# 基于 Petri 网的数字媒体分发协议的安全性证明

郭迎九[1,2],林 闯[2],尹 浩[2],田立勤[1]
(1. 北京科技大学信息工程学院,北京 100083;2. 清华大学计算机科学与技术系,北京 100084)

**摘 要**: 安全协议的形式化证明是目前的一个热点和难点问题. 本文以一种数字媒体分发协议(DMDP)为例,采用基于 Petri 网模型并结合进程代数和逻辑归纳方法对其进行形式化证明,新的方法有效避免了状态空间爆炸问题. 在证明过程中,采用协议安全性等价原则,对分发协议进行简化,使证明更加简洁. 文章同时对证明方法的完备性进行了讨论,说明了 Petri 网模型证明协议安全性的有效性.

**关键词**: Petri 网; 安全协议; 数字媒体
**中图分类号**: TP309 **文献标识码**: A **文章编号**: 0372-2112 (2009) 05-1030-07

# Proof of the Security of Digital Media Distributing Protocol Based on Petri Net Models

GUO Ying-jiu[1,2], LIN Chuang[2], YIN Hao[2], TIAN Li-qin[1]
(1. *Information Engineering School, University of Science and Technology Beijing, Beijing* 100083, *China*;
2. *Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*)

Abstract: The formal proof of the security protocol becomes a hot and hard issue. Taking the Digital Media Distribution Protocol as an example, the Petri Net model is adopted which combined with the process algebra and the logical induction methods to formally prove the present security protocol and can avoid the state explosion problem. In this proof an equality principle is used to transform the security protocols to guarantee the simplicity of the proof. At the same time, the completeness of the proof is discussed and what we have done shows the validity of proving the security of protocol with a Petri Net model.

Key words: Petri net; security protocol; digital media

## 1 引言

安全协议作为网络安全的基石,在媒体分发业务中已成为备受关注的问题. 然而,安全协议的证明是一个非常困难的工作. 作为图形化数学建模工具的 Petri,能方便描述系统的分布、并发、资源共享、同步、异步、冲突等重要特性,可融合基于规则推理系统模型[1]和基于代数系统的模型[2]的优点,是分析证明安全协议一种好的工具.

本文采用的 Petri 模型结合了进程代数、事件语义、逻辑归纳方法,可有效避免状态爆炸问题,使证明更加严密可行,并以一种数字媒体分发安全协议 DMDP(Digital Media Distribution Protocol)为例[3]进行了证明.

## 2 DMDP 协议介绍及 SP. Petri 模型定义

### 2.1 DMDP 协议介绍

DMDP 数字媒体分发安全协议是随着 P2P 网络的发展以及下一代互联网出现的情况下提出的[4,5],主要功能是在网络进行数字内容分发并对数字内容进行有效保护. DMDP 协议由内容提供方、内容分发方、收费网关、收费银行等几部分组成. 协议满足机密性、数据完整性、认证性和不可否认性等要求. 协议流程如图 1 示意.

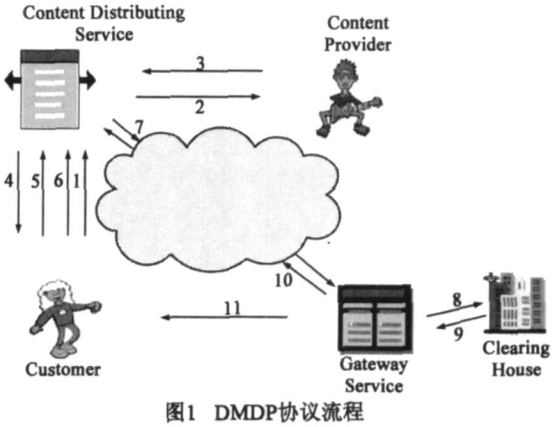



图1 DMDP协议流程

收稿日期:2008-04-08;修回日期:2008-06-12
基金项目:国家自然科学基金(No. 60673184,No. 60673187,No. 60673054,No. 90412012);973 计划前期研究专项(No. 2006CB708301);中国移动通信研究院项目和教育部科技创新培育重点项目(No. 707005)

步骤 1、2、3 为客户提交内容信息和权利要求信息以及内容提供方向内容分发方发送复合数字对象的过程. 步骤 4、5 为内容分发方发送加密复合数字对象给客户的过程. 步骤 6、7 为向收费网关提交用户和内容提供方账号信息的过程. 收费过程为 8 —11. 为了描述方便,定义了一些符号,见表 1.

表 1　符号及定义

| 符号 | 意义 | 符号 | 意义 |
|---|---|---|---|
| $N_A$ | 主体 A 的临时值 | HDO | 复合数字对象* |
| H(m) | 消息 m 的哈希值 | $M_k$ | 用密钥 k 对消息 M 加密 |
| PRIV(A), PUB(A) | 主体 A 的公钥、私钥 | CH, D | 收费银行、内容分发方 |
| C, G, ConP | 客户,网关和内容提供方 | Total Price | HDO 的消费价格 |
| CAN | 客户账号信息 | ConPCAN | 内容提供方账号信息 |
| TK_HDO | 复合数字对象密钥 | TK_CA | 客户和网关的会话密钥 |
| ContentID | 复合数字对象惟一 ID | ContentDesp | 复合数字对象内容描述 |
| RightInfo | 使用权利描述 | | |

DMDP 协议形式化描述如下:

(1) $C \rightarrow D: \{(C, N_C, OrderID, ContentID, ContentDesp, RightInfo)_{PUB(ConP)}, H((C, N_C, OrderID, ContentID, ContentDesp, RightInfo)_{PUB(ConP)})\}$.

