一种基于有色 Petri 网的安全协议分析方法研究

苏桂平[1],孙 莎[2]
(1.中国科学院研究生院 信息科学与工程学院,北京 100049;
2.中国科学院研究生院 工程教育学院,北京 100049)

摘 要:利用有色 Petri 网建模工具 CPN tools 中的查询函数对安全属性进行描述,搭建一个能够覆盖大部分安全性质的 CPN 查询函数库,提出一种基于 CPN 的通用和规范的安全协议形式化分析语言,该语言可以像用面向对象编程语言编程一样对安全协议进行建模。

关键词:有色 Petri 网;安全协议;形式化分析;面向对象编程语言
中图分类号:TP393.02 文献标识码:A 文章编号:1674-7720(2011)15-0001-03

Research of security protocols analysis language based on coloured Petri net

Su Guiping[1], Sun sha[2]
(1.School of Information Science and Engineering, Graduate School of CAS, Beijing 100049, China;
2 (College of Engineering and Education, Graduate School of CAS, Beijing 100049, China)

Abstract: Using the query faction of CPN tool to describ the security attribute. Building a CPN query function database which contained the most security attribute. This paper presents a formal analysis language of security protocols which general and standardization based on CPN. This language can build the model of security protocols like as object-oriented-programming language.

Key words: coloured Petri net; security protocol; formal analysis; OOPL

如何在一个无法确定的操作环境下,保证计算机间传送信息的安全性,从而确保通信双方主体之间的"信任"以及通信数据的秘密和完整,其中安全协议对保障网络安全起到至关重要的作用。但一些著名的协议在使用了相当长的时间后,相继被发现存在有若干安全漏洞。由于安全协议的运行是处于某种不安全的环境中,很难用人工识别的方法来分析其安全性,必须借助形式化的分析方法或工具来完成。

关于安全协议的形式化分析,国内外学者基于不同的模型进行了不少有益的研究。如 Yasinsac 提出的通用安全协议分析语言 CPAL[1]、Millen 开发的通用认证协议说明语言 CAPSL[2]、李梦君等人用扩展 Horn 逻辑模型对安全协议进行分析和验证方法[3]、怀进鹏等人用代数模型来研究协议的安全性[4]、WE 等人基于有色 Petri 网 CPN(Coloured Petri Net)提出一种集成的安全协议分析模型[5]。

现有的方法大多针对个别协议进行分析,很少能够通用于大部分的安全协议,并且大部分的方法还停留在理论上,缺少自动分析的工具[6]。

本文利用 CPN tools 建模语言(CPN ML)中的查询函数对安全属性进行描述,然后对 CPN tools 工具在规范协议描述、简化协议建模、自动检测进行扩展三方面,搭建一个能够覆盖大部分安全性质的 CPN 查询函数库,提出一种基于 CPN 的通用和规范的安全协议形式化分析语言,该语言可以像用面向对象编程语言编程一样对安全协议进行建模。

1 基于 CPN 的安全协议

1.1 有色 Petri 网(CPN)理论研究

Petri 网是一种可用于多种系统的图形化、数学化建模工具,为描述和研究具有并行、异步、分布式和随机性等特征的复杂系统提供了强有力的手段。

作为一种图形化工具,可以把 Petri 网看作与数据流图和网络相似的方法来描述系统模型;作为一种数学化工具,它可以用来建立状态方程、代数方程和其他描述

系统行为的数学模型。

在 CPN 模型中，有色标志表示系统中不同的资源，同时每个位置都与特定的颜色集绑定，表示该位置中只能存放相应颜色的标志。在弧上和变迁上标注的条件表达式和运算函数是用于解释弧的权值、运算所用的颜色以及变迁触发的条件。

CPN tools 是一个专用于有色 Petri 网编辑、模拟和分析的工具，除了有强大的 CPN 分析工具外，它还有简洁紧凑的 CPN 图形编辑工具，几乎所有的 CPN 元素(除数据类型、变量申明外)都能在模型图中表示。

CPN 是将 Petri 网具有相似性质的元素分类，用不同颜色区分不同类别，每一种颜色用一种标识符号来表示，将某种属性赋予标记。

$CPN=(\sum,P,T,A,N,C,G,E)$，在 CPN 的一个状态 M 下，t 上的绑定元素(t,b)是可实施的，当且仅当：

$\forall p\in P,E(p,t)<b>\leqslant M(p)$。

若把 t 实施之后产生的后继状态定义为 M'，则：

$\forall p\in P,M'(p)=(M(p)-E(p,t)<b>)+E(t,p)<b>$

可以称作 M'是从 M 出发，经过(t,b)变迁是可达的，记为 $M\ [(t,b)>M'$。如果存在一个变迁 σ 序列使得 M 可以达到状态 M'，则记为 $M[\sigma>M'$，由 M 出发的所有可达状态的集合表示为$[M>$。

