第32卷 第14期 计 算 机 工 程 2006年7月
Vol.32 № 14 Computer Engineering July 2006
·安全技术· 文章编号：1000—3428(2006)14—0119—03 文献标识码：A 中图分类号：TP393.08

基于规则推理的FPN误用入侵检测方法

张白一[1]，崔尚森[1,2]
（1. 长安大学信息工程学院，西安 710064；2. 西安交通大学电信工程学院，西安 710049）

摘 要：针对网络入侵攻击活动的模糊性，提出了一种基于模糊推理的模糊Petri网（FPN）误用入侵检测方法。该方法定义了一个六元组FPN，并将模糊产生式规则精化为两种基本类型。在此基础上给出了FPN表示模糊规则的模型、推理过程和基于FPN的推理算法。最后通过入侵检测的实例对该方法的正确性和有效性进行了验证，结果表明该方法推理过程简单直观、容易实现，而且具有并行推理能力，可适用于大规模的FPN模型，是误用入侵检测技术的一种非常有效的解决方案。

关键词：入侵检测；模糊Petri网；模糊推理

An Intrusion Detection Method Based on Reasoning Fuzzy Petri Net

ZHANG Baiyi[1], CUI Shangsen[1, 2]
(1. College of Information and Engineering, Chang'an University, Xi'an 710064;
2. School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049)

【Abstract】 According to the characteristics of the concurrence of network intrusion and the uncertainty of an attack action, a kind of intrusion detection method based on fuzzy Petri net model is extracted to express the knowledge and the reasoning rules. Firstly, the paper defines 6-tuple as the fuzzy Petri net structure. Secondly, two basic types of the fuzzy production rules are extracted from a number of practical rules. And then a fuzzy reasoning algorithm is programmed. Using a practical instance to test the algorithm at the last, the results show that the algorithm is simple, high-powered and universal. Specially, it has parallel reasoning ability and fits reasoning for the large-scale FPN model. It is an efficient method for intrusion detection.

【Key words】 Intrusion detection; Fuzzy Petri nets; Fuzzy reasoning

网络入侵检测系统从检测方法上分为误用入侵检测和异常入侵检测。基于规则的检测方法是误用入侵检测中的一种，其基本原理是运用人工智能技术收集非正常操作的特征，建立规则库，从以往的攻击入侵活动中归纳识别出对应的入侵模式，并将这些入侵模式存放于规则库中，然后将系统现有的活动与规则库中的规则进行模式匹配，从而判断是否有入侵行为发生。

模糊Petri网(FPN)是构造模糊产生式规则的良好图形建模工具，由于Petri网对知识表示和推理的独特优点，人们将Petri网用于表示产生式规则库[1]。1988年Looney C G提出了用模糊Petri网表示模糊产生式规则[2]。1990年Chen S M等人提出了基于Petri网可达图的模糊推理算法[3]，但该算法基本上是一种搜索过程，没能充分运用Petri网提供的并行推理能力，文献[2, 3]缺乏通用性。此外，文献[2～7]所描述的Petri网模型也比较复杂，提出的某些FPN推理规则也存在一定的缺陷，为后继的推理带来了困难，限制了其应用。

本文针对攻击入侵活动的模糊性，结合模糊Petri网对知识表示和推理的独特优点，提出了一种基于模糊推理的模糊Petri网(FPN)误用入侵检测方法。该方法将模糊产生式规则精化为两种基本类型，并用数据表来存储模糊产生式规则，在此基础上实现了基于FPN的推理算法。最后，通过入侵检测实例验证了该方法的正确性和高效性。

1 模糊规则库的模糊Petri网表示

1.1 模糊产生式规则

网络入侵活动具有很大的随机性和模糊性，是无法用精确的形式来表达的。模糊产生式规则刻画了多个命题之间的模糊关系，很适合表达这类模糊的或不确定的知识。本文定义的模糊产生式规则的一般形式如下：

