第 29 卷 第 1 期
2014 年 2 月

天津科技大学学报
Journal of Tianjin University of Science & Technology

Vol. 29 No. 1
Feb. 2014

DOI:10.13364/j.issn.1672-6510.2014.01.014

基于 Petri 网的病毒攻击建模

侯仁平，李孝忠
（天津科技大学计算机科学与信息工程学院，天津 300222）

摘 要：针对威胁计算机网络安全的病毒攻击行为，建立了基于 Petri 网的病毒入侵网络基本模型，利用 CPN tools 仿真工具分析了模型的活性和各个库所的有界性，以利于采取有效的网络防御措施和建立安全的防御体系. 利用安全策略域、域间通信信道的概念，根据病毒入侵传播的特性，建立了基于随机着色 Petri 网的企业网络模型，并给出了用该模型模拟与安全相关网络行为的方法.

关键词：病毒攻击；Petri 网；随机着色 Petri 网
中图分类号：TP391.9 **文献标志码**：A **文章编号**：1672-6510(2014)01-0069-06

A Model of Virus Attacks Based on Petri Nets

HOU Renping, LI Xiaozhong
(College of Computer Science and Information Engineering, Tianjin University of Science & Technology, Tianjin 300222, China)

Abstract: Virus attacks increasingly threaten the computer network. A preliminary model of virus invasion was established based on Petri net, and the activity of the model and the bounds of different places were analyzed by using CPN simulation tools. This model will help to adopt effective defense measures for the network and establish defense systems. Using the concepts of security policy domain and the communication channels of domain, and according to the characteristics of the dissemination of the virus invasion, a model of enterprise network was established based on the stochastic colored Petri net, and the network behavior related to security with this model was introduced in detail.

Key words: virus attacks; Petri net; stochastic colored Petri net

随着计算机网络的普及，计算机病毒攻击等入侵行为日益突出，对网络的安全构成极大威胁. 要增强互联网抵御病毒入侵的能力，就有必要深刻理解计算机病毒在互联网中的传播机理. 在充分认知互联网的复杂网络特性基础上，建立病毒入侵的数学模型并分析其传播机理，是计算机病毒[1]研究的一个重要组成部分.

目前，检测网络入侵有多种方法，如基于模式匹配、基于概率统计和基于神经网络的入侵检测方法等[2]，但是都需要一定的方法来描述网络事件，许多建模方法是基于事件的，缺乏对系统状态的明确体现，而 Petri 网基于状态的建模方法明确定义模型元素的状态，其演进过程受状态的驱动，不但严格区分了活动的授权和活动的执行，而且使过程定义具有更丰富的表达能力，能够动态地修改过程实例，使建模过程具有了更多的柔性特征[3].

本文讨论了如何利用安全域和域间通信信道概念在复杂网络中应用着色随机 Petri 网来建模和模拟安全问题，并在简化系统模型和丰富模型约束条件方面做一些有益的尝试.

1 Petri 网基础

1.1 Petri 网

1962 年，Petri[4]首次提出 Petri 网的概念. 经典 Petri 网包括 3 种节点类型：库所、变迁和有向弧，同时其动态效果由令牌等元素展现.

收稿日期：2013–06–08；**修回日期**：2013–07–12
基金项目：国家自然科学基金资助项目(61070021)；天津市高等学校科技发展基金资助项目(20120803)
作者简介：侯仁平（1985—），男，山东人，助理工程师，硕士研究生；**通信作者**：李孝忠，教授，lixz@tust.edu.cn.

Petri 网是一种系统的数学和图形的建模和分析工具，特别适用于对具有同步、并发、冲突的离散事件系统进行建模和分析，具有较为完善的数学表达. 应用 Petri 网相关技术及其分析方法，能够分析网系统静态的结构以及仿真时动态的行为，因而广泛应用于复杂系统的设计和分析中. 网络模型建模是 Petri 网的重要应用之一.