矩阵方程：

假定非负整数行向量 $\bar{q}$ 是 q 的动作实施计数向量，则有：

$M=M_0+C^{T}\times\bar{q}$

其中，矩阵 $C=\lfloor c_{ij}\rfloor(1\leqslant i\leqslant n,1\leqslant j\leqslant m)$ 是 CPN 的关联矩阵，$c_{ij}=W_{tj,si}-W_{si,tj}$、$W_{tj,si}$ 和 $W_{si,tj}$ 是弧权。

利用矩阵方程可以判断不安全状态的可达性。

在安全协议形式化分析方面，CPN 具有其独特的优势：(1)将分层思想与数据结构结合；(2)对时间因素的灵活描述；(3)强大的仿真及状态分析自动工具；(4)有效的化简方法。

1.2 基于 CPN 的安全协议

安全协议的形式化分析与验证是一个复杂的过程，首先都要用形式化方法的语义对安全协议进行描述与建模。然而，从协议的非形式化描述，尤其是自然语言描述转变成形式化说明的过程可能会有错误发生，将直接导致后续分析的不确定性。同时一些形式化方法的提出都是从个别安全协议出发来设计规范的术语，遇见了新的协议形式，再对原有规范加以扩展，这样的形式化术语存在通用性差的问题。所以在进行安全协议的形式化描述与建模之前，需要采用通用的安全协议形式化说明加以规范。

为了使得通用安全协议说明更加适合于 Petri 网方法，本文在 CAPSL 的基础上抽象出通用安全协议的基本要素，在此基础上建立与 Petri 网要素的一一对应，如表 1 所示。

表 1 CPN 元素与安全协议基本元素对照表

安全协议要素	CPN 元素(CPN Object)
原子消息(实体名称、密钥、随机数…)	简单颜色集(Small color set)
复合消息(原子消息经过加密或连接)	复合颜色集(Compound color set)
集合消息(一组原子消息或者复合消息)	颜色集列表 (List color set)
密码操作(加密、解密等)	查询函数 (CPN scenario or CPN ML functions)
协议运行环境	联合颜色集(Union color set)
时间	时间颜色集(Timed color set)
Performance	CPN 仿真 (CPN simulate)

2 对安全协议的描述和函数库的创建

CPN tools 提供给每个变迁一个用 CPN ML 语言编程的程序编辑区。当变迁发生时，执行所编辑的程序，完成所需的功能。程序编辑区有三条固定的语句：input()、output()、action()，分别表示输入参数、输出参数和执行语句。

2.1 用 CPN ML 语言对安全属性进行描述

安全协议的重要安全性质包括：机密性、认证性、完整性。描述如下：

机密性：针对受保护的特定内容 t 的泄密状态来进行定义：

PredAllNodes(*fn* n=>cf(t,Mark.Intruder'BUFF1 n)>0)

该函数表示搜索所有的状态结点，如果有结点满足断言函数 *fn*，说明机密信息 t 泄露。

认证性：实体经过解密或者验证签名来实现认证，并在其缓冲区中保留认证成功的证据，类型为 AUT 的颜色集 colset AUT=with auth；同时保留被认证者的身份的名称。用查询函数来定义：

PredAllNodes (*fn* n=>cf (auth,Mark.A'BUFF1 n)>0 andalso

cf (auth, Mark. B'BUFF 1 n) >0 andalso cf(t, Mark.In'BUFF 1 n)>0)

完整性：安全协议确保交互的消息不能被篡改、删除和替代，或者至少消息的改变是可以被发现的。用形式化定义来表示：

PredAllNodes(*fn* n=>cf(auth,Mark.A'BUFF 1 n)>0 andalso cf(auth,Mark.B'BUFF 1 n)>0 andalso (cf (t, Mark.A'BUFF 1 n)>0 andalso cf (t',Mark.A'BUFF 1 n)<=0)

2.2 搭建安全协议的 CPN 查询函数库

先建立好一个函数模型库，对应于常见的密码学操作，并不断地扩展。上层实体通过函数调用的方式，利用分层建模的设置子页面工具将上层操作变迁与函数对应起来。

通用安全协议的功能层其实就是安全协议函数库，

即在底层先建立好一个函数模型库，对应于常见的密码学操作，并不断地扩展。上层实体只需要通过函数调用的方式，利用分层建模的设置子页面工具将上层操作变迁与函数对应起来就可以了。

