基于双枝模糊逻辑和模糊着色 Petri 网的攻击模型*

高 翔, 祝跃飞, 卢锦江, 刘 龙
(解放军信息工程大学 信息工程学院, 郑州 450002)

摘 要: 定义了一种基于双枝模糊逻辑和模糊着色 Petri 网的网络攻击模型,从对攻击起促进和抑制作用这两方面对网络攻击进行综合考虑与分析,同时对模糊规则库中的不同变量用不同的颜色来区分,因此可构成一个简明的 BBFCPN 模型。在此基础上,给出了 BBFCPN 模型的基本推理规则和推理算法。针对攻击实例的分析进一步验证了提出的模型及相关推理算法。

关键词: 模糊着色 Petri 网; 双枝模糊逻辑; 攻击建模
中图分类号: TP301 **文献标志码**: A **文章编号**: 1001-3695(2013)05-1527-03
doi:10.3969/j.issn.1001-3695.2013.05.063

Attack model based on both-branch fuzzy logic and fuzzy colored Petri nets

GAO Xiang, ZHU Yue-fei, LU Jin-jiang, LIU Long
(*Institute of Information Engineering, PLA Information Engineering University, Zhengzhou* 450002, *China*)

Abstract: This paper proposed a both-branch fuzzy logic fuzzy colored Petri nets (BBFCPN) model for attack. It analyzed the promoting and suppressive factors to network attack and in this attack model. It also distinguished the different variable in rule base with a kind of color through making the best use of its characteristic of BBFCPN model. On this basis, it proposed the basic reasoning rules and algorithm. The network instance further validated the proposed model and reasoning algorithm.
Key words: fuzzy colored Petri net; both-branch fuzzy logic; attack modeling

0 引言

随着计算机网络的飞速发展,以及大规模、分布式高速网络被大量地应用,人们对网络的依赖性在不断增加,随之而来的信息安全问题变得尤为突出,不断增长和扩散的计算机病毒(如木马、蠕虫)和黑客攻击等对广大用户和企业造成了不可估量的损失。因此,面对各种网络威胁,必须采取有效措施来保证计算机网络的安全运行。传统的被动型安全防御技术(入侵检测、防火墙以及用户认证等)已不能满足人们的需要,国内外学者纷纷致力于研究主动的安全分析和评估方法,而网络攻击建模是网络安全评估和全面建立安全防御措施的基础。

目前,在网络攻击的建模方面已取得了一些成果。常见的模型有攻击树模型[1]、攻击图模型[2]、脆弱性状态图[3]、威胁传播模型[4],从不同角度分析和评估系统安全,反映了攻击者和网络系统的状态变化。但这些模型在对网络攻击进行描述和评估时,多是从网络攻击者的角度来进行攻击建模研究,对攻击发生发起积极作用的因素进行分析研究,而对攻击起抑制作用的防御因素很少涉及。黄光球等人[5]提出了基于双枝模糊逻辑和模糊 Petri 网的攻击模型,从对攻击起促进和抑制作用两个方面对网络攻击进行综合考虑与分析,但是普通模糊 Petri 网在描述知识时会随着规则知识的增加而变得十分复杂,这样得到的 Petri 网模型就非常庞大,给分析带来很大的不变。为了构成更简明的模型,本文以双枝模糊决策理论为基础,将 FPN 和 CPN 相结合,提出攻击模型 BBFCPN(both-branch fuzzy colored Petri nets)来描述攻击过程中的模糊信息,并进行基于模糊知识的推理,特别是对协同式网络攻击行为的描述。

1 攻击模型 BBFCPN

1.1 BBFCPN 的定义

定义 1 模糊 Petri 网可以描述为一个八元组:

$$\mathrm{FPN}=(P,T,D,\mathrm{IN},\mathrm{OUT},F,W,R)$$

其中:$P=\{p_1,p_2,\cdots,p_n\}$ 是库所的有限集合;$T=\{t_1,t_2,\cdots,t_n\}$ 为变迁的有限集合;$D=\{d_1,d_2,\cdots,d_n\}$ 为命题的有限集合;$\mathrm{IN}:P\to T$ 为输入函数,表示从库所到变迁的映射;$\mathrm{OUT}:T\to P$ 为输出函数,表示从变迁到库所的映射;$F:T\to[0,1]$ 表示变迁的可信度函数,每个变迁都有一个可信度,$F(t_j)=\mu_j(j=1,2,\cdots,m)$;$W:P\to[0,1]$ 表示库所 p_i 的可信度函数,$W(p_i)(i=1,2,\cdots,m)$;$R:P\to D$ 为相关函数,表示库所到命题的映射,即库所对应的命题。