经典 Petri 网也有其局限性：(1)它没有数据概念，因此其所构造的模型往往变得很庞大；(2)它没有等级概念，对结构中采用自顶向下或自底向上的分析方法构成了很大的局限性.

1.2　着色 Petri 网

20 世纪 80 年代，Jensen[5]在经典 Petri 网基础上提出和发展了具有层次结构的着色 Petri 网理论(colored Petri net，CPN)，并在不破坏经典 Petri 网的理论完整性前提下解决了经典 Petri 网的两大局限性. 它具有三大优点[6]：(1)CPN 理论在描述系统静态模型方面进行了比较完整的形式化定义；(2)CPN 有机地结合了层次分解以及数据结构，能同时用于评估系统性能、逻辑的正确性和验证系统功能；(3)它还能交互地或自动地进行仿真.

CPN 与经典 Petri 网的主要区别是：(1)CPN 为库所和变迁关联了对应的色彩集合 C，在为网系统引入相关颜色集后，托肯标记的不同颜色可以用来表示为任意不同复杂的数据类型，丰富了 Petri 网的语义；(2)使经典 Petri 网更加具有层次性，可以自顶向下或自底向上来建立复杂模型，从而 CPN 这类功能强大的建模工具可以用来处理大型的应用模型.

图 1 是一个简单的 CPN 模型，其中两个库所 P_1 和 P_2 具有相同的颜色值，其只有两种状态 true 或 false. 库所 1 的起始标记表示当前库所具有唯一的一个 true 托肯，变迁 T 的输入弧和输出弧具有相同颜色“true”. 因此，此种状态下变迁可以发生，发生后得到新的系统状态.

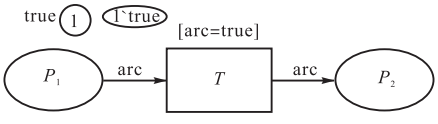

图 1　简单着色 Petri 网

Fig. 1　Simple CPN

1.3　随机 Petri 网

传统的 Petri 网一般没有时间参数，为了进行分析，需要建模时间、延迟等参数，在传统 Petri 网基础之上加入时间参数，因此每一个令牌拥有一个时间戳，变迁决定生产出的令牌的延迟，即随机 Petri 网[7](stochastic Petri net，SPN)，大大增强了模拟能力.

在 SPN 理论中，变迁实施延迟由随机变量描述，它分为离散变量和连续变量两类，然而随机变量均可定义多种函数，一般情况下离散时间类型随机变量为几何分布，连续时间类型随机变量为指数分布.

Molly、Florin 和 Natkin 等人独立提出把变迁与随机的指数分布实施延迟联系起来的思想[8]. 变迁实施分为三步：清除输入位置标记；实施延迟内变迁“保持”这些标记；标记移到变迁输出库所. 在指数分布的随机变量关联的变迁中，系统状态的延迟也是指数分布的随机变量.

在随机 Petri 网建模的过程中，时间变迁通常都和某个指数分布的速率一一对应，并且同时设定了时间变迁在模拟某个活动时所具备的平均处理速率. 随机 Petri 网中的每一个活动都和时间变迁一一对应，所有活动都能够并行执行互不干扰，一直到活动完成. 因此，随机 Petri 网很好地避免了死锁的发生.

图 2 是一个简单的随机 Petri 网模型，库所 P_1 的起始标记表示当前库所有唯一的一个托肯，变迁 T 有一个时间参数 T_0，取值是指数分布的随机参数 t_0，此时变迁的发生受时间参数的控制，在时间合适时变迁才会发生，托肯值由库所 P_1 移动至库所 P_2.

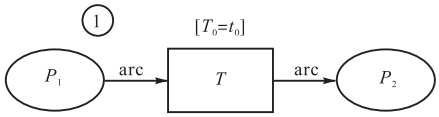

图 2　简单随机 Petri 网

Fig. 2　Simple SPN

2　安全相关的网络模型建模

2.1　安全策略域

在企业级网络安全建模过程中，需要定义系统以某种方式或样式以表示状态和状态变迁，为了这个目的 Peter Stephenson 较早的在建模进程中引入安全策略域[9]概念.