类型 1 IF p_1 AND p_2 AND…AND p_n THEN p_k (CF=μ),w_1,w_2,…,w_n,w_k

类型 2 IF p_1 OR p_2 OR…OR p_n THEN p_k (CF=μ), w_1,w_2,…,w_n,w_k

其中，p_i为条件命题或结论命题；w_i为命题的规则强度；μ为规则的置信度。

文献[2～4]给出的规则类型为3类，本文将他们提出的形如

IF p_1 THEN p_2 AND p_3 (CF=μ)),w_1,w_2,w_3

的这类模糊推理规则分解为

IF p_1 THEN p_2 (CF=μ),w_1,w_2和IF p_1 THEN p_3 (CF=μ), w_1,w_3

这样的两条或多条规则，这样做的好处是降低了后继推理工作的难度。

1.2 模糊Petri网模型定义

在模糊Petri网模型定义中，对于不同的应用，网的构成和构成元素的定义均不相同[3,4,6]。本文结合上述模糊产生式规则建立的模糊Petri网通用模型如下：

定义 1 基于模糊产生式规则的Petri网的结构为一个六元组：FPN=(*P, T, I, O, F, W*)。其中：

作者简介：张白一(1955—)，女，副教授，主研方向：人工智能技术；崔尚森，副教授、博士生

收稿日期：2006-02-09 **E-mail：**byzhang@chd.edu.cn

$P=\{p_1,p_2,...,p_n\}$是库所的有限集合，n>0 为库所的个数；

$T=\{t_1,t_2,...,t_n\}$是变迁的有限集合，m>0 为变迁的个数；

$P\cap T=\phi$(空集)；

$I: P\rightarrow T$ 是输入函数，表示从库所到变迁的映射；

$O: P\rightarrow T$ 是输出函数，表示从变迁到库所的映射；

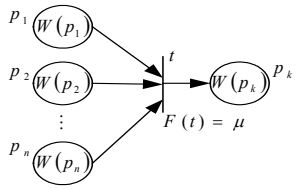
$F: T\rightarrow[0,1]$表示变迁的可信度函数，映射变迁到一个 0～1 之间的实际值，$F(t_j)=\mu_j\ (j=1,2,\ldots,m)$；

$W: P\rightarrow[0,1]$表示库所p_i的可信度函数，映射库所到一个 0～1 之间的实际值，$W(p_i),\ (i=1,2,\ldots,n)$。

定义 2 若$p_j\in I(t_i)$，$t_i\in T$,则从库所p_j到变迁t_i之间有一条有向弧，是变迁t_i的输入弧，p_j是变迁t_i的输入库所。若$p_j\in O(t_i)$，$t_i\in T$,则从变迁t_i到库所p_j之间有一条有向弧，是变迁t_i的输出弧，p_j是变迁t_i的输出库所。

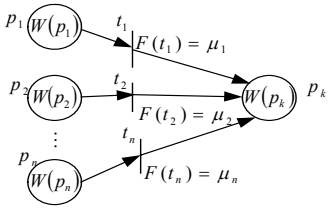
1.3 模糊推理规则的 FPN 描述

FPN 的每一个变迁对应一个规则，变迁的输入库所是规则的前提条件，变迁的输出库所是规则的结论。变迁的一个映射函数对应规则的可信度，库所中的标记值对应规则中命题的可信度，规则的匹配成功与 FPN 中变迁的发生对应。根据定义 1 和定义 2，可以将 1.1 节提出的两类模糊推理规则用如图 1、图 2 所示的 FPN 模型来表达。



$$W(p_k)=MIN(W(p_1),W(p_2),\ldots,W(p_n))*F(t)$$

图1 第1类模糊产生式规则的模糊推理过程



$$W(p_k)=MAX(W(p_1)*F(t_1),W(p_2)*F(t_2),\ldots,W(p_n)*F(t_n))$$

图2 第2类模糊产生式规则的模糊推理过程

2 FPN 模糊推理算法

我们提出的模糊推理算法采用模糊正向推理方法，即从条件命题到结论命题的推理过程。完整的算法包括 FPN 数据表结构，与算法有关的集合的定义，输入、输出信息和推理过程。现将整个算法分别描述如下：

2.1 FPN 的数据表结构

文献[3,4,7]的 FPN 模糊推理算法是通过建立数据表进行推理的。其中，文献[3,4]需要建立两个数据表：一个表中给出库所的立即可达和可达集合；另一个表给出相邻库所信息。文献[7]虽然只建一个数据表，但要给出变迁的立即可达输入库所和立即可达输出库所，并且还要给出变迁的可达输出库所集合。系统的规则越复杂，要求输入的信息(尤其是输入可达集合)也就越多，出错的机率也就越大，因此，文献[3,4,7]给出的推理算法也比较复杂。

本文给出的FPN模糊推理算法也是通过建立数据表进行推理的，与文献[3,4,7]数据表不同的是：只建立一个数据表，这张表中包含下述 3 类信息：(1)变迁(t_i)的映射函数值F(t_i)；(2)变迁的立即可达输入库所(BP(t_i))；(3)变迁的立即可达输出库所(FP(t_i))。具体内容由定义 3 给出。

定义 3 设p_j为一个库所，t_i为一变迁，如果$p_j\in I(t_i)$，则称p_j为t_i的立即可达输入库所。所有立即可达输入库所的集合称为t_i的立即可达集合，记为BP(t_i)；如果$p_j\in O(t_i)$，则称p_j为t_i的立即可达输出库所。所有立即可达输出库所的集合称为t_i的立即可达集合，记为FP(t_i)。