定义 2 BBFCPN 可以表示为如下元组形式:

$$\mathrm{BBFCPN}=(\Sigma,P,T,D,A,C,G,E,F,W,R,I)$$

其中:Σ 是一组有限非空数据类型的集合,又称为颜色集;$P=\{p_1,p_2,\cdots,p_n\}$ 为描述系统模糊产生式规则的库所的有限集合,称为模糊库所;$T=\{t_1,t_2,\cdots,t_n\}$ 为连接模糊库所的变迁的有限集合,称为模糊变迁;$D=\{d_1,d_2,\cdots,d_n\}$ 是命题的有限集合,$|P|=|D|$,并且 d_i 和 p_i 一一对应;A 是有限弧集,$A\subseteq P\times$

收稿日期: 2012-08-23; **修回日期**: 2012-10-22 **基金项目**: 郑州市科技创新团队资助项目(10CXTD150)

作者简介:高翔(1984-),男,辽宁辽阳人,博士研究生,主要研究方向为形式化建模与验证、网络与信息安全(feiyu4321@163.com);祝跃飞(1962-),男,教授,博导,博士,主要研究方向为应用数学、网络与信息安全;卢锦江(1982-)男,工程师,硕士,主要研究方向为网络信息安全;刘龙(1983-)男,助教,硕士,主要研究方向为网络信息安全.

$T \cup T \times P$,且弧仅存在于 P 和 T 之间;C 是颜色函数集,$C: P \to \Sigma$;G 是条件函数的集合,$G: T \to$ BoolExpression,表示变迁到变迁表达式的映射函数,且满足 $\forall t \in T: [\text{type}(G(t)) = \text{Boolean} \wedge \text{type}(\text{var}(G(t))) \subseteq \Sigma]$;$E$ 是弧函数的集合,$E: F \to FE$,满足 $\forall f \in F: [\text{type}(E(f)) = C(p)_{\text{MS}} \wedge \text{type}(\text{var}(E(f))) \subseteq \Sigma]$,$C(p)_{\text{MS}}$表示 $C(p)$上的多重集的集合;$F: T \to [0,1]$表示模糊变迁到 0 和 1 间的一个映射,$F(t_j) = \mu_j (j = 1,2,\cdots,m)$,$\mu_j$ 表示模糊规则 t_j 的置信度,即该节点在攻击过程中的攻击成功概率、代价等;$W: P \to [-1,1]$表示模糊库所到 -1 和 1 间的一个映射;$R: P \to D$ 为模糊库所和命题间的一一映射;I 是 BBFCPN 的初始标志,为一个二元组 (M_0, W_0),且有 $\forall p \in P: [\text{type}(M_0(p)) = C(p)_{\text{MS}}]$,$W_0(p_i)$为$[-1,1]$区间的双枝模糊集区间数,表示库 p_i 所的初始可信度,即命题 d_i 存在的真实程度。若 $W_0(p_i) \in (0,1]$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;$W_0(p_i) \in [-1,0)$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;$W_0(p_i) = 0$ 表示命题 d_i 所对应的因素作用不确定。

上述定义中,type(x)表示 x 的值的类型;Boolean 表示布尔类型,其值为 true 或 false;var(x)表示 x 为一个变量。

在 BBFCPN 模型中,命题的可信度取值与 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,则该命题对应的因素对网络攻击的抑制作用越大;从正向命题的可信度取值与 0 越接近,则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,则该命题对应的因素对网络攻击的抑制作用越小。

1.2 模糊产生式规则的 BBFCPN 表示

网络攻击行为具有很大的随机性和模糊性,无法用精确的形式来表达。模糊产生式规则刻画了多个命题之间的模糊关系,很适合表达这类不确定知识。BBFCPN 的每一个变迁对应一个规则,表示网络攻击的攻击过程及防御过程。变迁的输入库所和输出库所是规则的前提条件和结论命题,表示攻击及防御相关状态。BBFCPN 中变迁发生即相应的规则匹配成功。