(2) $D \rightarrow ConP: \{(C, N_C, OrderID, ContentID, ContentDesp, RightInfo)_{PUB(ConP)}, H((C, N_C, OrderID, ContentID, ContentDesp, RightInfo)_{PUB(ConP)})\}$.

(3) $ConP \rightarrow D: \{(ConP, N_C, N_{ConP}, (Total\ Price)_{PRIV(ConP)})_{PUB(C)}, (HDO)_{TK\_HDO}, H((HDO)_{TK\_HDO}), H((ConP, N_C, N_{ConP}, (Total\ Price)_{PRIV(ConP)})_{PUB(C)}, (HDO)_{TK\_HDO}, H((HDO)_{TK\_HDO})), (ConP, N_{ConP}, OrderID, ContentID, (Total\ Price, ConPCAN)_{PRIV(ConP)}, (TK\_HDO)_{PRIV(ConP)})_{PUB(G)}, H((ConP, N_{ConP}, OrderID, ContentID, (Total\ Price, ConPCAN)_{PRIV(ConP)}, (TK\_HDO)_{PRIV(ConP)})_{PUB(G)})$

(4) $D \rightarrow C: \{(ConP, N_C, N_{ConP}, (Total\ Price)_{PRIV(ConP)})_{PUB(C)}, (HDO)_{TK\_HDO}, H(HDO_{TK\_HDO})), H((ConP, N_C, N_{ConP}, (Total\ Price)_{PRIV(ConP)})_{PUB(C)}, (HDO)_{TK\_HDO}, H(HDO_{TK\_HDO}))\}$

(5) $C \rightarrow D: \{(C, N_C, N_{ConP})_{PUB(ConP)}, (C, N_C, OrderID, ContentID, H(HDO)_{TK\_HDO}, (Total\ Price, CAN, TK\_CA)_{PRIV(C)})_{PUB(G)}, H((C, N_C, N_{ConP})_{PUB(ConP)}, (C, N_C, OrderID, ContentID, H(HDO)_{TK\_HDO}, (Total\ Price, CAN, TK\_CA)_{PRIV(C)})_{PUB(G)})\}$

(6) $D \rightarrow ConP: \{(C, N_C, N_{ConP})_{PUB(ConP)}, H(C, N_C, N_{ConP})_{PUB(ConP)})\}$

(7) $D \rightarrow G: \{(D, N_D)_{PUB(G)}, (C, N_C, OrderID, ContentID, H(HDO)_{TK\_HDO}, (Total\ Price, CAN, TK\_CA)_{PRIV(C)})_{PUB(G)}, (ConP, N_{ConP}, OrderID, ContentID, (Total\ Price, ConPCAN)_{PRIV(ConP)}, (TK\_HDO)_{PRIV(ConP)})_{PUB(G)}, H((HDO)_{TK\_HDO}), H((D, N_D)_{PUB(G)}, (C, N_C, OrderID, ContentID, H(HDO)_{TK\_HDO}, (Total\ Price, CAN, TK\_CA)_{PRIV(C)})_{PUB(G)}, (ConP, N_{ConP}, OrderID, ContentID, (Total\ Price, ConPCAN)_{PRIV(ConP)}, (TK\_HDO)_{PRIV(ConP)})_{PUB(G)}, H((HDO)_{TK\_HDO}))\}$

(8) $G \rightarrow CH: Request$

(9) $CH \rightarrow G: Response$

(10) $G \rightarrow C: \{((TK\_HDO)_{PRIV(ConP)})_{TK\_CA}, (G, N_G, N_C, (INVOICE)_{PRIV(G)})_{PUB(C)}, H(((TK\_HDO)_{PRIV(ConP)})_{TK\_CA}, (G, N_G, N_C, (INVOICE)_{PRIV(G)})_{PUB(C)})\}$

## 2.2　SP_Petri(Security Protocol Petri)模型定义

有关 Petri 网概念知识读者可参阅文献[6].

**定义 1**　定义 SP_Petri 模型为六元组$(P, T, F, E, M, M0)$,其中 $M$ 表示协议的状态空间集合; $M0$ 表示系统的初始状态空间集合; $T \subseteq M \times M$ 表示协议状态变迁; $P$ 表示协议实体元素集合或者系统局部状态, $M \rightarrow 2^P$; $F$ 是弧集, $F \subseteq (P \times T) \cup (T \times P)$; $E$ 为弧函数,为发生状态变迁的点火条件.

进程代数使用代数方法研究通信并发系统,能精确描述安全协议中角色与参与的会话以及不同角色之间的交互过程. 因此我们在 SP_Petri 模型中引入进程代数概念准确描述协议过程. 在模型中,定义实体元素集合(通信主体及消息集合等) Names(包括 $n, m, A, B$),其相应的变量区分为名称变量和消息变量. 定义进程 Proc 描述协议状态变化过程,定义事件 $Ev$ 为组成进程的基本单位. 事件定义参见文献[7].

事件条件分控制条件、名称条件和网络条件. 控制条件和名称条件在事件发生时使用一次就被消耗掉了,而网络条件是一种持久的条件,可以在网络中持久保存. 定义变量 $\sigma$ 作为消息或进程的替代变量,定义 $Ic(Proc)$ 表示进程控制条件, $((M1))$, $((M2))$, , , , , $((Mj))$ 表示网络存在的消息集合.

