用双枝模糊逻辑和模糊 Petri 网构建的攻击模型

黄光球,赵阿妮,任大勇
HUANG Guang-qiu,ZHAO A-ni,REN Da-yong

西安建筑科技大学 管理学院,西安 710055
School of Management,Xi'an University of Architecture and Technology,Xi'an 710055,China
E-mail:huangnan93@sohu.com

HUANG Guang-qiu,ZHAO A-ni,REN Da-yong.Attack model based on both-branch fuzzy logic and fuzzy Petri net. Computer Engineering and Applications,2010,46(2):99-103.

Abstract: Based on both-branch fuzzy logic and Fuzzy Petri Net(FPN),a new network attack model named Both-Branch Fuzzy Logic Petri-net Attack Net(BBFLPAN) is put forward.The promoting and suppressive factors to network attack are analyzed in this attack model.In order to make fine distinction between attack actions and effects,the process of attack and defense actions are depicted as the place of FPN and the system states are depicted as the transition.The changes of network attack states can be represented directly.Based on the both-branch fuzzy logic analysis,a reasoning algorithm is proposed which applies incertitude consequence way and the effectiveness of the algorithm is verified by experiment.This paper originally considers together the factors pro-and-con that has effect on attack so that a closer network attack description to reality is made by this model.
Key words: fuzzy Petri net;both-branch fuzzy logic;attack modeling

摘 要:以双枝模糊逻辑和模糊 Petri 网(Fuzzy Petri net,FPN)理论为基础,定义了一种全新的网络攻击模型 BBFLPAN,将网络攻击中对攻击起促进与抑制作用的两方面进行综合考虑与分析,用变迁表示攻击、防御行为的产生发展过程,库所表示系统所处的状态,将网络攻击与防御行为和攻击与防御结果进行了区分,直观地表示网络攻击的演变情况。同时结合双枝模糊逻辑,分析了 BBFLPAN 模型的基本推理规则,并提出了 BBFLPAN 的推理算法,并通过实验验证了算法的正确性。将对网络攻击实施起正反两方面的因素一起考虑和分析,使其对网络攻击的描述更加切近实际情况。
关键词:模糊 Petri 网;双枝模糊逻辑;攻击建模
DOI:10.3778/j.issn.1002-8331.2010.02.031 **文章编号**:1002-8331(2010)02-0099-05 **文献标识码**:A **中图分类号**:TP393.08

1 引言

随着网络攻击技术和安全防御技术的不断发展,攻击和防御已经成为网络安全的两个密切相关的侧面,不深入研究攻击理论和技术就不能做到知己知彼,也就无法有效地保护网络信息系统的安全。网络攻击研究的一个关键问题是对攻击的认识和描述。而攻击过程采用不同的攻击行为组成,不同的攻击行为又有不同的阶段和状态。攻击模型能对整个攻击过程进行结构化和形象化的描述,有助于分析和充分利用已知的攻击行为研究成果,进一步提高攻击检测和安全预警的效率。目前常用的几种攻击模型基本上都处于理论研究阶段。根据主要功能的不同可以将攻击模型分为两种,即适用于安全知识共享的模型和适用于攻击检测和安全预警的模型[1]。适用于知识共享的攻击模型主要有 Attack Tree[2-6]和 Attack Net[7-8]模型,适用于攻击检测和安全预警的攻击模型主要有基于系统状态集合的攻击模型[9]。

以往在对网络攻击进行描述和评估时,一般都只针对网络漏洞与弱点,利用攻击树和模糊 Petri 网技术,从网络攻击者的角度来进行攻击建模研究。其中,文献[4]针对 Phishing 攻击行为进行了分析介绍,并利用攻击树构建了攻击森林和 Phishing 攻击模型;文献[5]使用攻击树对分布式拒绝服务攻击进行建模,同时引入 Object_Z 语言对具体攻击模式进行了面向对象的形式化描述;文献[6]提出 BGP 的攻击树模型,并将该模型应用在域间路由系统的安全性测试中,有效地发现了 BGP 潜在的安全漏洞;文献[7]利用模糊 Petri 网实现了攻击知识的表达和入侵检测的推理模型,解决了误用入侵检测系统中现有知识表示方法不能并行推理的问题,以及传统的基于 Petri 网可达图搜索求解导致模型描述复杂、推理缺少智能的问题。

但是,以上研究从网络攻击者的角度出发,多是对攻击发生起积极作用的因素进行分析研究,而对攻击起抑制作用的因素很少涉及。攻击和防御已经成为网络安全的两个密切相关的侧面,单从攻击者的角度所构建的攻击模型,必不能直观地表示网络攻击的演变情况,从而也就无法提到很好的攻击检测和安全预警功能。已在文献[10]中,以双枝模糊决策理论[11-12]为基

基金项目:陕西省自然科学基金(the Natural Science Foundation of Shaanxi Province of China under Grant No.2007E217);陕西省教育厅专项基金项目(No.09JK524)。
作者简介:黄光球(1964-),男,教授,博导,博士,主要研究方向:网络安全、计算机仿真。
收稿日期:2008-07-24 **修回日期**:2008-10-15

