Petri Net Model and Analysis for Electronic Payment Security Protocol

电子支付安全协议的Petri网模型及分析

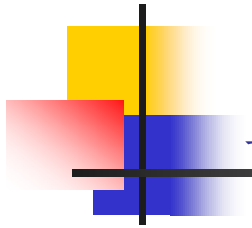
林 松

aboc_lin@sina.com

四川大学信息安全研究所

CERNET第十二届学术年会

2005年11月3日于大连



主要内容

- Petri网简介
- 电子支付安全协议的Petri网模型
- 构建电子支付安全协议的可达树
- 分析电子支付安全协议
- 小结

前言

- 电子支付是客户利用电子账户，通过计算机网络来实施的支付，随着计算机和通信的发展，电子支付已经成为各银行生存、发展和参与竞争的重要手段
- 如果没有安全保障，电子支付很难真正发展起来
- 因此电子支付安全协议的研究就成为了一个重要的课题

Petri网简介

- 1962年，德国的C.A. Petri在他的博士论文《用自动机通信》中首次使用网状结构模拟通信系统，这是Petri网建立系统模型的起点
- Petri网兼顾了严格定义与图形语言两个方面，具有丰富而严格的模型语义，同时又是一种图形化的语言，具有直观、易懂与易用的优点
- 它采用库所(place)、变迁(transition)、弧(arc)的连接来表示系统的功能和结构

库所、变迁、弧和托肯的说明

- 库所表示系统中的条件、资源和信息等可以静态表达的事物，在图形具体表示中，用圆圈“O”或椭圆表示
- 变迁表示系统中的变化，如状态的变化、条件的变化、信息的流动以及资源的消耗和产生等需要动态表达的事件，用矩形“口”或短棒“▌”代表
- 弧表示库所与变迁之间的流关系，用 “→”来表示有向弧，用“—◦”来表示抑制弧(inhibitor arc)
- 托肯表示库所中代表的事物的数量，用黑点“•”表示库所中含有的托肯