**定义 2**　四类基本事件:事件 Out、事件 In、事件 new、事件 $ch$,如图 2 - 6 所示. 这四类基本事件代表了协议的基本行为. 基本事件的发生默认附带有控制条件 $Ic(Proc)$.

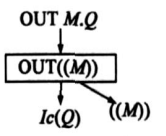


图2　out事件

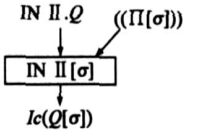


图3　in事件

图4　New事件

多进程选择事件 $ch$ 关联多个进程,在多个进程间转移控制条件,单进程选择事件 $ch$ 关联单一进程,根据进程输入到网络上的消息转移控制条件.

**定义 3**　进程为事件和初始状态的集合,即 $Proc =$

* 复合数字对象是通过将多种类型的信息有机地组织起来,封装完善的行为方法与元数据,从根本上解决信息组织与服务之间的矛盾,并能提供完善的版权保护.

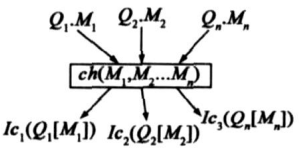



图5 多进程选择事件

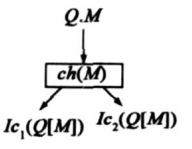



图6 单进程选择事件

$(Ev(Proc), M0), M0 = \{s0, ((M1)), ((M2)) \cdots\cdots ((Mj))\} \cup Ic(Proc)$,其中 $s0$ 表示初始名称集合.

(1) *Nil* 终止进程;

(2) $new(\sigma).Proc$ 产生一个新鲜数与进程中变量 $\sigma$ 绑定;

(3) $outM.Proc$ 将消息 $M$ 输出到网络媒介中;

(4) $in\Pi.Proc$ 等待一个与模式 $\Pi$ 匹配的输入;

(5) □ *Proc* 选择进程,有以下两种选择:

(a) $[M = N].Proc$ 指如果 $M = N$ 继续执行进程 *Proc*,否则终止;

(b) $[M > \Pi].P$ 指消息 $M$ 是否与模式 $\Pi$ 匹配,如匹配$(\Pi.M)$继续执行进程 *Proc*,否则$(!\ \Pi.M)$终止.

6. $\|_{i\in I}Pi$ 并行进程,$I$ 为整数集合,$i$ 为进程索引

7. $|_{i\in I}Pi$ 串行进程,$I$ 为整数集合,$i$ 为进程索引

**定义 4** 如果 $P$ 是一个进程,$M0$ 是初始状态.$M$,$M$ 为进程状态,$e \in Ev(P)$ 为一个事件,定义 $M \xrightarrow{e} M'$ 如果下述条件满足[7]:

(1) $\cdot e \subseteq M$

(2) $M' = (M/\cdot e) \cup e\cdot$

状态 $M$ 可达如果

$$M0 \xrightarrow{e_0} \cdots \xrightarrow{e_{(i-1)}} Mi = M$$

**定义 5** (消息新鲜性定义)给一个事件 $e$,iff $n \in Names$ 在事件 $e$ 中是新鲜的,即 $Fresh(n,e)$,如果 $s \in \cdot e, s' \in e\cdot, n \notin s$ 且 $n \in s'$.

**定义 6** 如果协议参与方在某点的密钥被泄露,则称此点为坏点(*Bad*).

**定理 1** SP_Petri 网模型是完备性的.

**证明**:对任意有限状态的安全协议,其 SP_Petri 模型设为 $SP$,进程为 $P$,其安全性要求集合为 $A$,设 $\phi \in A$,需要证明对于 $\forall\phi, \exists(M0 \cdots M') \in SP$,且$(M0 \cdots M') \vdash \phi$.

用 $e < e_1$ 表示事件 $e$ 先于事件 $e_1$ 发生.设进程中某一运行段为 $\eta, [e_i \cdots e_l] \subset \eta, [e_i \cdots e_k] \subset \eta$,其中 $e_l < e_k$.如果 $P[e_i \cdots e_l] \rightarrow \phi, P[e_i \cdots e_k] \rightarrow \neg\phi$ 成立,则 $\exists e_a \in \eta$,其中 $e_l < e_a < e_k$,使得 $P[e_i \cdots e_{a-1}] \rightarrow \phi, P[e_i \cdots e_a] \rightarrow \neg\phi$ 成立.由定义 4 事件与状态的关系,可得出存在 $Mi \xrightarrow{e_i} \cdots \xrightarrow{e_{(a-1)}} Mi \supset \phi$,且 $Mi \xrightarrow{e_i} \cdots \xrightarrow{e_{(a-1)}} Mi \supset \neg\phi$ 成立.因此 $\exists(M0 \cdots M') \in SP$,且$(M0 \cdots M') \vdash \phi$.

## 3 DMDP 安全协议的简化

### 3.1 安全简化条件

Mei Lin Hui ,Gavin Lowe 在文献[8]提出了安全协议简化的条件,本文在文献[8]研究的基础上,提出了安全协议等价性的概念,并依据安全协议等价性条件,将 DMDP 安全协议进行简化,方便我们的证明.

**定义 7** 我们将协议参与主体、密钥及新鲜数列为基本消息项,也称为原子消息(*Atom*).原子消息经过加密或连接运算构成复合消息.

假设 *fact* 为协议中的消息,$f$ 为转换函数,定义形式变换为:

$$f: fact \rightarrow fact$$

**定义 8** (安全协议)一个安全协议可以定义为一个二元组,即 $P = (\Omega, \Gamma)$,其中 $\Omega$ 表示协议的初始假设集合(包括各主体的信念、接受消息、理解消息和解释消息),$\Gamma$ 是该协议应该达到的目标集.$\Omega$ 和 $\Gamma$ 都可用形式语言描述.