一般产生式模糊规则的前提部分或结论部分含有 AND、OR,而且规则的前提命题和结论命题都是变量的子集,如变量主机存在漏洞类型,其子集为缓冲区溢出漏洞、配置不当的软件、脆弱的口令等。把不同规则中的相同变量作为一个库所颜色,如主机存在的漏洞类型就是一个库所颜色,其内容是该变量的模糊子集。如图 1 所示,BBFCPN 模型具有三个库所变量,它对应的规则如下:

if $d_{11}(w_{11})$ AND $d_{21}(w_{21})$ then $d_{31}(w_{31})$ $(CF = \mu_1)$

if $d_{12}(w_{12})$ AND $d_{22}(w_{22})$ then $d_{32}(w_{31})$ $(CF = \mu_2)$

其中:d_{11}、d_{12}、d_{21}、d_{22}、d_{31}、d_{32}是包含模糊变量的命题;d_{11}、d_{21}为第 1 个输入变量的两个模糊子集;d_{21}、d_{22}为第 2 个输入变量的两个模糊子集;d_{31}、d_{32}是输出控制量的两个模糊子集;w_{11}、w_{12}、w_{21}、w_{22}、w_{31}、w_{32}分别是对应命题的可信度;μ_1、μ_2 是模糊规则的置信度。

因此,颜色集 $C(p_1) = \{d_{11}, d_{12}\}$,$C(p_2) = \{d_{21}, d_{22}\}$,$C(p_3) = \{d_{31}, d_{32}\}$,$\mu_j = \{\mu_1, \mu_2\}$。

因此,本文定义的模糊产生式规则的一般形式如下:

type1 if $d_{1i}(w_{1i})$ AND $d_{2j}(w_{2j})$ AND $\cdots$ AND $d_{nm}(w_{nm})$ then $d_{gk}(W_{gk})$ $(CF = \mu_i)$

type2 if $d_{1i}(w_{1i})$ OR $d_{2j}(w_{2j})$ OR$\cdots$OR $d_{nm}(w_{nm})$ then $d_{gk}(w_{gk})$ $(CF = \mu_i)$

其中:$d_{1i}, d_{2j}, \cdots, d_{nm}$表示一组前提和状态;$d_{gk}$表示若干结论;$w_{1i}, w_{2j}, \cdots, w_{nm}, w_{gk}$是命题的可信度;$\mu_i \in [0,1]$是规则的置信度。

以上两类模糊推理规则可用图 2 和 3 的 BBFCPN 模型来表达。

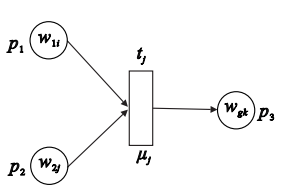

图1 三库所变量模糊规则的BBFCPN模型

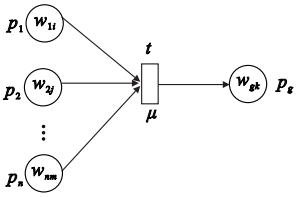

图2 第1类模糊产生式的BBFCPN模型

BBFCPN 攻击模型是建立在双枝模糊逻辑[6,7]基础之上的,结合模型的定义,同时参考双枝模糊逻辑的几种基本形式[8],给出推理的基本规则。

对于第 1 类与规则,其相应的 BBFCPN 模型如图 2 所示,根据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两种形式:

a)若 $w_{nm} \in [0,1]$,即库所 p_n 对应的因素都对攻击起促进作用,则

$$w_{gk} = \min(w_{1i} \times \mu, w_{2j} \times \mu, \cdots, w_{nm} \times \mu) \tag{1}$$

b)若 $w_{nm} \in [-1,0]$,即库所 p_n 对应的因素都对攻击起抑制作用,则

$$w_{gk} = \max(w_{1i} \times \mu, w_{2j} \times \mu, \cdots, w_{nm} \times \mu) \tag{2}$$