础,综合考虑了对网络攻击起促进和抑制作用的两种因素,对此进行了初步的尝试。同时,也发现双枝模糊决策理论在逻辑推理上的不足,而由刘刚等人所提出双枝模糊逻辑理论[13-15],却能很好的适应模糊推理的要求。故而在该文中,将以双枝模糊逻辑理论为基础,对网络攻击模型再次进行深入研究。

在基于双枝模糊逻辑和模糊 Petri 网(Fuzzy Petri Net,FPN)的基础上,以对网络攻击既有促进作用、又有抑制作用的网络攻击为研究对象,提出了攻击模型 BBFLPAN(Both-Branch Fuzzy Logic Petri-net Attack Net),网络攻击中对攻击起积极促进,与消极抑制作用的两种因素进行综合考虑与分析。模型用变迁表示攻击、防御行为的产生发展过程,库所表示系统所处的状态,将网络攻击与防御行为和攻击与防御结果进行了区分,因而更加直观地表示网络攻击的演变情况,特别是对协同式网络攻击行为的描述。

2 攻击模型 BBFLPAN

2.1 BBFLPAN 的定义

文献[6]利用$|\theta_i^0|$表示命题 d_i 存在的真实程度,将命题 d_i 的属性和存在的真实程度进行了分离,在一定程度上简化模型的 Petri 网表示方法,但是却减弱了命题 d_i 表示的概念清晰性,同时也加剧了推理算法的复杂性,致使模型不能得到很好的安全预警功能,而依据双枝模糊逻辑理论所提出的攻击模型 BBFLPAN 却能解决以上问题。

BBFLPAN 定义为七元组:

BBFLPAN=$(P,T,D,\boldsymbol{I},\boldsymbol{O},F,\theta)$

其中,$P=\{p_1,p_2,\cdots,p_n\}$是一个库所的有限集合,其中的任一库所 p_i 表示攻击阶段;$T=\{t_1,t_2,\cdots,t_m\}$是一个变迁的有限集合,其中的任一变迁 t_j 表示攻击过程;$P\cap T=\varnothing$,$P\cup T\neq\varnothing$;$\boldsymbol{I}:P\to T$ 为输入矩阵,$\boldsymbol{I}=\{\delta_{ij}\}$,$\delta_{ij}$ 为逻辑量,$\delta_{ij}\in\{0,1\}$,当 p_i 是 t_j 的输入时,$\delta_{ij}=1$,当 p_i 不是 t_j 的输入时,$\delta_{ij}=0$,$i=1,2,\cdots,n$,$j=1,2,\cdots,m$;$\boldsymbol{O}:T\to P$ 为输出矩阵,$\boldsymbol{O}=\{\gamma_{ij}\}$,$\gamma_{ij}$ 为逻辑量,$\gamma_{ij}\in\{0,1\}$,当 p_i 是 t_j 的输出时,$\gamma_{ij}=1$,当 p_i 不是 t_j 的输出时,$\gamma_{ij}=0$,$i=1,2,\cdots,n$,$j=1,2,\cdots,m$;$\boldsymbol{I}$,$\boldsymbol{O}$ 为 $n\times m$ 阶矩阵;$\boldsymbol{F}$ 为检测估计权值矩阵,$\boldsymbol{F}=\mathrm{diag}(\mu_1,\mu_2,\cdots,\mu_m)$,$\mu_j\in[0,1]$表示了模糊规则 t_j 的置信度,即该节点在攻击过程中的满足程度、攻击可能性、代价等;$D=\{d_1,d_2,\cdots,d_n\}$为一个命题集合,$|P|=|D|$,d_i 与 p_i 一一对应,为攻击阶段的 p_i 系统状态等的描述,$\boldsymbol{\theta}^0=(\theta_1^0,\cdots,\theta_n^0)^{\mathrm{T}}$,$\theta_i^0$ 是命题 d_i 的初始逻辑状态,θ_i^0 为[-1,1]区间的双枝模糊集区间数,表示了命题 d_i 存在的真实程度。若 $\theta_i^0\in(0,1]$即表示命题 d_i 所对应的因素对网络攻击具有积极促进作用;若 $\theta_i^0\in[-1,0)$则表示命题 d_i 所对应的因素对网络攻击具有消极抑制作用,$\theta_i^0=0$ 表示命题 d_i 所对应的因素对网络攻击,既可能具有积极促进作用,又可能具有消极抑制作用,它是网络攻击的中间状态节点。

一个布尔代数,取值为{0,1},表示命题和规则所涉及的概念是确切的、清晰的。BBFLPAN 中对命题可信度 θ 的描述,是基于双枝模糊集的,取值在区间[-1,1]上。在 BBFLPAN 中,θ 与 1,0 或-1 越接近,概念越清晰,与 1 越接近,则该命题对应的因素对网络攻击的促进作用越大;与-1 越接近,说明该命题对应的因素对网络攻击的抑制作用越大;从正向与 0 越接近,说明该命题对应的因素对网络攻击的促进作用越小;从负向与 0 越接近,说明该命题对应的因素对网络攻击的抑制作用越小。