**定义 9** (协议安全性等价) 设 $P1 = (\Omega 1, \Gamma 1)$,$P2 = (\Omega 2, \Gamma 2)$ 是两个安全协议,其中,如果安全协议 $P1$ 和 $P2$ 满足以下条件:

(1) 存在一般代换 $\alpha$,使得 $\Gamma 2 = \alpha\Gamma 1$;

(2) 假设变量 *fact* 的集合 $\Omega$ 和一个 *fact* $m$,如果 $m$ 能够从 $\Omega$ 和 $IK$(入侵者 Intruder 的初始知识)中产生,那么 $f(m)$ 能够从 $f(\Omega)$ 和 $IK'$(对入侵者 Intruder 的初始知识经过简化转换而产生的入侵者在简化系统中的初始知识)中产生.

$$\Omega \cup IK \rightarrow m \Rightarrow f(\Omega) \cup IK' \rightarrow f(m) \qquad (1)$$

(3) 简化系统中入侵者初始知识包括所有原始系统中初始知识的转换:

$$f(IK) \subseteq IK' \qquad (2)$$

则我们称安全协议 $P1$ 和 $P2$ 协议安全性等价.

不失一般性,我们假设协议系统包括两个诚实协议主体 $A$、$B$,Mei Lin Hui 描绘入侵者 Intruder 的能力为:

$INTRUDER(S) \triangleq$

$\square_{M\in Message} send?A?B!M \rightarrow INTRUDER((S) \cup \{M\})$

$\square_{M\in Message, S\vdash M} receive?A?B!M \rightarrow INTRUDER(S)$

$\square_{M\in Message, S\vdash M} leak, M \rightarrow INTRUDER(S)$

协议模型为:$SYSTEM \triangleq (\|_{A\in Agent} P_A) \ \|\ INTRUDER(IK_0)$

根据文献[8]对上式中 $S$ 和 $IK_0$ 的定义,可得出 $S \Leftrightarrow \Omega, IK_0 \subseteq IK$.又根据协议等价性的条件(2) (3),导出以下两个定理(System 为转换后系统)[8]:

**定理 2** 如果简化函数满足 条件(2) 和(3),则

$$INTRUDER(IK') \subseteq f(INTRUDER(IK)) \qquad (3)$$

$$\forall tr \in traces(SYSTEM), \quad f(tr) \in traces(SYSTEM') \qquad (4)$$

根据协议安全性等价条件和定理 2、定理 3,我们有下面的定理存在:

**定理 3**　设协议 $P1(\Omega 1, \Gamma 1)$ 与通过对 $P1$ 进行安全简化得到的协议 $P2(\Omega 2, \Gamma 2)$ 安全性等价,则如果证明简化后的协议 $P2$ 是安全的,那么原协议 $P1$ 也是安全的.

**证明**　设协议消息集合为 Message,根据定理的前提条件知(P2 sat Secrecy).假设 ¬(P1 sat Secrecy),则

$\exists(M \in Message, trace\ tr \in traces(\text{SYSTEM of P1}), M \subseteq tr)$ 且 $\neg Secrecy(tr) \wedge \neg Secrecy(M)$.

因为 $\Omega 1 \cup IK \rightarrow M \Rightarrow f(\Omega 2) \cup IK' \rightarrow f(M)$,由 $\neg Secrecy(M) \rightarrow \neg Secrecy(f(M))$,而 $f(M) \subseteq f(tr)$ 且 $f(tr) \in traces(\text{SYSTEM of P2})$,因此 ¬(P2 sat Secrecy).又因为 $\exists \alpha$,使得 $\Gamma 2 = \alpha\Gamma 1$.所以,原协议 $P1$ 的安全证明完全可以通过对简化后的协议 $P2$ 进行证明来实现.

### 3.2　简化方法

根据对 DMDP 协议的分析,我们提出简化规则(1)和(2)分别用于替换协议中的中间节点 $D$ 和删除起完整性分析作用的哈希域,以下为简化规则及其证明.

简化规则(1)

$$\begin{matrix} C \rightarrow D : M \\ D \rightarrow ConP : M \end{matrix} \Rightarrow C \rightarrow ConP : M \qquad (5)$$

证明:用 CSP 迹模型描述协议(5)如下:

$$\forall tr', tr'' \wedge (send.D.ConP.M) \leq tr \Rightarrow \exists\ receive.C.D.M\ in\ tr' \qquad (6)$$

设 $data(tr) \triangleq \{M \mid sned.n.D.ComP.M\ in\ tr\}$

由式(5)(6)

$$IK \cup data((tr)) \Leftrightarrow \forall tr', C, D, ConP, M. \left( \begin{matrix} tr''^{\wedge}(receive.C.D.M) \leq tr \\ \vee tr''^{\wedge}(sned.D.ConP.M) \leq tr \\ \vee tr''^{\wedge}(leak, M) \leq tr \end{matrix} \right) \Rightarrow IK \cup data(tr') \vdash M$$

同时,

$$tr \in traces(INTRUDER(IK')) \Leftrightarrow IK'' \cup data(f(tr)) \Leftrightarrow \forall tr', C, ConP, M. \left( \begin{matrix} tr''^{\wedge}(receive.C.ComP.M) \leq tr \\ \vee tr''^{\wedge}(leak, M) \leq tr \end{matrix} \right) \Rightarrow IK'' \cup data(tr') \vdash M \Rightarrow IK'' \cup data(f(tr)) \vdash M$$

由以上推导得出结论:$\Omega \cup IK \rightarrow M \Rightarrow f(\Omega) \cup IK' \rightarrow f(M)$　(7)

定义:$f(IK) \subseteq IK'$　(8)

而代换 $\alpha$ 存在,使得 $\Gamma 2 = \alpha\Gamma 1$　(9)

由式(7)～(9)得出式(5)前后两式安全性等价,因此可以按式(5)进行协议简化.