对于第 2 类或规则,其相应的 BBFCPN 模型如图 3 所示,根据库所对应网络攻击因素对网络攻击作用的不同,可以将或规则的推理分为以下两种形式:

a)若 $w_{nm} \in [0,1]$,即库所 p_n 对应的因素都对攻击起促进作用,则

$$w_{gk} = \max(w_{1i} \times \mu_1, w_{2j} \times \mu_2, \cdots, w_{nm} \times \mu_n) \tag{3}$$

b)若 $w_{nm} \in [-1,0]$,即库所 p_n 对应的因素都对攻击起抑制作用,则

$$w_{gk} = \min(w_{1i} \times \mu_2, w_{2j} \times \mu_2, \cdots, w_{nm} \times \mu_n) \tag{4}$$

另外,对于与、或规则可能出现第三种情况,即 $w_{nm} \in [-1,1]$,在 p_n 对应的因素中,既有攻击因素也有防御因素。那么可以将 BBFCPN 模型分解为攻击枝和防御枝[5]。w_{gk}^{+}代表库所对网络攻击起促进作用的因素对最终状态 p_g 的支持度;w_{gk}^{-}代表库所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

$$w_{gk}^{+} = \min(w_{1i} \times \mu, w_{2j} \times \mu, \cdots, w_{nm} \times \mu) \tag{5}$$

$$w_{gk}^{-} = \max(w_{1i} \times \mu, w_{2j} \times \mu, \cdots, w_{nm} \times \mu) \tag{6}$$

由式(3)和(4)可以得到

$$w_{gk}^{+} = \max(w_{1i} \times \mu_1, w_{2j} \times \mu_2, \cdots, w_{nm} \times \mu_n) \tag{7}$$

$$w_{gk}^{-} = \min(w_{1i} \times \mu_1, w_{2j} \times \mu_2, \cdots, w_{nm} \times \mu_n) \tag{8}$$

对于第三种情况,可以分别依据式(5)~(8),利用下面计算公式求解

$$w_{gk} = w_{gk}^{+} \oplus w_{gk}^{-} = \begin{cases} w_{gk}^{+} & |w_{gk}^{+}| > |w_{gk}^{-}| \\ 0 & |w_{gk}^{+}| = |w_{gk}^{-}| \\ w_{gk}^{-} & |w_{gk}^{+}| < |w_{gk}^{-}| \end{cases} \tag{9}$$

2　模糊推理算法

2.1　算法相关定义

定义 3　设 p_j 为一个库所,t_i 为一变迁,如果 p_j 是 t_i 直接输入库所,则所有直接可达输入库所的集合称为 t_i 的直接输入库所集,记为 $BP(t_i)$;如果 p_j 是 t_i 直接输出库所,则所有直接可达输出库所的集合称为 t_i 的直接输出库所集,记为 $FP(t_i)$。

根据定义 3,观察 $BP(t_i)$ 中开始库所的个数可以区分与、或两种模糊产生式规则。如图 2 所示,$BP(t_i)=\{p_1,p_2,\cdots,p_n\}$,$BP(t_i)$ 中直接输入库所个数大于 1,可以判定为与推理规则。同理如图 3 所示,若 $BP(t_i)$ 中直接输入库所个数等于 1,可以判定为或推理规则。

定义 npw 集合,用来存放所有库所名和库所的可信度,存放格式为 npw = $\{p_1,w_{1i},p_2,w_{2j},\cdots,p_n,w_{nm}\}$;定义 ubf 集合,用来存放模糊规则的置信度、变迁的直接输入库所名和直接输出库所名,存放格式为 ubf = $\{u_1,BP(t_1),FP(t_1),u_2,BP(t_2),\cdots,u_n,BP(t_n),FP(t_n)\}$;定义 nps 集合,用来存放开始库所名集合,存放格式为 nps = $\{p_{s1},p_{s2},\cdots,p_{ss}\}$。