2.2 BBFLPAN 的模糊 Petri 网表示

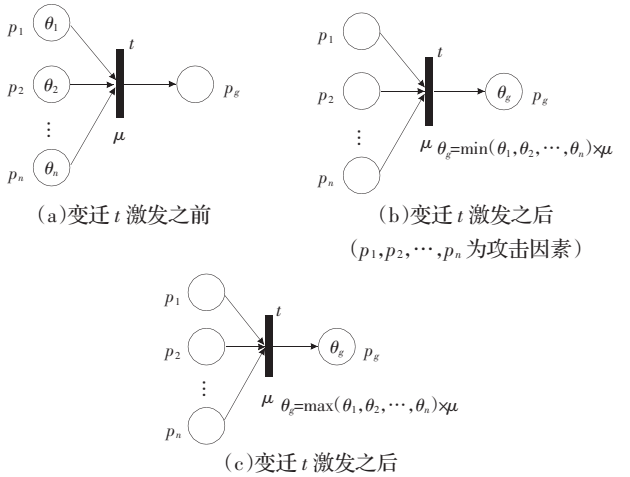
BBFLPAN 中的库所可以表示为三要元$(p_k,{}^{\cdot}p_k,p_k^{\cdot})$,${}^{\cdot}p_k$ 和 $p_k^{\cdot}$ 分别是 p_k 的输入变迁集和输出变迁集,${}^{\cdot}p_k$ 反映了导致 p_k 这一攻击阶段之前的攻击过程;$p_k^{\cdot}$ 反映了 p_k 这一攻击阶段的下一步攻击过程。若 ${}^{\cdot}p_k=\varnothing$,则 p_k 为攻击起点,并将 p_k 称作起始库所;若 $p_k^{\cdot}=\varnothing$,则 p_k 为攻击最终目标,并将 p_k 称作顶上库所或目标库所。变迁可以表示为三要元$(t_k,{}^{\cdot}t_k,t_k^{\cdot})$,${}^{\cdot}t_k$ 和 $t_k^{\cdot}$ 分别是 t_k 的输入库所集和输出库所集,分别反映了 t_k 这一攻击过程中系统的前后状态变化,${}^{\cdot}t_k\neq\varnothing$,为攻击前提集合,$t_k^{\cdot}\neq\varnothing$,为攻击结果集合。

当变迁 t_k 的输入库所集 ${}^{\cdot}t_k$ 中因素属于单一因素集时,一般的模糊 Petri 网能够清晰的描述变迁 t_k 的触发条件和结果。而在攻击模型 BBFLPAN 中,变迁 t_k 的输入库所集 ${}^{\cdot}t_k$ 中的因素既有可能是对网络攻击起促进作用的因素,也有可能是起抑制作用的因素,输入库所集 ${}^{\cdot}t_k$ 中因素不再从属于特定因素集,这已经超出了一般的模糊 Petri 网的应用范围。故而,根据攻击模型 BBFLPAN 的定义和双枝模糊逻辑理论,定义网络攻击模型 BBFLPAN 的模糊 Petri 网表示规则和相应的激发规则如下:

(1)网络攻击的攻击阶段及防御阶段表示为模糊 Petri 网的库所 p;

(2)网络攻击的攻击过程及防御过程表示为模糊 Petri 网的变迁 t;

(3)依据 BBFLPAN 的定义和模糊命题合取式的真值取各子式真值的最小值、模糊命题析取式的真值取各子式真值的最大值的基本原理,命题规则中的与、或关系的模糊 Petri 网表示和相应的激发规则如图 1、图 2 所示。



(a)变迁 t 激发之前　(b)变迁 t 激发之后

($p_1,p_2,\cdots,p_n$ 为攻击因素)

(c)变迁 t 激发之后

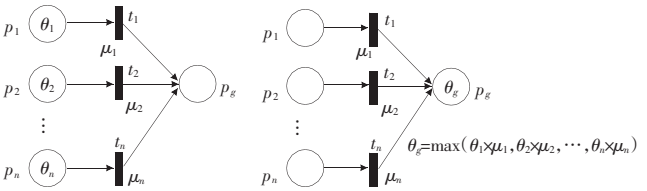
($p_1,p_2,\cdots,p_n$ 为防御因素)

图 1 与规则的 BBFLPAN 模型

与关系规则,如:IF $d_1(\theta_1)$AND $d_2(\theta_2)$AND⋯AND $d_n(\theta_n)$ THEN $d_g(\mathrm{CF}=\mu)$,其模糊 Petri 网表示和相应的激发规则如图 1 所示。

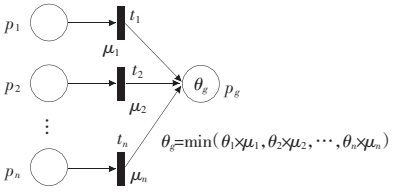
或关系规则,如:IF $d_1(\theta_1)$OR $d_2(\theta_2)$OR⋯OR $d_n(\theta_n)$THEN $d_g(\mathrm{CF}=\mu_j)j=1,2,\cdots,n$,其模糊 Petri 网表示和相应的激发规则如图 2 所示。