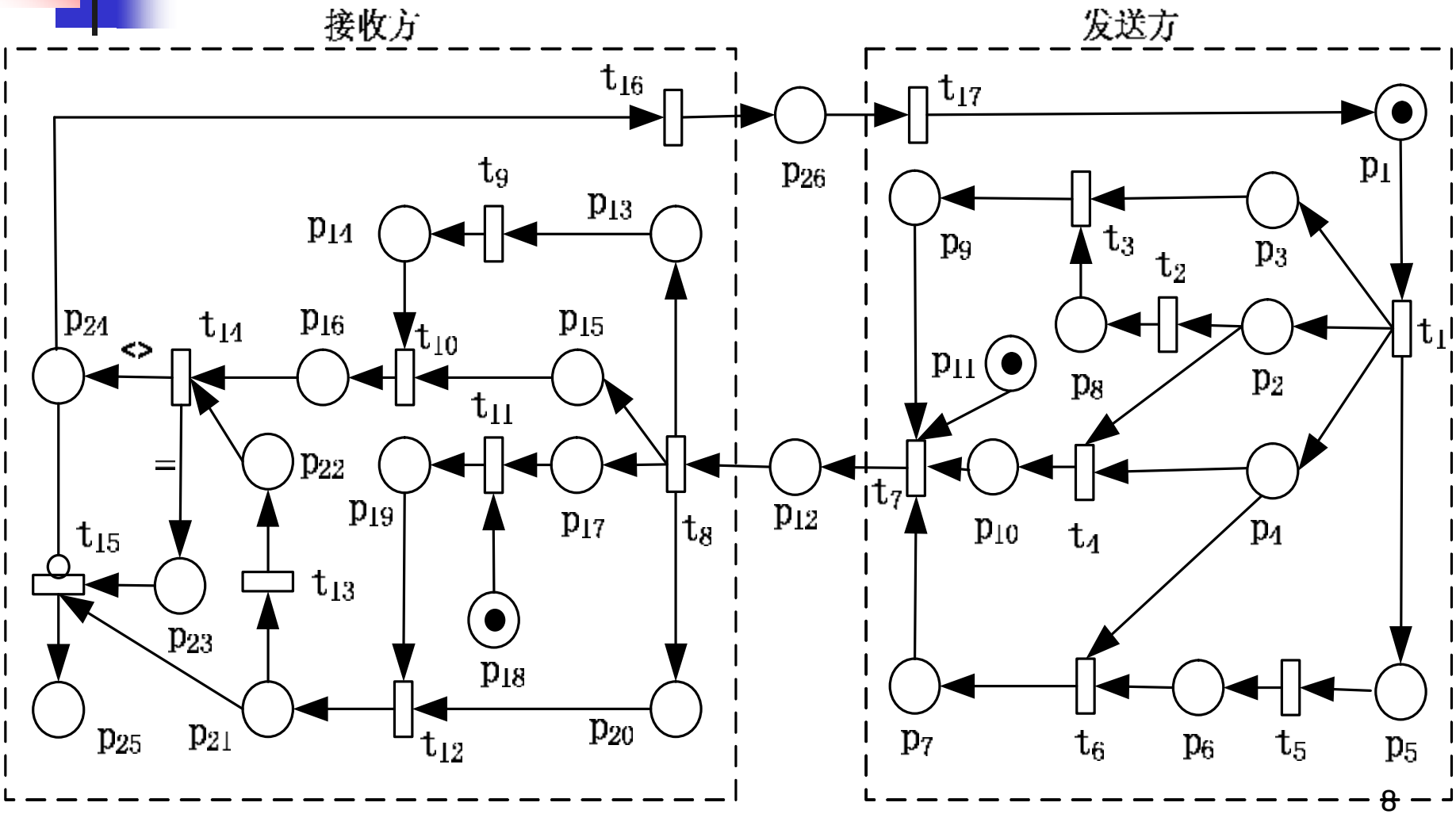
Petri网的特点

- Petri网将系统看成一个白盒子，通过对系统内各要素的抽象，分析这些要素相互作用引起的系统变化，是和黑盒子相反的分析方法，白盒子是通过给定输入信号，根据系统的功能，推导输出信号
- 只要满足给定的条件或约束，Petri网将会自动进行状态转换，体现了系统的动态行为特征
- Petri网综合了数据流、控制流和状态变迁，能方便地描述系统的分布、并发、资源共享、同步、异步、冲突等重要特性

SET安全协议研究内容

- SET(Secure Electronic Transaction)协议是电子支付中比较复杂的安全协议之一
- 对SET协议的安全处理过程进行描述与分析
- 重点研究加密和解密的安全处理流程
- 分析双重数字签名处理过程
- 用Petri网理论建立起支付协议的安全模型

电子支付密码协议的Petri网模型



模型中库所的含义

库所	含义	库所	含义	库所	含义
p_1	初始信息	p_{10}	发送的消息密文	p_{19}	对称密钥
p_2	发送的消息明文	p_{11}	发送方的数字证书	p_{20}	接收的消息密文
p_3	发送方的私人密钥	p_{12}	发送的数据	p_{21}	接收的消息明文
p_4	随机产生的对称密钥	p_{13}	发送方的数字证书	p_{22}	明文中得到消息摘要
p_5	接收方的数字证书	p_{14}	发送方的公开密钥	p_{23}	接收成功
p_6	接收方的公开密钥	p_{15}	接收的数字签名	p_{24}	接收失败
p_7	发送的数字信封	p_{16}	签名中得到的消息摘要	p_{25}	完整的明文信息
p_8	发送的消息摘要	p_{17}	接收的数字信封	p_{26}	成功或失败的标识
p_9	发送的数字签名	p_{18}	接收方的私人密钥		

模型中变迁的含义

变迁	含义	变迁	含义	变迁	含义
t_1	对初始数据拆分	t_7	数据打包并且发送	t_{13}	对明文哈希运算
t_2	对发送明文哈希运算	t_8	接收并且数据解包	t_{14}	比较消息摘要
t_3	用私人密钥签名摘要	t_9	获取发送方公开密钥	t_{15}	数据完整性判断
t_4	用对称密钥加密明文	t_{10}	用公开密钥验证签名	t_{16}	产生并发送标识
t_5	获取接收方公开密钥	t_{11}	解密发送方数字信封	t_{17}	接收标识的处理
t_6	加密公开密钥	t_{12}	解密消息密文		

发送方加密和接收方解密过程(一)