简化规则(2):

$$C \rightarrow D : M, Hash(M) \Rightarrow C \rightarrow D : M \qquad (10)$$

证明:式(10)推出

if $\Omega \vdash M'$ and $M = Hash(\mid M' \mid)$

then $\Omega \cup IK \vdash M'$

if $f(M') = ATOM\ nil$

then $f(\Omega) \cup IK' \vdash ATOM\ nil = f(M')$

if $f(M') \neq ATOM\ nil$

then $f(\Omega) \cup IK' \vdash f(M, Hash(\mid M' \mid)) = f(M')$

定义:$f(IK) \subseteq IK'$　(11)

同时,存在一般代换 $\alpha$,使得 $\Gamma 2 = \alpha\Gamma 1$　(12)

由以上证明及(11),(12)得出(10)前后两式安全性等价,因此可以按式(10)进行协议简化.

对 DMDP 协议,应用简化规则得到 DMDP 协议的简化协议(协议表达式后边括号内容是为以后证明的方便定义的消息描述符号,分别为发出和接收的消息).

(1) $C \rightarrow ConP : \{C, N_C, OrderID, ContentID, ContentDesp, RightInfo)_{PUB(ConP)}\}$; $(M0, M3)$

(2) $ConP \rightarrow C : \{ConP, N_C, N_{ConP}, OrderID, ContentID, (Totall\,Price)_{PRIV(ConP)}\}_{PUB(C)}, (HDO)_{TK\_HDO}$; $(M1, M4)$

(3) $C \rightarrow ConP : \{(C, N_C, N_{ConP})_{PUB(ConP)}\}$; $(M2, M5)$

(4) $C \rightarrow G : \{(N_C, C, OrderID, ContentID, H((HDO)_{TK\_HDO}), (Total\,Price, CAN, TK\_CA)_{PRIV(C)})_{PUB(G)}\}$; $(M6, M12)$

(4a) $ConP \rightarrow G : \{ConP, N_{ConP}, OrderID, ContentID, H((HDO)_{TK\_HDO}), ((TK\_HDO)_{PRIV(ConP)})_{PUB(G)}, (ConPCAN, Total\,Price)_{PRIV(ConP)})_{PUB(G)}\}$; $(M9, M15)$

(5) $G \rightarrow C : \{(G, N_C, N_G, OrderID, ContentID, (invoice)_{PRIV(G)})_{PUB(C)}, ((TK\_HDO)_{PRIV(ConP)})_{TK\_CA}\}$; $(M7, M13)$

(5a) $G \rightarrow ConP : \{(G, N_G, N_{ConP}, OrderID, ContentID, (note)_{PRIV(G)})_{PUB(ConP)}\}$; $(M10, M16)$

(6) $C \rightarrow G : \{(C, N_G)_{PUB(G)}\}$; $(M8, M14)$

(6a) $ConP \rightarrow G : \{(ConP, N_G)_{PUB(G)}\}$; $(M11, M17)$

## 4　DMDP 安全协议的 SP_Petri 网模型

根据 SP_Petri 网模型定义,我们给出 DMDP 协议的 SP_Petri 网模型,协议模型由分发复合数字对象协议模型和收费、分发密钥协议模型组成,如图 8～10 所示.入侵者攻击能力遵循 Dolev-Yao 模型假设[9],其 SP_Petri 网模型如图 7 所示.SP_Petri 网中消息符号意义参见第 3 节简化协议形式化描述所做的定义.图中,*Control_Conditon* 表示

$(OrderID, ContentID, Total\,Price, H((HDO)_{TK\_HDO}) \in C) \equiv (OrderID, ContentID, Total\,Price, H((HDO)_{TK\_HDO}) \in ConP)$

DMDP 协议的 SP_Petri 网模型由一系列并行和串行进程组成,位置 $P$ 代表参与协议的实体元素或者系

统局部状态,协议运行初始状态为 $M0$,事件发生意味着变迁 $T$ 触发,引起状态 $M$ 变化,弧 $F$ 上的弧函数 $E$ 代表变迁触发的点火条件,包括控制条件(图中没有画出)、名称条件和网络条件. 模型流程遵循 3.2 节转换后流程. 最终结果为协议主体 $C$ 得到密钥 TK. HDO,而主体 $G$ 支付给主体 ConP 从主体 $C$ 的 CAN 中扣除的消费费用.