根据 BBFLPAN 的定义和以上的三条表示规则,可以得到 BBFLPAN 模型的基本原理图,如图 3 所示。其中,$p_1,p_2,\cdots,p_a$ 表示对网络攻击起促进作用的因素,$p_{a+1},p_{a+2},\cdots,p_{a+b}$ 表示对网络攻击起抑制作用的攻击防御因素,$p_{a+b+1},\cdots,p_{n-1},p_n$ 表示攻击



(a)变迁 t_j 激发之前　(b)变迁 t_j 激发之后

($p_1,p_2,\cdots,p_n$ 为攻击因素)



(c)变迁 t_j 激发之后

($p_1,p_2,\cdots,p_n$ 为防御因素)

图 2　或规则的 BBFLPAN 模型

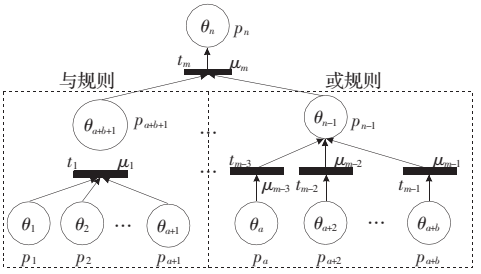


图 3　BBFLPAN 模型基本原理图

过程的中间状态。在 $p_1,p_2,\cdots,p_{a+1}$ 这些因素的共同作用下，网络攻击的状态将有可能转变到 p_{a+b+1} 状态，故此在图 3 中采用与规则的表示方法；而 $p_a,p_{a+2},\cdots,p_{a+b}$ 中的任何一个因素都有可能促进或是抑制网络攻击的状态转变到 p_{n-1} 状态，因此在图 3 中采用或规则的表示方法。

3　模糊推理算法

所提出的网络攻击模型 BBFLPAN 是建立在双枝模糊逻辑[13-14]的基础之上的，在其模糊推理算法中，首先以文献[15]中介绍的双枝模糊逻辑推理的几种基本形式为依据，提出 BBFLPAN 模型推理的基本规则。然后，根据 BBFLPAN 模型的基本推理规则，结合 BBFLPAN 模型的定义，给出其相应的推理算法。

3.1　基本推理规则

文献[11]中介绍了双枝模糊逻辑推理的几种基本形式，在此基础之上，结合 2.2 节提出以下 BBFLPAN 模型推理的基本规则。

对于与规则，如：IF $d_1(\theta_1)$AND $d_2(\theta_2)$AND…AND $d_n(\theta_n)$ THEN $d_g(\mathrm{CF}=\mu)$，其相应的 BBFLPAN 模型如图 1 所示，按照规则中命题(库所)对应网络攻击因素对网络攻击作用的不同，可以将与规则的推理分为以下三种形式：

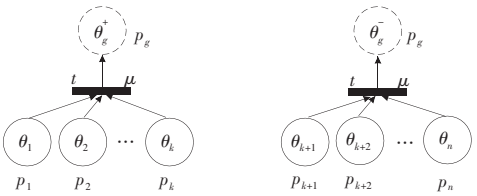
(1)若 $\theta_i\in[0,1],i=1,2,\cdots,n$，即 p_i 所对应的因素均对网络攻击起促进作用，则：

$$\theta_g=\min(\theta_1,\theta_2,\cdots,\theta_n)\times\mu=\min(\theta_1\times\mu,\theta_2\times\mu,\cdots,\theta_n\times\mu) \quad (1)$$

(2)若 $\theta_i\in[-1,0],i=1,2,\cdots,n$，即 p_i 所对应的因素均对网络攻击起抑制作用，则：

$$\theta_g=\max(\theta_1,\theta_2,\cdots,\theta_n)\times\mu=\max(\theta_1\times\mu,\theta_2\times\mu,\cdots,\theta_n\times\mu) \quad (2)$$

(3)若 $\theta_i\in[-1,1],i=1,2,\cdots,n$，即 p_i 所对应的因素中，既有对网络攻击起促进作用的因素，也有起抑制作用的因素。假设：$p_1,p_2,\cdots,p_k(1\leqslant k<n)$所对应的因素，对网络攻击起促进作用，则 $\theta_h\in[0,1],h=1,2,\cdots,k$；$p_{k+1},p_{k+2},\cdots,p_n$ 所对应的因素，对网络攻击起抑制作用，则 $\theta_l\in[-1,0],l=k+1,k+2,\cdots,n$。那么图 1 所示的 BBFLPAN 模型，可以分解为攻击枝 BBFLPAN 和防御枝 BBFLPAN，如图 4 所示。