在建模过程中，如果把每个设备都单独考虑，由于网络环境的高度复杂性，其建模任务必将是不可接受的艰巨任务. 为了实现建模并大大减轻建模任务的工作量，应用安全策略域是很好的方法. 安全策略域包含所有受制于同种安全策略的设备的集合，可以认为这是数据分类方法的一种扩展实例，但是在某种程度上又具有一些更为精细的规模.

2.2　域间通信信道

当模拟网络系统中的安全行为时，为了达到建模的目的，Peter Stephenson 同时提出域间通信信道概念. 域间通信信道可以帮助建模域间的通信流程和甄别被禁止的通信行为.

2.3　网络模型

从实际应用角度来看，可以用库所来表示安全策略域，而用变迁来表示域间通信信道. 既然变迁描述网络的行为，在变迁的发生上设置适当的约束条件，就意味着在变迁的输入库所和输出库所之前的通信上应用约束条件. 由此，尽管网络看起来十分地复杂，实际上如此网络建模[10]就变得十分的直观和相当地简单.

3　基于 Petri 网的网络建模

3.1　库所和变迁的确定

在网络建模中，用库所来表示安全策略域，库所表示系统状态，因此在建模中的库所状态也就是安全策略域.

在建模中，使用变迁来表示域间通信信道，因为域间通信信道的行为决定着安全策略域（库所）与其他安全域之间的可达性. 在信道得以授权的情况下，从输入库所到输出库所之间可达.

3.2　约束条件的确定

3.2.1　着色约束

变迁是否授权视为约束条件，也就是其颜色设定为布尔型. 颜色为 true 或无时，变迁发生没有任何限定因素.

变迁发生，输入库所托肯流动到输出库所，也就是系统状态发生了变化，这种状态的变化通过输入和输出库所托肯的增减显现出来. 在模型中，变迁发生即认为该库所被病毒感染，而此时系统状态经历了由先前状态到新状态的变化，变化的发生完全建立在两库所间的通信被授权的前提上.

3.2.2　时间约束

变迁的时间因素也不得不视为约束条件，此处将其时间变量设定为服从指数分布特性.

病毒[11]具有潜伏性、隐蔽性和可触发性，因此时间因素的引入至关重要，其特性决定使用随机性对其描述更加恰当. 而且在实际运用随机 Petri 网建模过程中，一般时间变迁都与某个指数分布的速率一一对应，同时设定了时间变迁在模拟某个活动时所具备的平均处理速率. 在分布环境中的每一个活动都会和每一个时间变迁相对应，所有活动都能够并行执行，一直到活动的完成. 因为有随机时间的延迟，所以一般不可能发生活动之间的时间冲突，不需要对随机 Petri 网设置特殊机制来解决各个事件活动之间的冲突问题. 由此可见，时间因素的引入不仅是由网络病毒特性的客观需要，同时也能更好地描述网络模型并避免并发冲突的问题.

另外，随机 Petri 网给每个变迁赋予了一个随机的延迟时间，其状态空间同构于一个连续时间的马尔可夫链，结合马尔可夫过程的分析和计算方法，可为模型的数学评价和性能分析提供很好的途径.

4　实　例

4.1　建模

以中等规模企业网络为建模背景，以简化网络建模工作为主要目的进行建模，并以此作为网络分析的重要描述手段之一，利用CPN tools 软件建立模型，如图 3 所示. 图中将病毒单独列为库所 P_1，病毒的感染列为变迁 P_2，同时将初始托肯值设置为 1，病毒起源和数目不确定，故假定为自然数1 以做简单仿真之用.

库所的含义如下：P_1 为病毒源；P_2 为公共因特网；P_3 为内部无线网；P_4 为外部系统互联区；P_5 为隔离缓冲区；P_6 为内部系统互联区；P_7 为核心区.