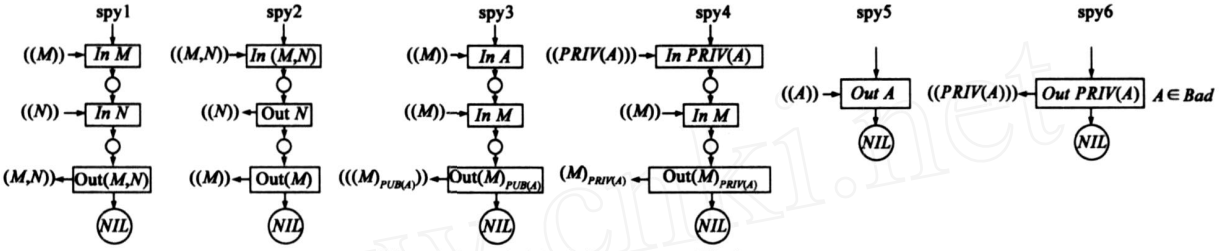



图7 入侵者攻击行为的SP_Petri网模型

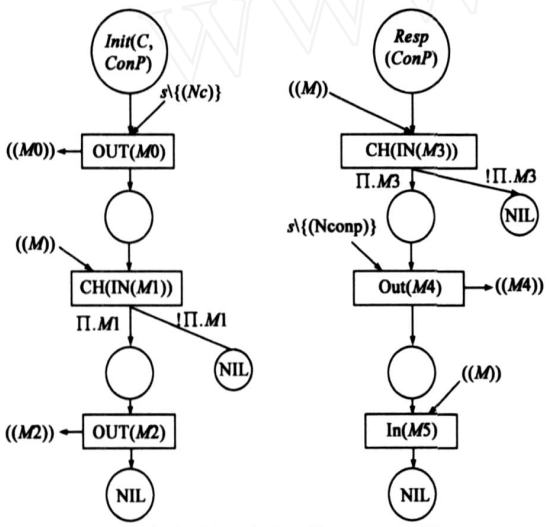



图8 分发复合数字对象协议的SP_Petri网模型

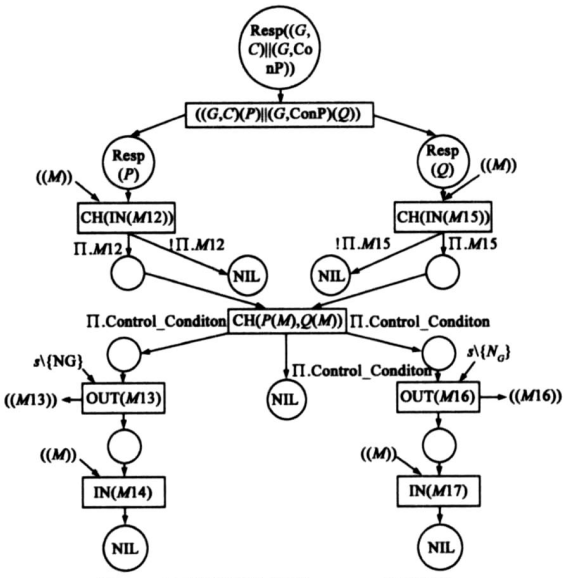



图10 分发密钥协议的SP_Petri网模型

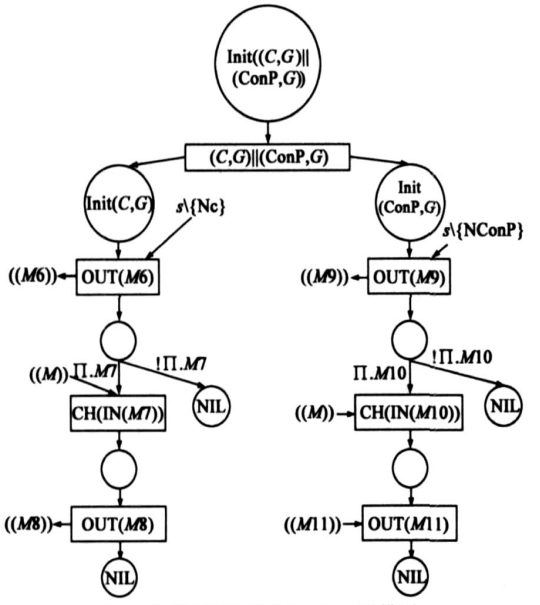



图9 分发密钥协议的SP_Petri网模型

## 5 DMDP 安全协议的证明

### 5.1 消息的机密性证明

**定义 10** 设 $\eta$ 为 DMDP 协议的部分运行段,主体私钥的机密性用 Key 表示,新鲜数的秘密性用 Nou 表示,传递复合数字对象的机密性用 Mse 表示. $key[\eta]=1$ 表示协议运行段的主体私钥满足机密性; $Nou[\eta]=1$ 表示协议运行段 $\eta$ 的新鲜数满足机密性; $Mse[\eta]=1$ 表示协议运行段 $\eta$ 传递复合数字对象满足机密性[10].

**定理 4** 设 $\eta$ 表示 DMDP 协议运行进程,$M0$ 为协议运行的初始状态,如果协议主体 $ConP \notin Bad \wedge G \notin Bad \wedge C \notin Bad$ 并且协议主体的私钥即 $priv(Conp) \notin M0 \wedge priv(C) \notin M0 \wedge priv(G) \notin M0$,则对于属于协议运行的任意状态的消息集合 $M$,主体私钥不会包含于消息集合 $M$ 中. 即 $\forall M \in \eta, \forall M \in M, priv(ConP) \not\subset M \wedge priv(C) \not\subset M \wedge priv(G) \not\subset M$.

**证明**:设 DMDP 协议进程 $\eta$ 以初始状态 $M0$ 开始运行,如图 8,9,10 所示.

$\because ConP \notin Bad$

$\therefore key[M0]=1$

假设 $e \in \eta$,且 $Key[M0 \cdots e] \wedge \neg Key[M0 \cdots eM]$.

考虑图 8,9,10 中向外部发送消息的 out 事件,I-DOP-SP 协议中没有包含 $Priv(Conp)$ 的 out 事件.

考虑图 7 入侵者攻击事件$\{in(M,N).outM.outN.nil\}$,如果 $Priv(ConP)\in M$,则第一个 out 事件 $outM$ 就会使 $Key=0$.

所以 $\exists M'<e$ 使得$((M,N))\in M'$,且 $Key[M0\cdots M']=0$.

而 $\neg Key[M0\cdots M']$与 $Key[M0\cdots e]$矛盾,所以事件 $e$ 不存在.

图 7 其他入侵者攻击事件同样可证明事件 $e$ 不存在.类似地,可对主体私钥 $priv(G)$ 和 $priv(C)$ 进行证明.得出结果 $\forall M\in\eta$, $\forall M\in M$, $priv(ConP)\notin M\wedge priv(C)\notin M\wedge priv(G)\notin M$,即 $Key[\eta]=1$.