2.2　推理算法

输入:npw 集合,ubf 集合,nps 集合。
输出:目标库所的可信度值。
推理过程:
$k=1$;
flag_p = false,flag_n = false;
//分别标志 $BP(t_i)$ 中攻击因素的性质
while(true)
{取出 nps 中的第 k 个库所名 p_s;
if(p_s = END)输出推理结果,算法结束
//END 是一个结束标志
for(int $i=1$; $i<=m$; $i++$)//m 为 ubf 集合中的个数
if ($p_s \in BP(t_i)$)
{$p_g \leftarrow FP(t_i)$;
$w_{gk} \leftarrow w(p_s) * \mu_i$;
if($w_{gk}=0$);//当库所 p_g 的可信度值未知时
$w(p_g) \leftarrow w_{gk}$;
else if ($BP(t_j)$中 p_s 个数大于 1)
//按照与规则进行推理计算
{
if(flag_p = true and flag_n = false)
//库所对应的因素都对攻击起促进作用
$w(p_g) \leftarrow \min(w_{gk}, w(p_g))$;
else If(flag_p = false and flag_n = true)
//库所对应的因素都对攻击起抑制作用
$w(p_g) \leftarrow \max(w_{gk}, w(p_g))$;
else $w(p_g) = w_{gk}^{+} \oplus w_{gk}^{-}$
//库所对应的因素既有攻击因素也有防御因素
//根据式(9)求得 $w(p_g)$
}
else { //按照或规则进行推理计算
if(flag_p = true and flag_n = false)
//库所对应的因素都对攻击起促进作用
$w(p_g) \leftarrow \max(w_{gk}, w(p_g))$;
else if(flag_p = false and flag_n = true)
//库所对应的因素都对攻击起抑制作用
$w(p_g) \leftarrow \min(w_{gk}, w(p_g))$;
else $w(p_g) = w_{gk}^{+} \oplus w_{gk}^{-}$
//库所对应的因素既有攻击因素也有防御因素
//根据式(9)求得 $w(p_g)$
}
if $p_g \notin$ nps 将 p_g 插入到 nps 集合的结束标志前;
}
$k++$;
}//endwhile

3　实验验证

下面以利用僵尸网络对目标主机实施 DDoS 攻击为例,说明 BBFCPN 模型的推理过程,实验环境如图 4 所示。在攻击过程中,不确定因素比较多且离散性大,因而采用 BBFCPN 进行专家知识的表示。

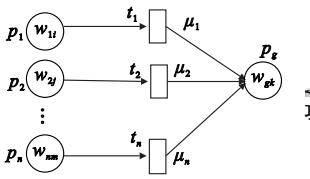

图3　第2类模糊产生式的BBFCPN模型

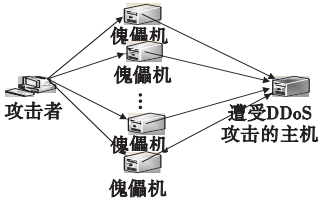

图4　实验拓扑结构

根据 BBFCPN 模型的定义,用命题 d_{1i}、d_{2i}、d_{3i}、d_{4i}、d_{5i}、d_{6i}、d_{7i}、d_{8i}分别表示规则的前提条件,且 $i=1,2,\cdots,n$;d_{aj}、d_{bj}、d_{cj}表示目标状态,且 $j=1,2,3$。其中,d_{1i}表示主机开放的危险端口种类;d_{2i}表示主机开启的防火墙类型;d_{3i}表示主机之间具有的信任关系类型;d_{4i}表示主机未启动的补丁管理软件类型;d_{5i}表示系统存在的漏洞类型;d_{6i}表示主机开启的查杀毒软件类型;d_{7i}表示主机所在网络未启动的网络流量监控器类型;d_{8i}表示主机干扰攻击者发送控制命令的方法类型。d_{ai}表示攻击者提升权限的等级;d_{bi}表示主机被植入僵尸程序的困难程度;d_{ci}表示目标主机到达 DDoS 攻击状态的困难程度。例如 d_{si}可以表示缓冲区溢出漏洞、配置不当的软件、脆弱的口令等。对于命题 d_{aj}、d_{bj}、d_{cj}($j=1,2,3$),分别代表大、中、小。这里,假设每台傀儡主机的对应的前提条件相同。

假设已知模糊产生式规则如下:

R1:if $d_{11}(w_{11})$ AND $d_{21}(w_{21})$ AND $d_{32}(w_{32})$ then $d_{a2}(w_{a2})(\mu=0.8)$;

R2:if $d_{31}(w_{31})$ AND $d_{41}(w_{41})$ AND $d_{51}(w_{51})$ then $d_{a2}(w_{a2})(\mu_2=1)$;

R3: if $d_{62}(w_{62})$ AND $d_{a1}(w_{a1})$ then $d_{b2}(w_{b2})(\mu_3=0.9)$;