根据定义 3 将图 1、图 2 所示 FPN 的推理过程模型映射到如表 1 所示的数据表上。

表 1 FPN 数据表样式

类型	F(t_i)	BP(t_i)	FP(t_i)
1	u_1	$\{p_1,p_2,\ldots p_n\}$	$\{p_k\}$
2	u_2	$\{p_1\}$	$\{p_k\}$
	u_3	$\{p_2\}$	$\{p_k\}$
	…	…	$\{p_k\}$

可以看出，数据表比文献[3,4,7]给出的数据表要简单得多。此外，由于将各种规则简化为两种类型，因此任何一个变迁的立即可达输出库只有一个，这样就为下一步的推理提供了方便。分析此表不难发现，在类型 1 规则下t_1变迁的FP值只有一个，而在类型 2 规则下t_i变迁的FP值将是多个。在后面论述的推理中将用到此特点。

2.2 定义与算法有关的集合

(1)定义 wpn 集合，用来存放所有库所名及库所的可信度值，存放格式为

wpn={p_1,w(p_1), p_2,w(p_2),…,p_n,w(p_n)}

(2)定义 tbf 集合，用来存放 FPN 数据表的变迁的映射函数值，变迁的立即可达输入库所名和立即可达输出库所名，存放格式为

tbf={F(t_1),{BP(t_1)},FP(t_1),F(t_2),{BP(t_2)},FP(t_2), …,F(t_m),{BP(t_m)},FP(t_m)}

其中{BP(t_i)}表示由一个或多个库所组成，根据FPN数据表而定；

(3)定义 KNS 集合，用来存放开始库所名集合和已知可信度的库所名，存放格式为

KNS={开始库所名集合，已知可信度的库所名}，例：KNS={$p_{s1},p_{s2},\ldots,p_{ss},p_{a1},p_{a2},\ldots,p_{at}$}

2.3 推理算法

2.3.1 算法的输入

(1) 输入库所名p_i与库所的可信度值w(p_i)，i=1,2,…,n到wpn集合中，若w(p_i)未知，则令w(p_i)=0；

(2) 输入相应的变迁值u_j和库所名p_j到tbf集合中；

(3) 输入已知w(p_i)的开始库所名集合到KNS中。

2.3.2 算法的输出

算法的输出是目标库所的库所名及可信度值。

2.3.3 推理过程

```
k←1;
while(true)
{取出 KNS 中的第 k 个库所名 ps；
if ps=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tbf集合中的ti的个数
if ps∈BP(ti)   //BP(ti)∈tbf
{ pg←FP(ti); //FP(ti)∈tbf
   wpg←w(ps)*F(ti); //w(ps)∈wpn
   if   w(pg)=0 //w(pg)∈wpn
w(pg)←wpg; //当 w(pg)是一个未知值时
else if   FP(tj)中pg的个数=1 //FP(tj)∈tbf,j=1,2,…,m
w(pg)←min(wpg,w(pg)); //当库所是规则类型 1 形成的与库所时
```

else w(pg)←max(wpg,w(pg));
//当库所是规则类型 2 形成的或库所时
if pg ∉ KNS 将 pg 插入到 KNS 集合的结束标志前；
}
k←k+1;
}//endwhile

3 实例分析

对于网络入侵检测来说，入侵模式规则库是产生式规则库的一种实例。规则条件包含规则的操作、协议、源 IP 地址和目标 IP 地址及其网络掩码和端口等；规则结论包括报警信息及需要检测的模式信息等。这里使用文献[5]提供的端口扫描攻击与后门攻击的规则抽象成如下规则：

R1(t_1): IF p_1 AND p_2 AND p_3 AND p_4 THEN p_{15} (CF=0.95), 0.8,0.9,0.95,0.78,0

R2(t_2): IF p_{18} AND p_5 AND p_6 AND p_7 AND p_8 THEN p_{16} (CF=0.98),0,1,1,1,1

R3(t_3): IF p_9 AND p_{10} AND p_{16} AND p_{18} THEN p_{17} (CF= 0.97),0.9,1,0,0

R4(t_4): IF p_{11} AND p_{12} AND p_{13} AND p_{14} THEN p_{18} (CF= 0.92),1,0.86,0.82,1