**定理 5**　设 $\eta$ 表示 DMDP 协议运行进程,如果 $Priv(Conp)\notin Leak\wedge Priv(CP)\notin Leak\wedge Priv(G)\notin Leak$,其中 $Leak$ 为私钥泄漏主体的集合(以下文章中 Leak 的含义都与此相同),则对于属于协议运行的任意状态的消息集合 $M$,新鲜数 $N_{ConP}$, $N_C$, $N_G$ 不会包含于消息集合 $M$ 中,即 $\forall M\in\eta$, $\forall M\in M$, $N_{ConP}\notin M\wedge N_C\notin M\wedge N_G\notin M\notin M$.

**证明**:假设 DMDP 协议进程 $\eta$ 以初始状态 $M0$ 开始运行,如图 8,9,10 所示.

如果 $Priv(ConP)\in Leak\vee Priv(C)\in Leak\vee Priv(G\in Leak)$,则 $Noun[\eta]=0$.

假定$(Priv(Conp)\notin Leak)\wedge(Priv(CP)\notin Leak)\wedge(Priv(G)\notin Leak)$, $\forall M\in\eta$, $\forall M\in M$, $\exists N_{ConP}\in M$,定义对 $N_{ConP}$的复合操作所得消息为 $Mc$,则 $\exists Mc\in M$.

如果 $Fresh(N_{ConP},e)$,则 $\forall M\in\eta$, $M<e$, $Noun[M0\cdots:M]=1$.

假定 $\exists e$ 且 $Non[M0\cdots e]\wedge\neg Noun[M0\cdots e\ M']$,则 $N_{ConP}\subset M'$分析图 8,9,10 不存在 $out$ 事件使 $N_{ConP}\subset M'$,且 $\neg Noun[M0\cdots e\ M']$.

分析图 7 入侵者攻击事件$\{in(M,N).outM.outN.nil\}$,无法产生包含 $N_{ConP}$的标识 $M'$,分析图 7 其他攻击事件,也得出 $\neg(\exists M'\supseteq N_{ConP})$,且 $\neg Noun[M0\cdots e\ M']$.故这样的事件 $e$ 不存在,即 $\forall M\in\eta$, $\forall M\in M$, $N_{ConP}\notin M$.

类似地,可对新鲜数 $N_C$ 和 $N_G$ 进行证明,得出结果 $\forall M\in\eta$, $\forall M\in M$, $N_{ConP}\notin M\wedge N_C\notin M\wedge N_G\notin M\notin M$,即 $Noun[\eta]=1$.

**定理 6**　设 $\eta$ 表示 DMDP 协议运行进程,如果 $Priv(Conp)\notin Leak\wedge Priv(CP)\notin Leak\wedge Priv(G)\notin Leak$,则对于属于协议运行的任意状态的消息集合 $M$,复合数字对象 HDO 不包含于消息集合 $M$ 中,即 $\forall M\in\eta$, $\forall M\in M$,$(HDO)\notin M$.

**证明**:假设 DMDP 协议进程 $\eta$ 以初始状态 $M0$ 开始运行,如图 8,9,10 所示.根据分析,要证明$(HDO)\notin M$,我们只须证明 $TK\_HDO$ 和 $TK\_CA$ 的机密性.

首先我们证明 $TK\_CA$ 的机密性.

$\because Fresh(TK\_CA,e)$(协议步骤 4)

$\therefore\forall M\in\eta, M_e<e, Noun[M0\cdots:M_e]=1$

设 $\exists e$ 且 $Mse[M_e\cdots e]\wedge\neg Mse[M_e\cdots e\ M']$,则 $TK_CA\subset M'$分析图 8,9,10 不存在 $out$ 事件使 $TK\_CA\subset M'$,且 $\neg Mse[M_e\cdots e\ M']$.

分析图 7 入侵者攻击事件$\{in(M,N).outM.outN.nil\}$,无法产生包含 $TK\_CA$ 的标识 $M'$,分析图 7 其他攻击事件,也得出 $\neg(\exists M'\supseteq TK\_CA)$,且 $\neg Mse[M_e\cdots e\ M']$.故这样的事件 $e$ 不存在,即 $\forall M\in\eta$, $\forall M\in M$,密钥 $TK\_CA\notin M$.

类似地,我们可证明 $TK\_HDO$ 的机密性.即协议运行段 $\eta$ 的消息满足秘密性,$Mse[\eta]=1$.

### 5.2　主体的认证性证明

**定理 7**　设 DMDP 协议中,$e_{ConP}1$, $e_{ConP}2$, $e_{ConP}3$ 分别为主体 $ConP$ 响应主体 $C$ 的第一、第二、第三个事件,对应着 $DMDP$ 协议中 1,2,3 步骤,如果 $Priv(Conp)\notin Leak$ 且 $Priv(C)\notin Leak$,如果存在响应者事件顺序 $e_{ConP}1<e_{ConP}2<e_{ConP}3$ 推导出协议事件顺序为 $e_c1<e_{ConP}1<e_{ConP}2<e_c2<e_c3<e_{ConP}3$($e_c1$、$e_c2$、$e_c3$ 为发起者事件,对应着 DMDP 协议中 1,2,3 步骤)则协议主体 $ConP$ 与 $C$ 满足认证性.

**证明**　$\because e_{ConP_1}<e_{ConP_2}<e_{ConP_3}$ 且 $e_{ConP_1}$ 为 $In$ 事件,分析图 8 可得出,当接收消息与 $M3$ 匹配时控制权才交给 $e_{ConP_2}$,发送消息 $M4$.