- 1.发送方获取自己的以及接收方的数字证书
- 2.认证接收方的数字证书，获得接收方的公开密钥
- 3.随机生成对称密钥
- 4.用接收方公开密钥对随机生成的对称密钥加密，将随机生成的对称密钥装入数字信封
- 5.用随机生成的对称密钥将准备发送的消息明文进行加密处理，生成消息密文

发送方加密和接收方解密过程(二)

- 6.准备发送的消息明文经过哈希运算，得到消息摘要
- 7.用发送方的私人密钥对消息摘要签名处理，得到数字签名
- 8.将数字信封、消息密文、数字签名和发送方的数字证书进行集成打包
- 9.发送打包后的数据
- 10.接收发送方的数据
- 11.将接收的数据拆分为消息密文、数字信封、数字签名和发送方的数字证书

发送方加密和接收方解密过程(三)

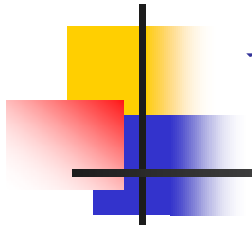
- 12.通过对发送方的数字证书进行认证，获取发送方的公开密钥
- 13.用发送方的公开密钥验证发送方的数字签名，得到一个消息摘要
- 14.用接收方的私人密钥对接收到的数字信封解密，从数字信封中取出对称密钥
- 15. 用对称密钥解密接收到的消息密文，还原出消息明文
- 16.对消息明文进行哈希运算，得到另外一个消息摘要

发送方加密和接收方解密过程(四)

- 17.比较这两个消息摘要，确认消息的完整性，如果两个消息摘要相等，则表明接收到了完整的发送数据，接收数据成功；反之就是数据接收不完整，接收数据失败
- 18. 将接收成功或失败的信息反馈给发送方
- 19.发送方根据反馈的信息决定后继处理，如果反馈回来的是成功的标识，则结束本次处理；反之，则继续重复发送上次的明文数据（可以给重复发送的次数设定一个固定值，超过该固定值时，则表示系统网络或设备等故障，整个操作强制结束，不会出现死锁现象）