R4: if $d_{61}(w_{61})$ AND $d_{71}(w_{71})$ AND $d_{81}(w_{81})$ AND $d_{b2}(w_{b2})$ then $d_{c2}(w_{c2})(\mu_4=0.9)$。

若令上述规则中命题的可信度分别为 $w_{11}=0.4$,$w_{21}=-0.6$,$w_{31}=0.9$,$w_{32}=0.5$,$w_{41}=0.7$,$w_{51}=0.8$,$w_{61}=-0.6$,$w_{62}=-0.3$,$w_{71}=0.7$,$w_{81}=-0.5$,求取命题 d_{a2}、d_{b2}、d_{c2}的可信度 w_{a2}、w_{b2}、w_{c2}。

根据专家规则可得其对应的 BBFCPN 模型,如图 5 所示。t_1 ~ t_4 表示不同的攻击行为,其中,t_1 表示特权提升;t_2 表示主机漏洞攻击;t_3 表示向对方主机植入僵尸程序;t_4 表示僵尸主机下载并运行针对特定主机的 DDoS 攻击程序。

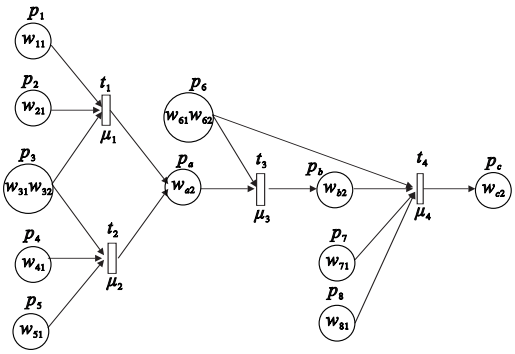

图5　利用僵尸网络实施DDoS攻击的BBFCPN模型

(下转第 1543 页)

(3)符合。这表明,随着节点对将来利益的重视程度,数据包的成功发送概率也在提高,并且在相同的 δ 下,检测率越高,数据包发送的成功概率也越高。

5　结束语

本文借鉴博弈论的思想,提出了基于无线传感网的重复博弈模型。利用重复博弈论中贴现值对模型进行分析,得出节点攻击与否对未来收益的影响。通过分析模型中节点与 IDS 的重复博弈过程,可以有效地检测出攻击节点并对其进行惩罚。实验中,首先运用博弈论工具 Gambit 验证了模型的可行性,使用 MATLAB 分析了在无线传感网中本文提出的模型,分析各个参数得到实验图。理论分析及实验结果验证了模型的可行性。下一步的工作将会深入研究入侵检测率对本文模型的影响。由于制定基于重复博弈的惩罚策略可以有效地权衡检测率和网络资源,在进一步的研究中,将通过构建真实无线传感网的条件来验证所提方案的各项性能,降低人为干预,提高系统适应能力。

参考文献:

[1] 林闯. 物联网关键理论与技术:专题前言[J]. 计算机学报,2011,34(5):761-762.

[2] AKYILDIZ I F, SU W, SANKARASUBRAMANIAM Y, *et al*. Wireless sensor networks: a survey[J]. Computer Networks, 2002, 38(4):393-422.

[3] SHEN Shi-gen, YUE Guang-xue, CAO Qi-ying. A survey of game theory in wireless sensor networks security[J]. Journal of Networks, 2011, 6(3):521-532.

[4] JADIDOLESLAMY H. A high-level architecture for intrusion detection on heterogeneous wireless sensor networks: hierarchical, scalable and dynamic reconfigurable[J]. Wireless Sensor Network. 2011, 3(7):241-261.

[5] KRONTIRIS I, BENENSON Z, GIANNETSOS T, *et al*. Cooperative intrusion detection in wireless sensor networks[C]//Proc of the 6th European Conference on Wireless Sensor Networks. Berlin: Springer-Verlag, 2009:263-278.

[6] REDDY Y B. A game theory approach to detect malicious nodes in wireless sensor networks[C]//Proc of the 3rd International Conference on Sensor Technologies and Application. Washington DC: IEEE Computer Society, 2009:462-468.

[7] SHEN Shi-gen, LI Yuan-jie, XU Hong-yun. Signaling game based strategy of intrusion detection in wireless sensor networks[J]. Computers & Mathematics with Applications, 2011, 62(6): 2404-2416.