$\therefore e_{ConP_1}<e_{ConP_2}$.

当网络消息与 $M5$ 匹配时,事件 $e_{ConP_3}$ 触发.由图 8 看出,$e_{ConP_3}$ 为 $in$ 事件,假设 $\exists e$,且 $e$ 为 $out$ 事件发送消息 $M5$,即 $e_{ConP2}<e<e_{ConP_3}$.

$\because Fresh(N_{ConP},e_{ConP2})\wedge Priv(C)\notin Leak$

$\therefore e$ 的主体为 $C$,故 $e_{ConP2}<e_c3<e_{ConP3}$.

因 $e_{ConP2}$事件为 $out$ 事件,故存在 $in$ 事件 $e2$, $e_{ConP2}<e2$, $e2$ 接收网络消息 $M4$.

$\because Fresh(N_{ConP},e_{ConP2})\wedge Priv(C)\notin Leak$

$\therefore e2$ 的主体为 $C$,故 $e2=e_c2$,又因为 $e_c2<e_c3$.联系以上证明的结论可以得出 $e_{ConP}1<e_{ConP}2<e_c2<e_c3<e_{ConP}3$.又因为 $e_{ConP1}$为 in 事件,必存在事件 $e$ 为 out 事件发送消息 $M3$.

如事件 $e$ 的主体是发起方 $C$,则 $e=e_{c1}$.

如 $e$ 的主体不是 $C$,则 $\exists e1$, $e1<e$. $e1$ 是 in 事件,假设 $e1$ 的主体为 $I$,那么事件 $e1$ 必为主体为 $I$ 的 In 事件,接收新鲜数 $N_C$.

$\because Fresh(N_C, e) \wedge Priv(Conp) \notin Leak \wedge Priv(C) \notin Leak$

$\therefore$事件 $e$ 的主体是发起方 $C$,则 $e = e_{c1}$,即 $e_{c1} < e_{ConP}1$.

综合以上的证明,我们得出结论 $e_c1 < e_{ConP}1 < e_{ConP}2 < e_c2 < e_c3 < e_{ConP}3$,协议主体 $ConP$ 与 $C$ 满足认证性. 同样可证明主体 $G$ 与主体 $C$, $ConP$ 之间的认证性.

依据定理4的证明方法,可对协议消息的不可否认性进行证明,因篇幅关系,具体证明省略.

## 6 结束语

实用安全协议的安全性证明是一件很复杂的工作,形式化方法用一种正规的、标准的方法对协议进行分析证明,为安全协议的设计和使用具有重要的理论和现实意义.

**参考文献**:


[1] Millen J, Rueb H. Protocol - independent secrecy[A]. Proceedings of the 2000 IEEE Symposium on Security and Privacy [C]. Berkeley, California, 2000. 110 - 120.

[2] Canetti R. A unified f ramework for analyzing security of protocols (preliminary version) [R]. Electronic Colloquium on Computational Complexity, ECCC Report TR012016, 2001, 8 (16).

[3] Yingjiu Guo, Chuang Lin, Hao Yin. Design and analysis of IPTV digital copyright management security protocol [A]. Intelligent Signal Processing and Communication Systems [C]. Xiamen, China, 2007. 554 - 557.

[4] 林闯,雷蕾. 下一代互联网体系结构研究[J]. 计算机学报,2007,30(5):693 - 710.
Chuang Lin, Lei Lei. Research on next generation internet architectur[J]. Chinese Journal of Computer, 2007, 30(5):693 - 710. (in Chinese)

[5] 范科峰,莫玮,曹山,赵新华,裴庆祺,数字版权管理技术及应用研究进展[J]. 电子学报,2007,35(6):1139 - 1147.
Kefeng Fan, et, al. Advances in digital rights management technology and application [J]. Acta Electronica Sinica, 2007, 35 (6):1139 - 1147. (in Chinese)

[6] 林闯,随机 petri 网和系统性能评价[M]. 北京:清华大学出版社,2005. 8.
Chuang Lin. Stochastic Petri nets and Performance Evaluation of Systems [M]. Beijing: Tsinghua university press, April, 2005. (in Chinese)

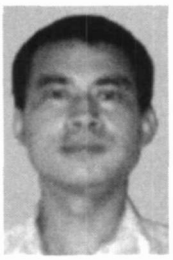
[7] Federico Crazzolara, Glynn Winskel. Petri nets in cryptographic protocols[A]. Parallel and Distributed Processing Symposium, Proceedings 15th International [C]. San Francisco, CA, IEEE Computr Society Apr 2001 Page(s):1507 - 1515.

[8] Mei Lin Hui, Gavin Lowe. Safe simplifying transformations for security protocols or not just the needham schroeder public key protocol[A]. 12th IEEE Computer Security Fondations Workshop [C]. Mordano, Italy: IEEE Computer Society Press, June 28 - 30, 1999. 32 - 43.

[9] Dolev D, Yao A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2):198 - 208.

[10] 王剑,等. 基于 Petri 网的密码协议分析[J]. 计算机工程,2006,28(2):24 - 27.
Jian Wang et al. Analysis of cryptographic protocols based on petri nets[J]Computer Engineering. 2006, 28(2):24 - 27. (in Chinese)


**作者简介**:

**郭迎九** 男,1969 年生于河南卢氏,博士生,研究方向为网络安全与数字版权保护、随机 Petri 网的理论和应用.
E-mail:guoyingjiu @csnet1. cs. tsinghua. edu. cn

**林 闯** 男,1948 年生于辽宁沈阳,教授,博士生导师. 主要研究领域为计算机网络和系统性能模型及评价.
E-mail :chlin @tsinghua. edu. cn