电子支付安全协议模型说明

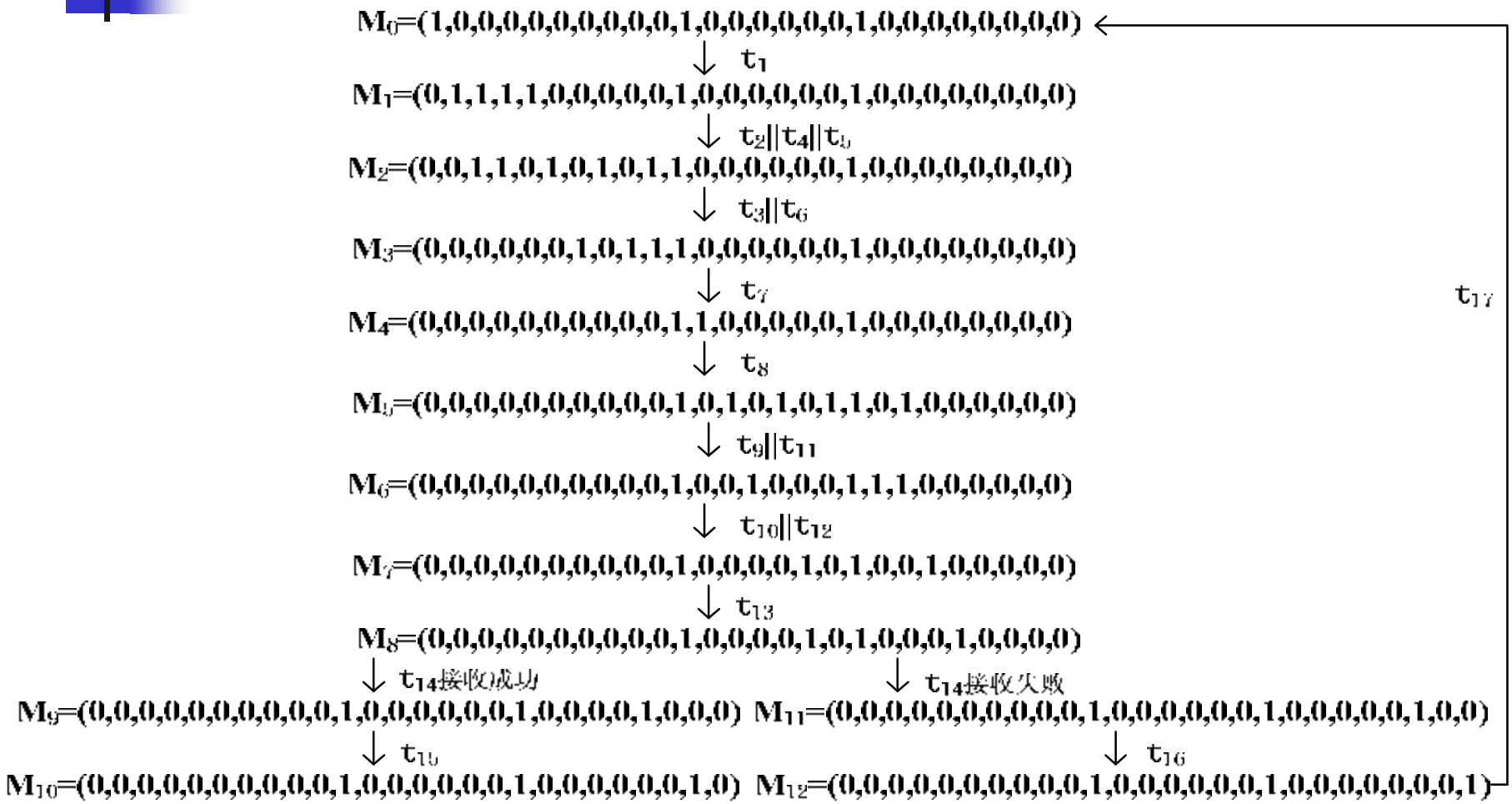
- 用Petri网详细地描述了发送方加密和接收方解密的处理过程，可以直观地阐述电子支付的安全处理流程
- 其中库所p_{24}到变迁t_{15}的弧为抑制弧(inhibitor arc)，表示只要库所p_{24}有托肯，则变迁t_{15}就不能激发，库所p_{24}没有托肯时，变迁t_{15}才能激发
- 可以得出系统的输入、输出以及关联矩阵
- 系统将非对称加密和对称加密结合使用：使用非对称密码体制交换密钥，使用对称密码体制传递信息正文



可达树的概念

- 可达树(Reachability Tree) 用来表示标识的可以变化的过程
- 以初始标识作为树根，由可到达的标识作为树的后继结点，每条连接结点的弧表示一个变迁的点火，它将一个标识变换到另一个标识
- 给定一个Petri网系统，从初始标识开始，可以得到数量与有效变迁一样多的新标识

电子支付协议的可达树



电子支付协议的可达树说明

- 图中“||”表示变迁可以并行引发，无论变迁引发的次序如何，可达树都归结到同一个标识结点
- 初始标识为 =(1,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0)
- 激发t_{14}时，比较两个信息摘要，判断是否接收完整
- 当两个消息摘要相同时，表示接收成功，变迁序列 $=t_1t_2t_3t_4t_5t_6t_7t_8t_9t_{10}t_{11}t_{12}t_{13}t_{14}t_{15}$，成功的终止标识为 =(0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0)
- 否则变迁序列$=t_1t_2t_3t_4t_5t_6t_7t_8t_9t_{10}t_{11}t_{12}t_{13}t_{14}t_{16}t_{17}$，将出错信息反馈给发送方，接收数据失败的终止标识为 =(1,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0)
- 发送方在一定重发次数的限定范围内重新发送上次的数据