变迁的含义如下：T_1 为染毒途径；T_2 为隐秘途径；T_3 为公共因特网与隔离缓冲区间信道；T_4 为隔离缓冲区与内部系统互联区信道；T_5 为内部系统互联区与核心区信道；T_6 为外部系统互联区与内部系统互联区信道；T_7 为内部无线网与内部系统互联区信道；T_8 为内部系统互联区与外部系统互联区信道；T_9 为内部系统互联区与内部无线网信道；T_{10} 为核心区与内部系统互联区信道；T_{11} 为内部系统互联区与隔离区信道；T_{12} 为内部系统互联区与公共因特网信道. 标记 p、ph、PH 均为颜色标记.

表 1 中列出了模型中具体变迁的前集和后集的详细情况. 其中，P_1 是为描述病毒来源而单独设立的库所，不属于安全策略域的概念范畴，另外，T_1、T_2 染毒设备变迁仅为描述病毒的存在对象而设立的变迁，亦不属于域间通信信道的概念范畴. 模型中，此两处为例外.

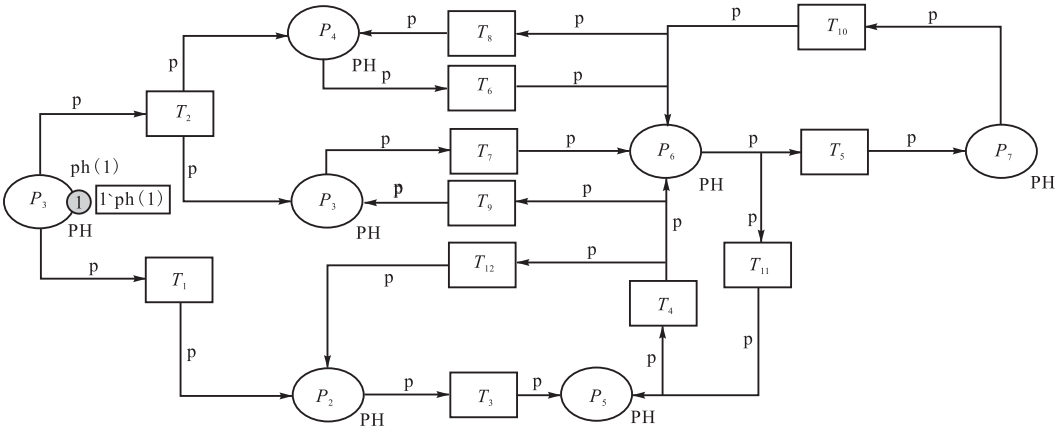

图 3　着色随机 Petri 网模型

Fig. 3　Stochastic colored Petri net model

表 1　变迁的前集和后集

Tab. 1　Preset and postset of transition

变迁	前集	后集	变迁	前集	后集
T_1	P_1	P_2	T_7	P_3	P_6
T_2	P_1	P_3,P_4	T_8	P_6	P_4
T_3	P_2	P_5	T_9	P_6	P_3
T_4	P_5	P_6	T_{10}	P_7	P_6
T_5	P_6	P_7	T_{11}	P_6	P_5
T_6	P_4	P_6	T_{12}	P_6	P_2

建立的模型中，初始状态较为简单. 在病毒源库所假定存在 1 个 true 颜色的托肯，代表网络中有 1 个病毒源处于被感染状态. 模型中各个弧和变迁初始设置均为 true 颜色，也就是模拟最简单的不带任何安全设备和策略的网络环境，各个信道所代表的变迁都满足变迁发生的条件，在网络环境中存在安全设备或者授权不足时，相应的颜色将会设置为 false，代表变迁不满足发生的条件. 该模型中，托肯并不是简单地在网络模型中流动，托肯在特定位置出现代表该处已被病毒感染. 在仿真应用中，可以通过设定不同的颜色约束来模拟和仿真繁杂的网络信息流情况.