[8] AGAH A, DAD S K. Preventing DoS attacks in wireless sensor networks: a repeated game theory approach[J]. International Journal of Network Security, 2007, 5(2):145-153.

[9] 王博,黄传河,杨文忠,等. Ad hoc 网络中基于惩罚机制的激励合作转发模型[J]. 计算机研究与发展, 2011, 48(3):398-406.

[10] 陆音,石进,谢立. 基于重复博弈的无线自组网络协作增强模型[J]. 软件学报, 2008, 19(3):755-768.

[11] MANSHAEI M H, ZHU Quan-yan, ALPCAN T, *et al*. Game theory meets network security and privacy[R]. [S. l.]: ACM Computing Surveys, 2011.

[12] AFRAND A, DAS S K, BASU K, *et al*. Intrusion detection in sensor networks: a non-cooperative game approach network computing and applications[C]//Proc of the 3rd IEEE International Symposium on Network Computing and Application. Washington DC: IEEE Computer Society, 2004:343-346.

[13] KANTZAVELOUA I, KATSIKAS S. A game-based intrusion detection mechanism to confront internal attackers[J]. Computers & Security, 2010, 29(8):859-874.

[14] 周四清,李志艳,刘田. 无线传感器网络入侵检测的重复博弈建模研究[J]. 计算机工程与应用, 2009, 45(3):119-123.

[15] McKELVEY R D, McLENNAN A M, TUROCY T L. Gambit: software tools for game theory[EB/OL]. (2007-01-30). [2009-01-20]. http://gambit.sourceforge.net.

(上接第 1529 页)

图 5 中的颜色集,定义如下

$C(p_1)=\{d_{11}\}, C(p_2)=\{d_{21}\}, C(p_3)=\{d_{31}, d_{32}\}, C(p_4)=\{d_{41}\}, C(p_5)=\{d_{51}\}, C(p_6)=\{d_{61}, d_{62}\}, C(p_7)=\{d_{71}\}, C(p_8)=\{d_{81}\}, C(p_a)=\{d_{a2}\}, C(p_b)=\{d_{b2}\}, C(p_c)=\{d_{c2}\}, \mu_j=\{\mu_1, \mu_2, \mu_3, \mu_4\}$。

将上述数据用于本文的推理算法进行攻击实例推理,可得 d_{a2} 命题的 $w_{a2}=0.7$,说明攻击者提升了攻击权限,并且该节点以 0.7 的高可信度对后续攻击起促进作用;d_{b2} 命题的 $w_{b2}=0.63$,说明主机被植入僵尸程序,可信度为 0.63;命题 d_{c2} 的 $w_{c2}=0.567$,说明目标主机处于 DDoS 的攻击状态,可信度为 0.567。

4　结束语

本文提出了一种基于双枝模糊逻辑和着色 Petri 网的网络攻击模型,该模型的知识表示具有网络模型简明、容易实现的特点,对于处理网络攻击中的不确定知识具有一定的优势。从攻击和防御两方面对网络攻击进行综合考虑分析,并给出了 BBFCPN 模型的推理规则和推理算法。基于 BBFCPN 模型的推理算法不仅推理过程简单直观,而且还具有并行推理能力。实验结果表明,该模型能清晰表示网络攻击和防御情况,推理算法是有效可行的。

参考文献:

[1] 任丹丹,杜索果. 一种基于攻击树的 VANET 位置隐私安全风险评估的新方法[J]. 计算机应用研究, 2011, 28(2):728-732.

[2] 吴金宇,金舒原,杨智. 基于网络流的攻击图分析方法[J]. 计算机研究与发展, 2011, 48(8):1497-1505.

[3] 冯萍慧,连一峰,戴英侠,等. 面向网络系统的脆弱性利用成本估算模型[J]. 计算机学报, 2006, 29(8):1375-1381.

[4] 陈锋,刘德辉,张怡,等. 基于威胁传播模型的层次化网络安全评估方法[J]. 计算机研究与发展, 2011, 48(6):945-954.

[5] 黄光球,赵阿妮,任大勇. 用双枝模糊逻辑和模糊 Petri 网构建的攻击模型[J]. 计算机工程与应用, 2010, 46(2):99-103.

[6] 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.

[7] 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, 107.

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