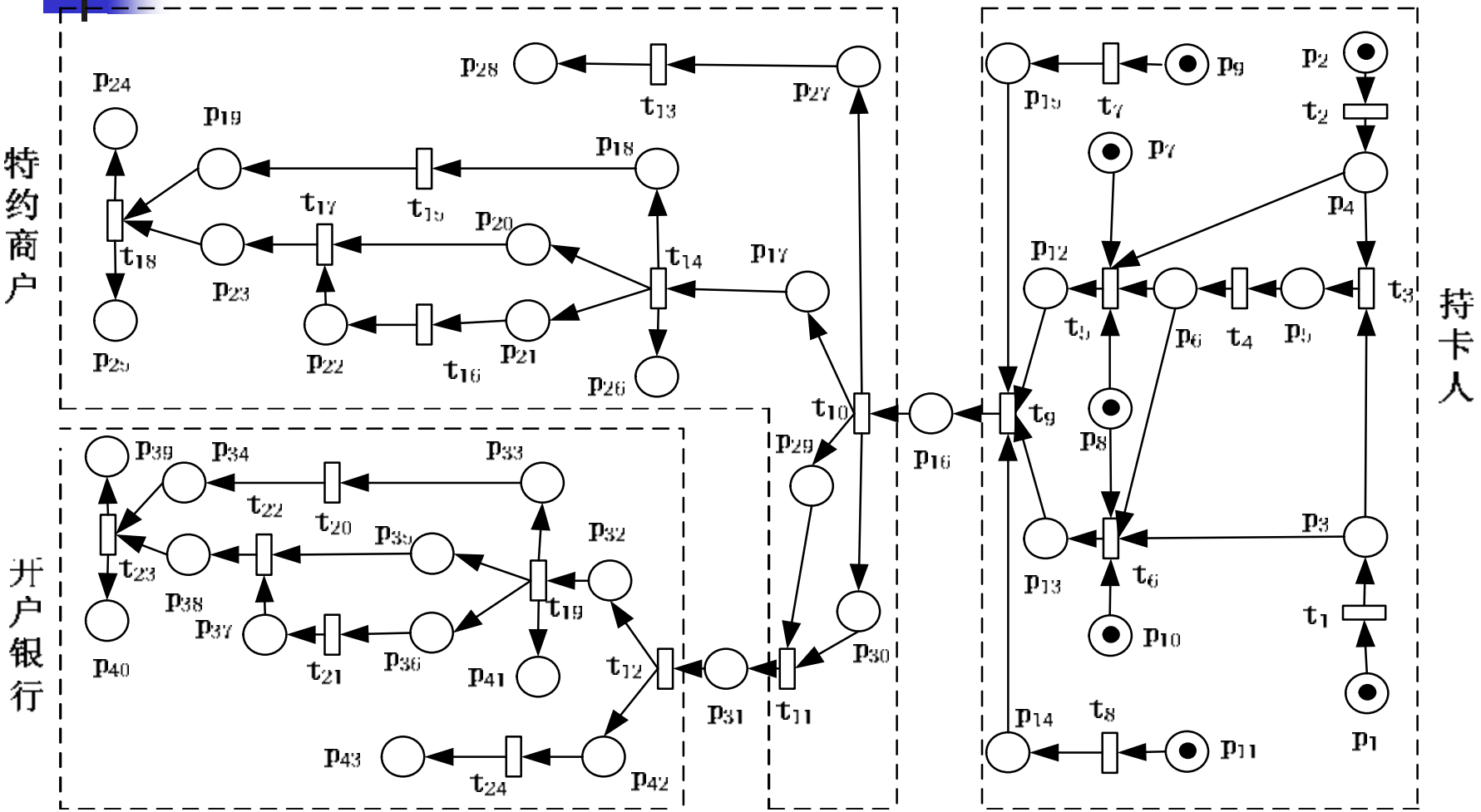
电子支付协议的可达树分析

- 可达树中各结点库所包含的托肯数不超过两个，因此该电子支付协议是有界的、安全的
- 可达树中各变迁至少引发一次，没有从不引发的变迁，树中每个标号都有后继标号，即每个标号都是可以引发的，根据活性的定义，可以得知该网是活的，不会有死锁发生
- 对于任意一个变迁，在引发之前，其它变迁都只能引发有限次，因此该Petri网是公平的
- 整个电子支付过程是可达的

双重数字签名介绍

- 电子支付系统中，持卡人向特约商户提出购物信息的同时，也给银行付款信息，以便开户行付款，但是持卡人不希望特约商户知道自己的银行账号信息，只需按照金额进行借记或者贷记账户
- 双重数字签名能够满足需要发送两个相关的信息给接收者，接收者只能打开一个，而另一个只需转发，不能打开看其内容的安全需求