(a)与规则攻击枝 BBFLPAN　(b)与规则防御枝 BBFLPAN

图 4　BBFLPAN 与规则的分解图

在图 4 中，将 p_g 库所一分为二，与在图 1 中的意义已经发生了变化，故而将其表示为虚圈，以示区别。θ_g^+ 表示了 $p_h(h=1,2,\cdots,k)$所对应的对网络攻击起促进作用的因素，对最终状态 p_g 的支持度；θ_g^- 表示了 $p_l(l=k+1,k+2,\cdots,n)$所对应的对网络攻击起抑制作用的因素，对最终状态 p_g 的支持度。

由式(1)和(2)，可以得到：

$$\theta_g^+=\min(\theta_1,\theta_2,\cdots,\theta_k)\times\mu=\min(\theta_1\times\mu,\theta_2\times\mu,\cdots,\theta_k\times\mu) \quad (3)$$

$$\theta_g^-=\max(\theta_{k+1},\theta_{k+2},\cdots,\theta_n)\times\mu=\max(\theta_{k+1}\times\mu,\theta_{k+2}\times\mu,\cdots,\theta_n\times\mu) \quad (4)$$

对于或规则，如：IF $d_1(\theta_1)$OR $d_2(\theta_2)$OR…OR $d_n(\theta_n)$THEN $d_g(\mathrm{CF}=\mu_j)j=1,2,\cdots,n$，其相应的 BBFLPAN 模型如图 2 所示，按照规则中命题(库所)对应网络攻击因素对网络攻击作用的不同，也可以将或规则的推理分为以下三种形式：

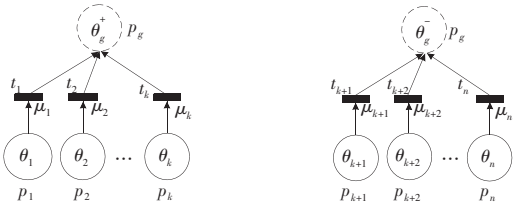
(1)若 $\theta_i\in[0,1],i=1,2,\cdots,n$，即 p_i 所对应的因素均对网络攻击起促进作用，则：

$$\theta_g=\max(\theta_1\times\mu_1,\theta_2\times\mu_2,\cdots,\theta_n\times\mu_n) \quad (5)$$

(2)若 $\theta_i\in[-1,0],i=1,2,\cdots,n$，即 p_i 所对应的因素均对网络攻击起抑制作用，则：

$$\theta_g=\min(\theta_1\times\mu_1,\theta_2\times\mu_2,\cdots,\theta_n\times\mu_n) \quad (6)$$

(3)若 $\theta_i\in[-1,1],i=1,2,\cdots,n$，即 p_i 所对应的因素中，既有对网络攻击起促进作用的因素，也有起抑制作用的因素。依照与规则中的假设，可以将图 2 所示的 BBFLPAN 模型，分解为攻击枝 BBFLPAN 和防御枝 BBFLPAN，如图 5 所示。



(a)或规则攻击枝 BBFLPAN　(b)或规则防御枝 BBFLPAN

图 5　BBFLPAN 或规则的分解图

在图 5 中，将 p_g 库所采用与图 4 中相类似的方法，将其表示为虚圈，以示区别。其中，θ_g^+ 和 θ_g^- 所表示的意义和与规则中的一致。

由式(5)和式(6)，可以得到：

$$\theta_g^+=\max(\theta_1\times\mu_1,\theta_2\times\mu_2,\cdots,\theta_k\times\mu_k) \quad (7)$$

$$\theta_g^-=\min(\theta_{k+1}\times\mu_{k+1},\theta_{k+2}\times\mu_{k+2},\cdots,\theta_n\times\mu_n) \quad (8)$$

对于与、或两种规则第三种情况下，库所 p_g 的可信度 θ_g，可以分别依据式(3)、(4)、(7)、(8)求得，计算公式如下：

$$\boldsymbol{\theta}_g=\theta_g^+\oplus\theta_g^-=\begin{cases}\theta_g^+ & 若|\theta_g^+|>|\theta_g^-|\\ 0 & 若|\theta_g^+|=|\theta_g^-|\\ \theta_g^- & 若|\theta_g^+|<|\theta_g^-|\end{cases} \tag{9}$$

3.2 基于推理规则的模糊推理算法

文献[10]依据 MYCIN 置信度方法[16]所提出的推理算法,强调了推理的最终结果,忽视了整个推理过程中各个结点的状态变化情况,致使模型不能提到很好的安全预警功能。就攻击模型而言,更多的时候关注的并不是这次网络攻击的最终结果,而是要发现网络系统当中最脆弱的结点。在该文推理算法中,预设了起始库所集 $Pset$、中间状态库所集 P_g、可激发变迁集 $Tset$,通过这三个集合可以清晰地观测到网络攻击的整个过程,从而发现那些最危险的结点,为安全预警提供了依据。

在该模糊推理算法中,首先根据的 θ_i^0 取值情况,将库所集 P 分为起始库所集 $Pset$ 和中间状态库所集 P_g。然后根据起始库所集 $Pset$,构造可激发变迁集 $Tset$,并对 ${}^{\cdot}t_j$ 按照与规则进行推理计算,并将推理计算结果存放在矩阵 $\boldsymbol{\theta}_g$ 中。最后,再对中间状态库所集 P_g 中库所的输入变迁按照或规则进行推理计算,从而得到中间状态库所集 P_g 中每个库所所对应命题的可信度。