4.2　有界性与活性分析

利用CPN tools 仿真软件中的 State Space 模块生成模型报告文档，得出所有库所托肯值至多为 2，模型各个库所都是有界的，符合建模实际要求，有界性分析结果如表 2 所示.

表 2　有界性分析

Tab. 2　Bounds analysis

最优整数界	上界	下界	最优整数界	上界	下界
P_1	1	0	P_5	2	0
P_2	2	0	P_6	2	0
P_3	2	0	P_7	2	0
P_4	2	0			

另外，模型中也不存在死标识，所有变迁除 T_1 和 T_2 外均是活的，活性分析结果如表 3 所示.

表 3　活性分析

Tab. 3　Activity analysis

活性情况	分析结果
Dead Markings	None
Dead Transition Instances	None
Live Transition Instances	$T_3, T_4, \cdots, T_{12}$

4.3　基于马尔可夫过程的性能分析

本文选取模型的子系统(图 4)来进行马尔可夫过程分析，与其同构的马尔可夫模型如图 5 所示.

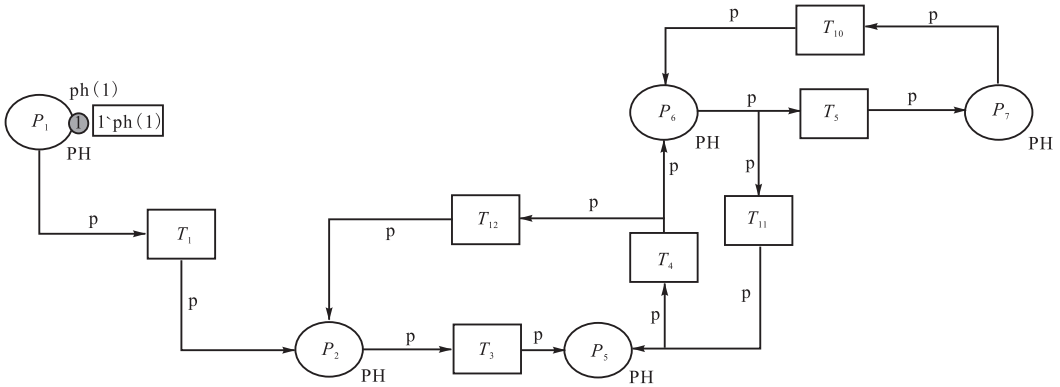

图 4　着色随机 Petri 网模型子系统

Fig. 4　Stochastic colored Petri net model subsystem

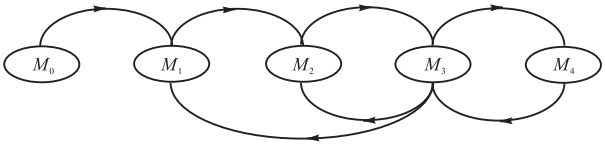

图 5　MC 模型

Fig. 5　MC model

根据连续时间的随机 Petri 网同构于连续时间马尔可夫链的特性，与模型同构的马尔可夫链的状态可达标识见表 4，数字“0”或“1”表示库所中的托肯数.

表 4　状态可达标识

Tab. 4　Reachable state marking

可达标识	P_1	P_2	P_5	P_6	P_7
M_0	1	0	0	0	0
M_1	0	1	0	0	0
M_2	0	0	1	0	0
M_3	0	0	0	1	0
M_4	0	0	0	0	1

模型中托肯无拥塞，无瓶颈，也不存在死锁. 故模型合理.

取λ = {2，1，2，1，1，1，2}，列出平衡状态方程，可得方程组

$$\begin{cases} 2X_0 = 0 \\ X_1 = 2X_0 + 2X_3 \\ 2X_2 = X_1 + X_3 \\ 4X_3 = 2X_2 + X_4 \\ X_0 + X_1 + X_2 + X_3 + X_4 = 1 \end{cases}$$

解此方程组可得各个状态稳定概率(取值保留 4 位有效数字)：$P[M_0] = 0 = X_0$，$P[M_1] = 0.363\,6 = X_1$，$P[M_2] = 0.272\,7 = X_2$，$P[M_3] = 0.181\,8 = X_3$，$P[M_4] = 0.181\,8 = X_4$.

