献[8]属性攻击图构建方法给出文献[8]的属性攻击图，并且分析攻击图中的路径和威胁转移概率。

图7是本文利用文献[8]方法根据实验数据生成的属性攻击图，为了方便阅读者更好地理解本文和文献[8]生成攻击图之间的区别，在图7中属性节点使用的是本文的节点表述方法。由于文献[8]没有考虑网络节点间的业务访问关系Pr，因此，图7缺失了许多关于Pr的攻击路径，如不能分析DataServer和MainServer的安全状况；另外，由于文献[8]虽然考虑了权限增长原则，但是没有应用在攻击图环路消解中，因此存在如图7中的红色箭头的攻击转移路径的环路。

文献[8]和文献[9]与本文研究内容在研究攻击路径、攻击成功概率、是否全局攻击路径、是否消解了攻击图中的环路、攻击者权限增长和系统业务关系对系统攻击图的影响等方面的比较如表5所示。

本文在已有的研究基础上，加入了网络系统中的业务应用关联关系，分析研究其对攻击者攻击路径和攻击成功概率的影响；并且在生成的攻击图

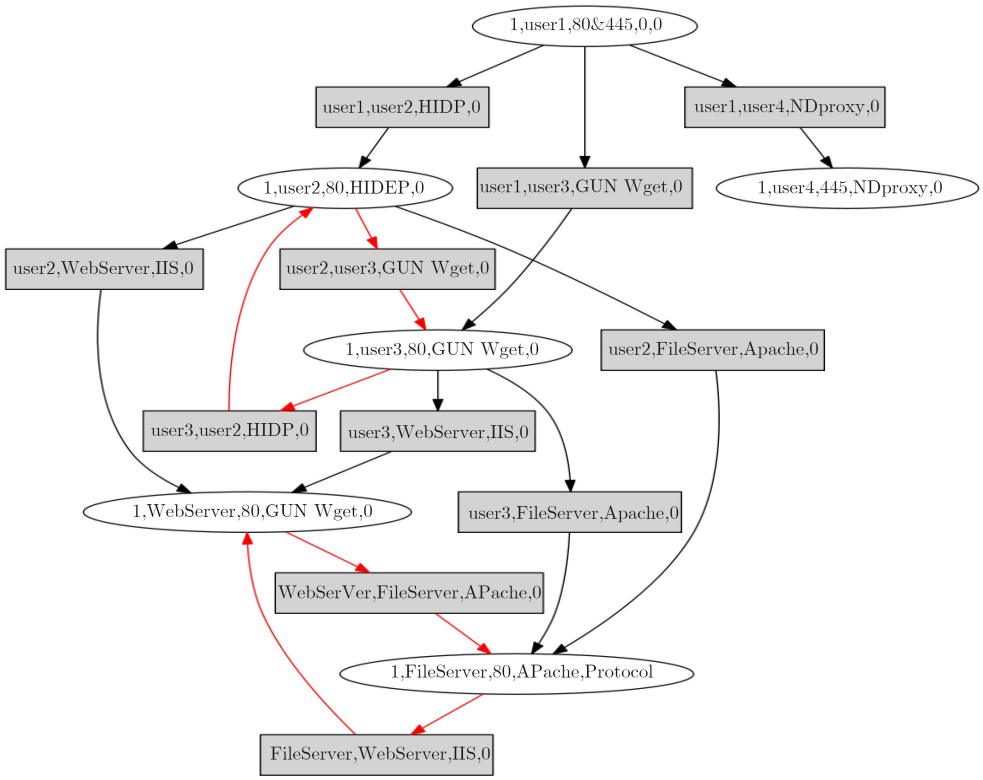


图 7 文献[8]实验图

**表 5 关联分析表**

| | 攻击路径 | 攻击成功概率 | 全攻击路径 | 消解环路 | 权限 | 系统业务关系 |
|---|---|---|---|---|---|---|
| 文献[8] | √ | √ | × | √ | √ | × |
| 文献[9] | √ | √ | √ | × | × | × |
| 本文 | √ | √ | √ | √ | √ | √ |