推理算法如下:

步骤 1 分别构造起始库所集 $Pset$ 和中间状态库所集 P_g:若 $\theta_i^0\neq 0$,则 $p_i\in Pset$,否则,$p_i\in P_g$。构造矩阵 $\boldsymbol{\theta}_g=\{\theta_{gij}\}$,$\theta_{gij}$ 初值设为 0,矩阵 $\boldsymbol{\theta}_g$ 为 $n\times m$ 阶矩阵。构造变迁集 Ts 用以记录可激发变迁集 $Tset$ 中已经激发的变迁,$Ts=\varnothing$;

步骤 2 构造可激发变迁集 $Tset$:若 $\forall p_i\in{}^{\cdot}t_j, p_i\in Pset$ 且 $t_j\notin Ts$,则 $t_j\in Tset$;

步骤 3 对 $\forall p_i\in Pset, t_j\in Tset$,对 t_j 进行如下操作:

```
int θ_g^+=1,θ_g^-=-1;
boolean flag_pos=false,flag_neg=false;//分别用于标记 ·t_j 中攻击因素的性质
for(i=1;i≤n;i++){
  if(I[i][j]==1){//对 ·t_j 按照与规则进行推理计算
    if(θ_i≥0){
      flag_pos=true;//若 ·t_j 中因素对网络攻击起促进作用,则 flag_pos 为真
      if(θ_g^+>min(θ_g^+,θ_i×μ_j)){θ_g^+=min(θ_g^+,θ_i×μ_j);}
    }
    else{
      flag_neg=true;//若 ·t_j 中因素对网络攻击起抑制作用,则 flag_neg 为真
      if(θ_g^-<max(θ_g^-,θ_i×μ_j)){θ_g^-=max(θ_g^-,θ_i×μ_j);}
    }
  }
}//end for
Ts=Ts+{t_j};//将已经激发的变迁 t_j,放入变迁集 Ts
if(flag_pos=true and flag_neg=false)
    θ_gj=θ_g^+;//·t_j 中仅存在对网络攻击起促进作用的因素
else if(flag_pos= false and flag_neg= true)
    θ_gj=θ_g^-;//·t_j 中仅存在对网络攻击起抑制作用的因素
else θ_gj=θ_g^+⊕θ_g^-;//否则,根据式(9)求得 θ_gj
for(i=1;i≤n;i++){
  if(O[i][j]==1){
    θ_g[i][j]=θ_gj;//将 ·t_j 中库所对 t_j 库所的支持度放入矩阵 θ_g
  }
}//end for
```

步骤 4 对 $\forall p_i\in P_g$,对 p_i 进行如下操作:

```
boolean flag=false;//用于标记 ·p_i 中是否未激发的变迁
int θ_g^+=0,θ_g^-=0;
for(j=1;j≤m;j++){
  if(O[i][j]==1 and t_j∉Ts){flag=true;} //·p_i 中存在未激发的变迁
}
for(j=1;j≤m;j++){
  if(O[i][j]==1 and flag= false){//对 ·p_i 中已激发的变迁按照或规则进行推理计算
    if(θ_g[i][j]≥0){
      if(θ_g^+<max(θ_g^+,θ_g[i][j])){θ_g^+=max(θ_g^+,θ_g[i][j]);}
    }
    else{
      if(θ_g^->min(θ_g^-,θ_g[i][j])){θ_g^-=min(θ_g^-,θ_g[i][j]);}
    }
  }
}//end for
θ_gi=θ_g^+⊕θ_g^-;//根据式(9)求得 θ_gi
θ_i=θ_gi;//得到库所 p_i 所对应命题的可信度
Pset=Pset+{p_i};//将库所 p_i 加入到起始库所集 Pset 中
Pg=Pg-{p_i};//从中间状态库所集 Pg 删除库所 p_i
```

步骤 5 若 $Pg=\varnothing$ 则转步骤 6,否则转步骤 2;

步骤 6 推理结束。

4 实验验证

为了比较该文推理算法和文献[10]中推理算法有效性,仍以攻击者利用系统漏洞试图获取目标系统的访问权限,即特权提升作为实例,对算法进行验证。文献[17]借鉴操作系统实现中的不同用户角色具有不同程度的特权的思想,引入了"特权集"属性的分类特征,将访问者权限和特权等级相对应,如表 1 所示。

表 1 访问权限与特权等级对照表

访问权限	特权集合	角色描述
root	Proot	系统管理员,管理系统设备、系统文件和系统进程等一切资源
supuser	Psupuser	具有普通用户所没有的一些特殊权限,没有获得 root 权限
user	Puser	系统普通用户,有自己独立私有的资源
guest	Pguest	匿名登陆访问计算机系统的来宾,具有 user 的部分权限
access	Paccess	访问网络服务的远程访问者,可以和网络进程交互数据