在求得稳定概率的基础上还可以进一步分析模型的其他性能，如标记密度函数、变迁利用率、变迁标记流速等.

4.4　模型仿真

使用 CPN tools 仿真软件进行仿真模拟，可以得到如图 6 所示的模拟效果图.

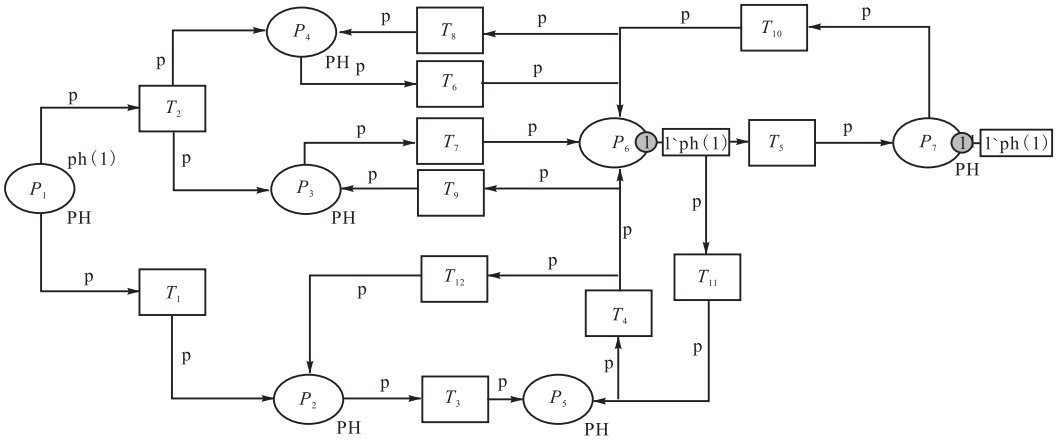

图 6　仿真效果

Fig. 6　Simulation result

通过图 6 仿真可以看出，在没有任何安全措施的情况下，图中各个库所均出现了病毒托肯，代表实际网络中各处均有感染病毒出现. 出于深度保护网络免于病毒感染的考虑，必须在病毒与潜在感染设备之间设置尽可能多的拦截设备或者策略. 此外，通过设定不同位置的变迁颜色 false，即加入相应安全措施后，与颜色 false 相对应的变迁后的库所就不再出现病毒感染，据此可以发现在网络中处于关键位置的节点和变迁，网络管理者需要对其重点关注和配置相应安全策略.

另外，通过仿真也验证了简化后的 Petri 网模型在描述网络信息流应用方面的巨大优势，同时证明了模型的合理与有效性.

5　结　语

本文通过引入安全策略域和域间通信信道的概念，结合着色和随机两大约束条件，进行有界企业级网络系统的简单网络模型系统建模. 由此，简化了网络系统模型的建模工程任务量，并为宏观分析网络系统提供了实例模型，同时也为更进一步地细化和深入研究奠定了理论基础.

今后，应逐步细化和深入探讨模型中的着色与随机两大特性，进一步深入了解和分析网络特性.

参考文献：

[1] 许丹，李翔，汪小帆. 复杂网络理论在互联网病毒传播研究中的应用[J]. 复杂系统与复杂性科学，2004，1(3)：10–26.

[2] White G B，Fish E A，Pooch U W. Computer system and network security[M]. Boca Raton，USA：CRC Press，1996：91–111.

[3] 张羽. Petri 网在入侵检测系统中的应用研究[D]. 西安：西安电子科技大学，2007.

[4] Petri C A. Kommunication mit automaten[D]. Bonn：Institutefur Instrumentelle Mathematik，1962.