双重数字签名的Petri网模型

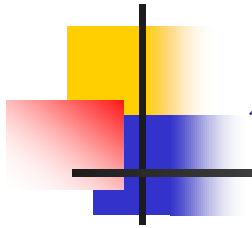


双重数字签名模型中库所的含义

库所	含义	库所	含义	库所	含义
p_1	订货信息OI	p_{16}	持卡人给商户的信息	p_{31}	商户给银行的信息
p_2	支付信息PI	p_{17}	接收的商户密文EM_B	p_{32}	接收的银行密文EM_C
p_3	订货消息摘要MD_B	p_{18}	接收的数字签名DS	p_{33}	接收的数字签名DS
p_4	支付消息摘要MD_C	p_{19}	数字签名的摘要MD_{BC}	p_{34}	数字签名的摘要MD_{BC}
p_5	订货和支付摘要MD_{BC}	p_{20}	接收的银行信封MD_C	p_{35}	接收的商户信封MD_B
p_6	数字签名DS	p_{21}	商户订货信息B(OI)	p_{36}	银行支付信息C(PI)
p_7	商户订货信息B(OI)	p_{22}	计算的订货摘要MD_B	p_{37}	计算的支付摘要MD_C
p_8	PB_A和S_{CA}	p_{23}	计算的混合摘要MD^*_{BC}	p_{38}	计算的混合摘要MD^*_{BC}
p_9	PB_B和S_{CA}	p_{24}	摘要相符接收正确	p_{39}	摘要相符接收正确
p_{10}	银行支付信息C(PI)	p_{25}	摘要不符接收失败	p_{40}	摘要不符接收失败
p_{11}	PB_C和S_{CA}	p_{26}	接收的PB_A和S_{CA}	p_{41}	接收的PB_A和S_{CA}
p_{12}	商户的密文EM_B	p_{27}	接收的商户信封DE_B	p_{42}	接收的银行信封DE_C
p_{13}	银行的密文EM_C	p_{28}	利用PV_B解密得SK_1	p_{43}	利用PV_C解密得SK_2
p_{14}	银行的数字信封DE_C	p_{29}	接收的银行信封DE_C		
p_{15}	商户的数字信封DE_B	p_{30}	接收的银行密文EM_C		

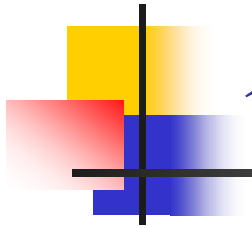
双重数字签名模型中变迁的含义

变迁	含义	变迁	含义	变迁	含义
t_1	哈希运算订货信息	t_9	发送数据集成	t_{17}	混合成消息摘要MD^*_{BC}
t_2	哈希运算支付信息	t_{10}	商户接收数据	t_{18}	比较摘要MD_{BC}和MD^*_{BC}
t_3	混合成消息摘要MD_{BC}	t_{11}	商户向银行发送数据	t_{19}	利用SK_2解密EM_C
t_4	用PV_A签署数字签名	t_{12}	银行从商户接收数据	t_{20}	用PB_A从DS得到MD_{BC}
t_5	用对称密钥SK_1加密	t_{13}	利用PV_B解密DE_B	t_{21}	从C(PI)得到MD_C
t_6	用对称密钥SK_2加密	t_{14}	利用SK_1解密EM_B	t_{22}	混合成消息摘要MD^*_{BC}
t_7	用SK_1和PB_B加密成数字信封	t_{15}	利用PB_A从DS得到MD_{BC}	t_{23}	比较摘要MD_{BC}和MD^*_{BC}
t_8	用SK_2和PB_C加密成数字信封	t_{16}	从B(OI)得到MD_B	t_{24}	利用PV_C解密DE_C



小结

- 这里利用Petri网理论，通过对安全电子支付的详细分析，尤其是发送方加密和接收方解密的处理，以及对双重数字签名的研究，建立了电子支付安全协议的Petri网模型
- 通过构建可达树，研究了电子支付SET协议的正确性、保密性、活性以及公平性
- 说明了电子支付安全协议Petri网模型的优点和特点



今后的工作

- 可以引入时间Petri网分析安全协议的执行效率
- 考虑入侵检测进行抗攻击分析
- 可以利用关联矩阵(incidence matrix)的方法分析系统的执行状态
- 利用随机Petri网来研究安全协议的性能
- 利用有色Petri网来解决状态空间爆炸的问题

欢迎指正

谢谢大家