依据 BBFLPAN 模型的定义,用 $p_1,p_2,p_3,p_4,p_5,p_6,p_7,p_8,p_9$ 分别标识系统中的弱点实例,$p_{10},p_{11},p_{12},p_{13}$ 分别标识对网络攻击起抑制作用的攻击防御实例,另外 $p_{14},p_{15},p_{16},p_{17}$ 标识了 P_{guest},P_{user},$P_{supuser}$,P_{root},。其中,p_1 表示系统开放了有漏洞的网络服务,设其初始置信度为 0.8;p_2 表示系统中存在大量打开的端口,设其初始置信度为 1.0;p_3 表示防火墙规则配置失误,设其初始置信度为 0.5;p_4 表示操作系统以 IP 地址作为认证依据,设其初始置信度为 0.7;p_5 表示系统主机之间具有信任关系,设其初始置信度为 0.5;p_6 表示共享目录读写权限过大,设其初始置信度为 0.6;p_7 表示应用程序对系统调用错误不做处理,设其初始置信度为 0.7;p_8 表示系统保留默认的口令和账号,设其初始置信度为 0.4;p_9 表示攻击者利用非技术性手段获得系统关键信息,设其初始置信度为 0.8;p_{10} 表示防火墙技术,设其初始置信度为

-0.4；p_{11} 表示身份认证系统，设其初始置信度为-0.8；p_{12} 表示调整系统共享信息设置，设其初始置信度为-0.7；p_{13} 表示定期更换管理员口令，设其初始置信度为-0.5。同时，用 $\mu_1,\mu_2,\mu_3,\mu_4,\mu_5,\mu_6,\mu_7,\mu_8$ 表示各个规则的置信度，则可以得到规则库如下所示：

规则 1 IF p_1(0.8)AND p_2(1.0)THEN $p_{14}(\mu_1=0.8)$；

规则 2 IF p_4(0.7)AND p_{11}(-0.8)AND p_{14} THEN $p_{15}(\mu_2=0.6)$；

规则 3 IF p_3(0.5)AND p_{10}(-0.4)AND p_{14} THEN $p_{15}(\mu_3=0.5)$；

规则 4 IF p_5(0.5)AND p_{11}(-0.8)AND p_{15} THEN $p_{16}(\mu_4=0.6)$；

规则 5 IF p_6(0.6)AND p_{12}(-0.7)AND p_{15} THEN $p_{16}(\mu_5=1.0)$；

规则 6 IF p_7(0.7)THEN $p_{16}(\mu_6=0.8)$；

规则 7 IF p_7(0.7)THEN $p_{17}(\mu_6=0.8)$；

规则 8 IF p_8(0.4)AND p_{13}(-0.5)AND p_{16} THEN $p_{17}(\mu_7=1.0)$；

规则 9 IF p_9(0.8)AND p_{13}(-0.5)AND p_{16} THEN $p_{17}(\mu_8=0.1)$。

按照 2.2 节和以上规则，可以特权提升的 BBFLPAN 模型如图 6 所示。

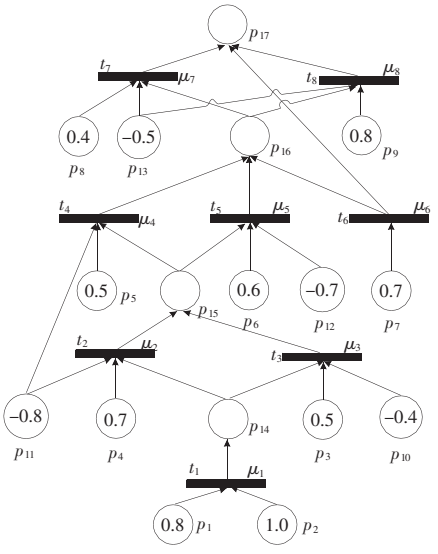


图 6　特权提升 BBFLPAN

根据 BBFLPAN 的定义和规则库，可以得到：$\boldsymbol{\theta}^0=(0.8,1.0,0.5,0.7,0.5,0.6,0.7,0.4,0.8,-0.4,-0.8,-0.7,-0.5,0.0,0.0,0.0,0.0)^{\mathrm{T}}$，则 $Pset=\{p_1,p_2,p_3,p_4,p_5,p_6,p_7,p_8,p_9,p_{10},p_{11},p_{12},p_{13}\}$，$P_g=\{p_{14},p_{15},p_{16},p_{17}\}$。

当算法第一轮执行时，可激发变迁集 $Tset=\{t_1,t_6\}$，通过一轮的推理计算，可以得到：$\theta_{14}=0.64$，$Pset=\{p_1,p_2,p_3,p_4,p_5,p_6,p_7,p_8,p_9,p_{10},p_{11},p_{12},p_{13},p_{14}\}$，$P_g=\{p_{15},p_{16},p_{17}\}$；

经过算法的第二轮推理计算，可以得到：$\theta_{15}=-0.48$，$Pset=\{p_1,p_2,p_3,p_4,p_5,p_6,p_7,p_8,p_9,p_{10},p_{11},p_{12},p_{13},p_{14},p_{15}\}$，$P_g=\{p_{16},p_{17}\}$；