在上面描述和对扩展的基础上，建立一个安全性质查询函数库。本文建立了一个能够覆盖绝大部分安全性质的查询函数库，用户只需要调用相应函数即可完成协议的相关安全性质的检查而不需要自己利用 CPN ML 语言编写查询函数。

2.3 一种基于 CPN 的通用安全协议形式化分析方法

本项目利用前面基于 CPN 的安全协议描述、对 CPN tools 的扩展、CPN 的安全协议操作函数库的建立，再结合实体模型中类似面向对象的类、派生对象概念，利用通用和规范的方法建模，提出一种基于 CPN 的通用安全协议形式化分析语言，该语言使用时就像用面向对象编程语言进行编程一样方便有效。

基于 CPN 的安全协议形式化分析语言工作流程图如图 1 所示。

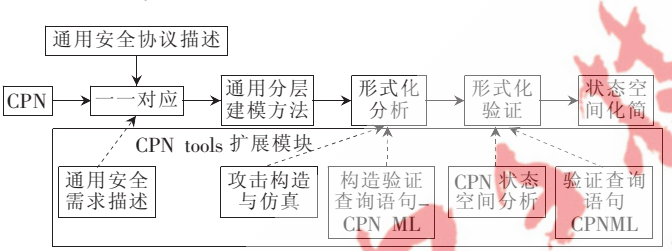

图 1 基于 CPN 的安全协议形式化分析语言工作流程图

针对具体协议，将安全属性用 CPN ML 查询函数进行形式化描述：首先用断言函数定义不安全状态，即协议满足安全属性时不可能出现的状态，如会话密钥泄露时的状态；再定义搜索函数对状态空间的所有状态进行断言函数的测试，寻找符合的结点标识；最后运行搜索查询函数，分析实验结果。

3 应用举例

本文以 ASW(Asokan-Shoup-Waidner)协议为例，利用本文提出的基于 CPN 模型对协议的安全性进行分析。

3.1 基于 CPN 模型对协议建模

ASW 协议由 exchange、abort、resolve_A 和 resolve_B 4 个子协议构成。在正常情况下，只执行 exchange 子协议。仅当 A 或 B 认为协议执行出现问题时，才执行其他子协议。

协议的 exchange 子协议具体描述如下：

EOO =(me1,Na);EOR =(me1,me2,Nb);EOD = affidavit_token

其中，Na、Nb 分别为 A 与 B 生成的临时值；m 为 A 向 B 发送的电子邮件；$C=\{m,Na,K_a,K_b\}K_{ttp}$ 是加密电子邮件。

Exchange sub-protocol：

$A\rightarrow B: me_1=K_a,K_b,TTP,C,h(m),\{K_a,K_b,TTP,C,h(m)\}Ka^{-1}$

IF B gives up THEN quit ELSE

$B\rightarrow A: me_2=h(N_b),\{me_1,h(N_b)\}K_b^{-1}$

IF A gives up THEN abort ELSE

$A\rightarrow B: me_3=m,N_a$

IF B gives up THEN resolve_B ELSE

$B\rightarrow A: me_4=N_b$

IF A gives up THEN resolve_A ELSE

Abort sub-protocol：

$A\rightarrow TTP: ma_1=aborted,me_1,\{aborted,me1\}Ka^{-1}$

IF B has resolved THEN resolve_A ELSE

$TTP\rightarrow A: abort\_token=aborted,ma_1,\{aborted,ma_1\}Kttp^{-1}$

Resolve_B sub-protocol：

$B\rightarrow TTP: mrb_1=Kb,me_1,me_2,N_b$

IF aborted THEN

$TTP\rightarrow B: mrb_2=abort\_token$

ELSE

$TTP\rightarrow B: mrb_3=m,a$

Resolve A sub-protocol：

$A\rightarrow TTP: mra_1=Ka,me_1,me_2,m,Na$

IF aborted THEN

$TTP\rightarrow A: mra_2=abort\_token$

ELSE

$TTP\rightarrow A: affidavit\_token=affidavit,mra_1,\{affidavit,mra1\}Kttp^{-1}$

在 exchange 子协议中，如图 2 所示，Alice 生成 me1 并发送给 B。如果 A 在合理的时间范围内没有收到 me2，A 将异常终止协议；否则，A 将 me3 发送给 B。如果等待 me4 的时间超时了，A 将异常终止协议并激活 resolve_A 子协议；否则，exchange 子协议成功运行结束。函数 gen_time(result)随机生成了一个延迟时间。条件 if temptime<timeout, then 1′1 else 1′0 判断超时是否发生。在这个模型中，由于使用了随机数作为延迟时间，超时的发生是随机的。如果 me1 的接收是超时的，Bob 将退出协议，否则 Bob 生成临时值 Nb，并将 me2 发送给 A。接着，如果 B 没有及时收到消息 me3，B 将激活 resolve_B