中，利用攻击者权限增长原则，在没有减少攻击路径数的前提下，实现不需要限制攻击步骤来消解攻击图中环路的目的。

## 5　结束语

本文首先利用属性攻击图理论构建了动态威胁属性攻击图模型，相对现有模型仅能描述漏洞引起的威胁转移关系，本文模型能够同时刻画系统漏洞和网络服务导致的威胁转移关系，并针对模型中的转移概率度量问题，给出了单步威胁转移概率和综合威胁转移概率的度量算法；其次设计了动态威胁属性攻击图生成算法，在不限制攻击路径长度的条件下解决了攻击图的威胁传递环路问题。要想本文研究成果在网络动态威胁分析中得到应用，下一步还需要结合网络报警信息，基于生成的攻击图模式库开展网络攻击行为实时跟踪与分析技术的研究。

## 参 考 文 献


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

[2] SWILER L P, PHILLIPS C, ELLIS D, *et al*. Computer-attack graph generation tool[C]. DARPA Information Survivability Conference and Exposition II, DISCEX'01, Anaheim, CA, USA, 2001, 2: 307–321. doi: 10.1109/DISCEX.2001.932182.

[3] INGOLS K, CHU M, LIPPMANN R, *et al*. Modeling modern network attacks and countermeasures using attack graphs[C]. 2009 Annual Computer Security Applications Conference, Honolulu, Hawaii, USA, 2009: 117–126. doi: 10.1109/ACSAC.2009.21.

[4] 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.

[5] LEE J, MOON D, KIM I, *et al*. A semantic approach to improving machine readability of a large-scale attack graph[J]. *The Journal of Supercomputing*, 2018: 1–18. doi: 10.1007/s11227-018-2394-6.

[6] 胡浩, 刘玉岭, 张红旗, 等. 基于吸收Markov链的网络入侵路径预测方法[J]. 计算机研究与发展, 2018, 55(4): 831–845. doi: 10.7544/issn1000-1239.2018.20170087.
HU Hao, LIU Yuling, ZHANG Hongqi, *et al*. Route prediction method for network intrusion using absorbing markov Chain[J]. *Journal of Computer Research and Development*, 2018, 55(4): 831–845. doi: 10.7544/issn1000-1239.2018.20170087.

[7] HU Hao, LIU Yuling, 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: 57871012. doi: 10.1155/2018/5787102.

[8] 吴迪, 连一峰, 陈恺, 等. 一种基于攻击图的安全威胁识别和分析方法[J]. 计算机学报, 2012, 35(9): 1938–1950. doi: 10.3724/SP.J.1016.2012.01938.
WU Di, LIAN Yifeng, CHEN Kai, *et al*. A security threats identification and analysis method based on attack graph[J]. *Chinese Journal of Computers*, 2012, 35(9): 1938–1950. doi: 10.3724/SP.J.1016.2012.01938.

[9] HOMER J, ZHANG Su, OU Xinming, *et al*. Aggregating vulnerability metrics in enterprise networks using attack graphs[J]. *Journal of Computer Security*, 2013, 21(4): 561–597. doi: 10.3233/JCS-130475.

[10] 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.

[11] 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.

[12] 张海霞, 苏璞睿, 冯登国. 基于攻击能力增长的网络安全分析模型[J]. 计算机研究与发展, 2007, 44(12): 2012–2019.
ZHANG Haixia, SU Purui, and FENG Dengguo. A network security analysis model based on the increase in attack ability[J]. *Journal of Computer Research and Development*, 2007, 44(12): 2012–2019.

[13] SINGH U K, JOSHI C, and GAUD N. Information security assessment by quantifying risk level of network vulnerabilities[J]. *International Journal of Computer Applications*, 2016, 156(2): 37–44. doi: 10.5120/ijca2016912375.

[14] 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.

[15] 陈锋, 张怡, 苏金树, 等. 攻击图的两种形式化分析[J]. 软件学报, 2010, 21(4): 838–848. doi: 10.3724/SP.J.1001.2010.03584.
CHEN Feng, ZHANG Yi, SU Jinshu, *et al*. Two formal analyses of attack graphs[J]. *Journal of Software*, 2010, 21(4): 838–848. doi: 10.3724/SP.J.1001.2010.03584.

[16] 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.

[17] CVSS v3.0 specification document[EB/OL]. https://www.first.org/cvss/specification-document, 2018.

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

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

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 .

常德显：男，1977年生，副教授，研究方向为信息安全.

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.