经过算法的第三轮推理计算，可以得到：$\theta_{16}=0.6$，$Pset=\{p_1,p_2,p_3,p_4,p_5,p_6,p_7,p_8,p_9,p_{10},p_{11},p_{12},p_{13},p_{14},p_{15},p_{16}\}$，$P_g=\{p_{17}\}$；

经过算法的第四轮推理计算，可以得到：$\theta_{17}=0.56$，$Pset=\{p_1,p_2,p_3,p_4,p_5,p_6,p_7,p_8,p_9,p_{10},p_{11},p_{12},p_{13},p_{14},p_{15},p_{16},p_{17}\}$，$P_g=\varnothing$。

由于 $P_g=\varnothing$，所以算法推理结束。

由以上推理过程可以发现，在整个的攻击过程中，攻击者首先获取了结点 p_{14} 的控制权，并且该结点还以 0.64 的高可信度对后续攻击起到促进作用。随后攻击者试图获取结点 p_{15} 的控制权，但是未能取得相应的权利，这主要得力于结点 p_{10}、p_{11} 的保障作用，同时该结点还对后续攻击起到了抑制作用。在结点 p_{15} 受挫并没有阻止攻击者获取结点 p_{16} 的控制权，这主要是攻击者通过结点 p_7 得到的，随后在的结点 p_7 协助下，攻击者很容易地就获取了最终结点 p_{17} 的控制权。由此可见，结点 p_7 是整个系统当中最危险的一个结点，应及时对此采取相应的防御措施。

较之文献[10]中的推理更能清晰地反映攻击模型中各个结点在不同时刻的状态，从而使模型更加真实直观地反映了网络攻击的演变情况，能更好地发现和认识网络系统的漏洞，有针对性地采取相应的安全防御措施。

5　结论

攻击模型是一个较新的研究领域，从攻击模型化的角度出发，再次将对网络攻击起积极和消极的正反两种因素进行综合考虑分析，提出了一种基于双枝模糊逻辑和模糊 Petri 网(FPN)的攻击模型 BBFLPAN，并给出了相应的推理算法，经实验验证，该模型更能有效的表示攻击和防御情况，其推理算法是有效的。

BBFLPAN 作为一种全新的网络攻击建模工具，充分地利用了双枝模糊逻辑和 FPN 的优点，并将它们有力地结合起来，一方面丰富了攻击建模的研究方法，扩展了双枝模糊逻辑的研究领域。另一方面，也使得其具有良好的知识表示能力、推理过程的并行性和模糊性等。

参考文献：

[1] 陈春霞，黄皓.攻击模型的分析与研究[J].计算机应用研究，2005(7)：115-118.

[2] Moore A P，Tllison R，Linger R C.Attack modeling for information security and survivability，CMU/SEI-2001-TN-001[R].2001.

[3] Tidwell T，Larson R，Fitch K.Modeling internet attacks[C]//Proceedings of the 2001 IEEE Workshop on Information Assurance and Security，2001：54-59.

[4] 张博，李伟华.Phishing 攻击行为及其防御模型研究[J].计算机工程，2006，32(14)：125-128.

[5] 张基温，叶茜.分布式拒绝服务攻击建模与形式化描述[J].计算机工程与设计，2006，27(21)：4125-4129.

[6] 念其锋，蔡开裕，杜秀春.基于攻击树的边界网关安全测试[J].计算机工程与科学，2006，28(8)：14-19.

[7] 危胜军，胡昌振，谭惠民.模糊 Petri 网知识表示方法在入侵检测中的应用[J].计算机工程，2005，31(2)：130-133.

[8] Mcdrmott J.Attack net penetration testing[C]//The 2000 New Security Parading Workshop，2000：5-22.

[9] 赖海光，黄皓，谢俊元.基于系统状态集合的攻击模型及其应用[J].计算机应用，2005，25(7)：1535-1539.

[10] 黄光球，任大勇.基于双枝模糊决策和模糊 Petri 网的攻击模型[J].计算机应用，2007，27(11)：2689-2693.

[11]史开泉，李岐强.双枝模糊决策与决策识别问题[J].中国工程，2001，3(1)：71-77.

[12] Shi Kai-quan，Cui Yu-quan.Both-branch fuzzy decision and decision encryption authentication[J].Science in China：Series F，2003，46(2)：90-103.

[13] 刘刚，赵建辉，刘强.双枝模糊逻辑(Ⅱ)[J].计算机工程与应用，2005，41(19)：47-49.

[14] 刘刚，徐衍亮，赵建辉，等.双枝模糊逻辑[J].计算机工程与应用，2003，39(30)：96-98.

[15] 刘刚，刘强.双枝模糊推理框架[J].计算机工程与应用，2003，39(32)：102-105.

[16] 李英华，叶天荣，张虹霞.计算机非传统推理[M].北京：宇航出版社，1992.

[17] 张涛，胡铭曾，王晓春，等.基于故障树的计算机安全分析模型[J].高技术通讯，2005，15(7)：18-23.