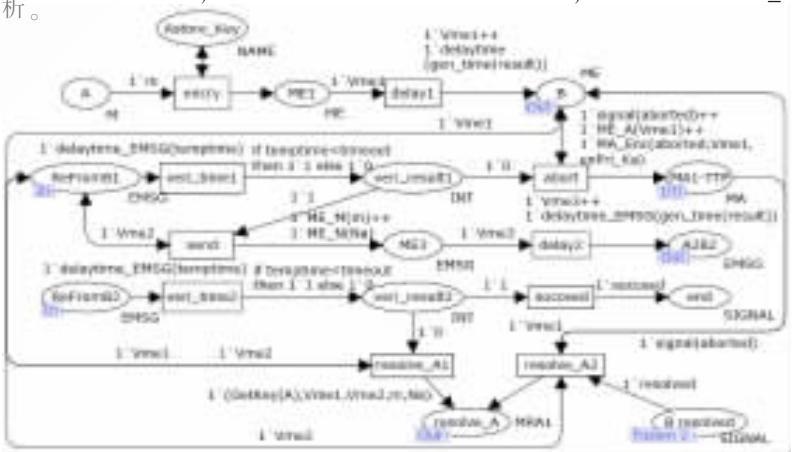

图 2 ASW 协议的 Alice 模型

子协议，否则，B 将消息 me4 发送给 A。

3.2 分析和验证

本文分别针对在 exchange 子协议异常终止和正常结束的两种情况下进行模型检测。因此在计算完全部状态空间后，修改了函数 fun Verif_Fairness，分别执行了以下两个 ML 查询函数：

```
fun Verif_Fairness_suc (con_id:INT, succeed:SIGNAL):
                                        Node list
=PredAllNodes (fn n=>
cf(con_id,Mark.Alice´ veri_result2 1 n)<>
cf(con_id,Mark.Bob´ veri_result2 1 n) andalso
cf(succeed,Mark.Alice'end 1 n)==1) );
fun Verif_Fairness_fail (amsg:AMSG,,emsg:EMSG,
                                rmsg:RMSG):Node list
=PredAllNodes (fn n=>
cf(amsg, Mark.TTP´ abort_token 1 n)<>empty andalso
cf(emsg, Mark.TTP´ TTP2B 1 n)<>empty andalso
cf(rmsg, Mark.TTP' TTP2A 1 n)<>empty) );
```

函数 fun Verif_Fairness_suc 查询的是在 exchange 子协议正常结束的情况下，是否有不满足公平性的状态。结果为 0，说明当 exchange 子协议成功结束后，协议满足可追究性和公平性。相反，fun Verif_Fairness_fail 的查询结果列出了一些不安全状态，说明当协议异常终止后，不满足安全性。

本文将面向对象方法及其概念(如类、对象、函数等)引入建模中，并直接嵌入通用安全协议描述中，以此为基础的协议建模就具有了抽象、重用、继承等性质，简化了建模过程，使得图型化的 CPN 建模能够像面向对象编程语言一样方便和有效。利用 CPN tools 提供的复制和分层次工具实现函数调用以及派生实体的快速建模，将面向对象思想中的派生实体与函数调用思想应用于建模过程中。本文提出通用的安全协议分析语言，具有通用性、易用性、图形化等特点。

参考文献

[1] 李梦君，李舟军，陈火旺.安全协议的扩展 Horn 逻辑模型及其验证方法 [J]. 计算机学报，2006，29 (9)：1666-1678.

[2] 怀进鹏，李先贤.密码协议的代数模型及其安全性[J].中国科学(E 辑)，2003，33(12).

[3] 冯登国，范红.安全协议理论与方法[M].北京：科学出版社，2003.

[4] YASINSEC A. A formal semantics for evaluating cryptographic protocols[D]. University of Virginia, 1996.

[5] MILLEN J. CAPSL: common authentication protocol specification language [R]. Technical Report MP97B48, The MITRE Corporation, 1997.

[6] Wei Jin, Su Guiping. An integrated model to analyze cryptographic protocols with colored Petri Nets. In Proceeing [C]. 11th IEEE Symposium on High Assurance Systems Engineering Symposium，2008.

(收稿日期：2011-05-02)

作者简介：

苏桂平，女，1963 年生，博士，副教授，硕士生导师，主要研究方向：信息安全。

孙莎，女，1981 年生，硕士研究生，主要研究方向：计算机应用。