以上规则的模糊 Petri 网的表示如图 3 所示，相应的 FPN 数据表见表 2。

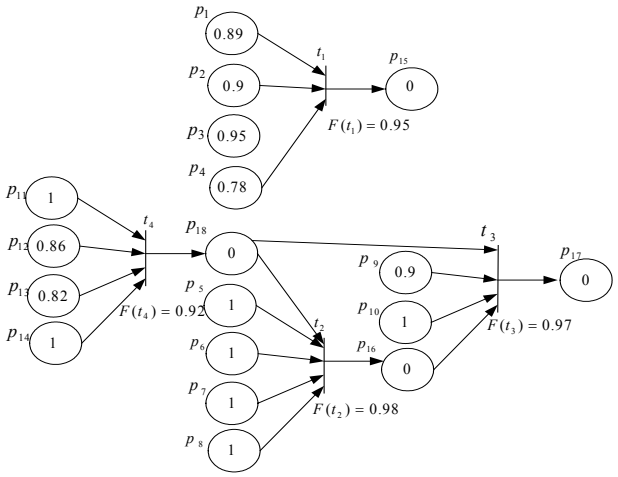


图 3 端口扫描攻击与后门攻击的 FPN 表示

表 2 端口扫描与后门攻击数据

$F(t_i)$	$BP(t_i)$	$FP(t_i)$
0.95	$\{p_1, p_2, p_3, p_4\}$	$\{p_{15}\}$
0.98	$\{p_5, p_6, p_7, p_8, p_{18}\}$	$\{p_{16}\}$
0.97	$\{p_{18}, p_9, p_{10}, p_{16}\}$	$\{p_{17}\}$
0.92	$\{p_{11}, p_{12}, p_{13}, p_{14}\}$	$\{p_{18}\}$

将上述数据用于我们的推理算法进行攻击实例推理，可得：p15 库所的 W(p15)=0.741，说明输出端口扫描攻击发生的可能性为 0.741，p18 库所的 W(p18)=0.754，说明利用口令猜测获得普通用户权限攻击发生的可能性为 0.754；p17 库所的 W(p17)=0.717，说明放置后门攻击的可能性为 0.717；p16 库所的 W(p16)=0.739，说明利用 mail 组件漏洞获得 root 权限攻击发生的可能性为 0.739。

4 结论

为了对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性，本文给出了一种基于 FPN 的模糊推理的误用入侵检测方法。该方法的特点如下：(1)将大量的模糊产生式规则划归为两种基本类型，并用这两种基本类型代替了文献[2～4]提出的复杂模糊产生式规则。(2)建立了模糊产生式规则的模糊 Petri 网通用模型，解决了文献[2～5]提出的这类模型的复杂性问题及文献[2,3]给出的这类模型不通用的问题。(3)实现了基于 FPN 数据表的推理算法。该算法的推理过程不仅简单直观，而且还具有并行推理能力。

通过入侵检测实例验证，结果表明该方法是网络安全系统中误用入侵检测技术的一种非常有效地解决方法。

参考文献

1 Zisman M D. Use of Production Systems for Modelling Asynchronous Concurrent Processes[M]. London: Academic Press, 1978: 53-68.

2 Looney C G. Fuzzy Petri Nets for Rule-based Decision Making[J]. IEEE Trans. on Syst., Man., 1988, SMC-18(1): 178-183.

3 Chen S M, Ke J S, Chang J F. Knowledge Representation Using Fuzzy Petri Nets[J]. IEEE Trans. on Knowledge and Data Engineering, 1990, 2(3): 311-319.

4 江志斌. Petri 网服及其在制造系统建模与控制中的应用[M]. 北京: 机械工业出版社, 2004.

5 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): 130-132.

6 Xin Jianqiang, Dickerson J E, Dickerson J A. Fuzzy Feature Extraction and Visualization for Intrusion Detection[C]. Proc. of the 12th IEEE International Conference on Fuzzy Systems, 2003-05-25, 2: 1249-1254.

7 Yang Rong, Leung W S, Heng P A, et al. Improved Algorithm on Rule-based Reasoning Systems Modeled by Fuzzy Petri Nets[C]. Proceedings of the IEEE International Conference on Fuzzy Systems, 2002-05-12, 2: 1204-1209.

（上接第 118 页）

参考文献

1 Harn L. Efficient Sharing(Broadcasting) of Multiple Secret[J]. IEE Proc. of the Comput. Digit. Tech., 1995, 143(3): 237-240.

2 Lin T Y, Wu T C. Threshold Verifiable Multisecret Sharing Scheme Based on Factorization Intractability and Discrete Logarithm Modulo: A Composite Problems[J]. IEE Proc. of the Comput. Digit. Tech., 1999, 146(5): 264-268.

3 He W H, Wu T S. Comment on Lin-Wu Threshold Verifiable Multisecret Sharing Scheme[J]. IEE Proc. of the Comput. Digit. Tech., 2001, 148(3): 139.

4 Chang T Y, Hwang M S, Yang W P. An Improvement on The Lin-Wu Threshold Verifiable Multi-secret Sharing Scheme[J]. Applied Mathematics and Computation, 2005, 163(1): 169-178.

5 张福泰，张方国，王育民. 一个安全高效的广义可验证秘密分享协议[J]. 软件学报, 2002, 13(7): 1187-1192.

6 张福泰，王育民. 无条件安全的广义可验证秘密分享协议[J]. 计算机研究与发展, 2002, 39(10): 1199-1204.