[5] Jensen K. Colored petri nets and the invariant method[J]. Theoretical Computer Science，1981，14(3)：317–336.

[6] 袁崇义. Petri 网原理[M]. 北京：电子工业出版社，1984：12–75.

[7] Florin G，Fraize C，Natkin S. Stochastic Petri nets：Properties，applications and tools[J]. Microelectronics Reliability，1991，31(4)：669–697.

[8] 林闯. 随机 Petri 网和系统性能评价[M]. 北京：清华大学出版社，2000：19–40.

[9] 邱岚，谭彬. 安全域划分研究与应用[J]. 计算机安全，2012(6)：39–42.

[10] 唐圣学，陈丽，黄娇英. 关联复杂网络建模及辨识研究[J]. 计算机物理，2012，29(2)：308–316.

[11] 郭仁东. 计算机网络病毒及其防御探析[J]. 电脑知识与技术，2012，8(30)：7190–7198.

责任编辑：常涛

（上接第 68 页）

后下载(配置目标器件)到实验平台上. 用万用表(倍思特数字万用表 DT–9205，20 V 档，精确到小数点后 2 位)和本设计实现的数字电压表(精确到小数点后 3 位)检测并显示实验平台上 6 个测试点的电压值，结果见表 2. 测量的相对误差小于 3%.

表 2　万用表与本设计电压表对测试点的测量结果

Tab. 2　Measured voltages of the given test points with a multimeter and the new voltmeter

标称值/V	万用表		本设计	
	测量值/V	相对误差/%	测量值/V	相对误差/%
0.00	0.00	0.00	0.000	0.00
1.20	1.23	2.50	1.235	2.91
1.25	1.23	1.60	1.235	1.20
1.80	1.76	2.22	1.755	2.50
2.50	2.49	0.40	2.483	0.68
3.30	3.32	0.60	3.315	0.45

在测试中用万用表和本设计均检测出开发板上标称值为 1.2 V 的测试点与标称值为 1.25 V 的测试点电压值相同，可能是标称值有误. 另外，在 ISE10.1 的“Design Summary”窗口查看本设计占用资源的情况，其共占用 20 480 个 Slice Flip Flops(Slice 内部触发器)中的 19 个，占用 20 480 个 4 input LUTs(4 输入查找表)中的 77 个，占用资源小于 0.5%.

6　结　语

本文将 FPGA 与 TLV571 相结合设计的数字电压表能够对 0 ~ 3.3 V 的直流电压进行测量，最小分辨率为 0.013 V，其 FPGA 芯片资源占用率低，采用 4 位数码管显示被测电压值，可精确到小数点后 3 位. 通过实例和硬件测试验证了各种情况下 BCD 码加法运算的正确性；用 loop 循环语句编写 BCD 码加法运算的程序简洁明了，明显优于用 if 嵌套语句编程实现.

参考文献：

[1] 杨增汪，陈斯，戴新宇. 一种量程自动转换高精度数字电压表的设计[J]. 自动化与仪表，2011(11)：12–15.

[2] 翟永前，蒋芳芳. 基于 MSP430 单片机的智能数字电压表设计[J]. 化工自动化及仪表，2011，38(3)：297–300.

[3] 李奎霖. 基于 FPGA 的数字电压表设计[J]. 仪表技术，2010，12(10)：57–59.

[4] 路而红. 电子设计自动化应用技术：FPGA 应用篇[M]. 北京：高等教育出版社，2009.

[5] Azcondo F J，de Castro A，Brañas C. Course on digital electronics oriented to describing systems in VHDL[J]. IEEE Transactions on Industrial Electronics，2010，57(10)：3308–3316.

[6] Texas Instruments. TLV571 2.7 V to 5.5 V，1-Channel，8-Bit Parallel ADC[EB/OL]. 2000–02–09[2013–08–01]. http：// www.ti.com.cn/product/cn/tlv571.

责任编辑：常涛