基于半呼叫的SSF模型

任立勇　张　瑜　卢显良
（电子科技大学计算机学院　成都 610054）

摘　要　在半呼叫模型中，要很好地协调业务控制功能SCF和呼叫控制功能CCF，始终是业务交换功能SSF的难点。本文提出一个SSF模型的建立方案。该模型以单点控制为核心，独立区分上下两层功能单元的命令，灵活满足独立业务的需求，解决多业务的冲突问题，并实现多业务的触发。建立触发检出表EDP、事件检出表TDP和业务冲突表CDP是实现上述功能的重要手段，并结合了会话功能SESSION实现业务的映射，从而建立一个高效的SSF模型。

关键词　半呼叫模型，业务交换功能，呼叫连接段，检测触发点

The SSF Model Based on Partly Calls Model

REN Li-Yong　ZHANG Yu　LU Xian-Liang
(School of Computer Science and Engineering, UESTC, Chengdu 610054)

Abstract　The BICC agreement which planted in backbone network is Bearer-Independent-Call-Control protocol. This agreement is used for distinguishing the call controlling function (CCF) and service controlling function(SCF), used the "partly calls model". Nevertheless, it is difficult to harmonizing the SCF and CCF by service switch function (SSF). The main body of this paper brings forward a SSF model. That model is centering on single detection point controlling, distinguishing the orders from SCF and CCF, supplying the service needs, solving the conflicting problem and triggering the services. The EDP table, TDP table and the CDP table are the ways for actualizing those ideals. All of them combined with the SESSION have built a high-effect SSF model.

Keywords　Partly calls model, SSF, CSA, DP

1　引言

在电路域中建立一个呼叫，必然需要经历两个过程(或者说两个层次)：信令层的连接建立和媒体层的连接建立，而且信令层的连接建立一定早于媒体层连接的建立。完成这两个连接建立的控制单元分别称为呼叫控制单元和媒体控制单元。同时，呼叫过程中可能涉及一些呼叫业务，所以呼叫过程中还存在一个业务逻辑单元。

本文将从智能网的两大基本标准"业务实现与业务承载分离、业务控制与呼叫控制分离"入手介绍了半呼叫模型的逻辑结构、SCF和CCF的功能单元，接着对SSF的功能进行了研究，最后提出了本文的SSF模型。

整个模型的建立分为两个主要的方向，由业务控制层下把命令发到呼叫控制层和由呼叫控制层上发命令到业务控制层。通过对SSF功能的研究，模型围绕业务触发点DP的控制，即EDP表、TDP表的创建、维护和实现进行分析；当同一BCSM多次触发业务后，对新业务的处理方式即CDP表的创建、维护和实现进行描述；为了维护SCF和CCF的相互独立，设计了相关数据的存放、使用；设计多业务同时触发后，各个业务的独立管理的模型。

最后通过真实环境的测试，说明按照此思路的设计，本模型能很好地完成对"半呼叫"模型的支持，证实了本文的SSF模型设计的合理性和正确性。

2　半呼叫模型概述

半呼叫模型试图实现业务控制和呼叫控制的分离，解决一个呼叫中信令层连接的建立，并触发媒体层连接和完成一定的交互。半呼叫模型首先从两个层面对现实世界中的呼叫过程进行抽象：

(1)主叫端或者被叫端在呼叫过程中所经历的若干状态层面抽象出基本呼叫状态模型BCSM(图1)。BCSM对呼叫过程中的状态进行抽象描述，它包含了呼叫连接过程中状态及事件的变迁。BCSM根据发端和终端的不同分为O_BCSM和T_BCSM。它们之间相互独立，通过信令进行相互影响。

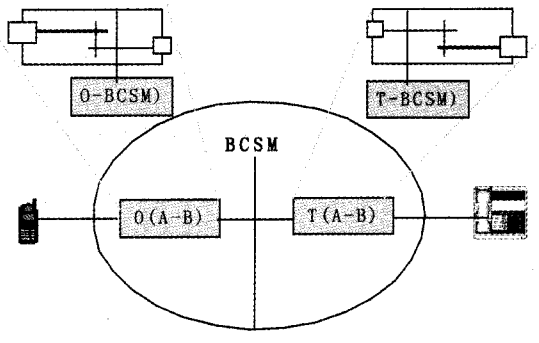


图1　BCSM的半呼叫模型

在BCSM中引入了呼叫点PIC的概念，即用PIC表示为完成业务逻辑功能所需进行的处理。每个呼叫过程可以从逻辑上分为多个PIC点。PIC点可以对入口事件根据其当前状态进行处理，同时对处理过程中收到的消息进行相应处理，之后根据不同的处理结果产生对应的出口事件。主叫端有11个PIC点，分别是："初始"、"始呼鉴权"、"收集信息"、"分析信息"、"路由选择"、"呼出鉴权"、"发起呼叫"、"震铃"、"建立呼

叫”、“呼叫悬置”、“异常”。被叫端有 8 个 PIC 点，分别是：“初始”、“呼入鉴权”、“路由选择”、“发起呼叫”、“震铃”、“建立呼叫”、“呼叫悬置”、“异常”。在每个 PIC 点的入口处设立检测点 DP。DP 是一些可以通过静态和动态配置的事件触发点，可以对入口事件进行判断，并对满足触发条件的事件进行上报。同时，DP 根据配置属性的不同而采取相应的处理机制，即：或只是上报事件，不等待 SCF 发送指令；或上报后暂停呼叫连接处理，等待 SCF 的指令。SCF 根据 DP 的上报事件，可以了解呼叫状态，也可以发送相应指令对呼叫连接进行控制。

(2)从主叫端或者被叫端在整个呼叫过程中连通性的变化抽象出引脚 LEG、连接点 CP、呼叫段 CS 和呼叫段关联 CSA，也就是连接视图 CV。SSF 所看到的 CCF 是数量众多的 LEG，SSF 的工作就是要找到主叫 LEG 和被叫 LEG，然后把它们连接起来，连接的方式就是把两条 LEG 同时连接到一个连接点 CP 上。同时 CCF 认为不同的 CS 之间并不是彼此独立的，在特定条件下它们可以关联起来形成 CSA。

SCF 描述整个网络完整的呼叫过程，也就是描述 CVS 的状态变迁过程，共有 14 个状态。把所有状态串连起来就形成了状态迁移图。SCF 根据 CVS 状态迁移图运用 INAP 接口，形成不同的状态迁移，完成不同的补充业务。

业务交换功能是连接 SCF 和 CCF 的“桥梁”，描述 CSA 的 CS 和 LEG 的连接拓扑结构、处理 CCF 上报 DP 事件、实现呼叫过程中的业务触发和业务冲突防止，以及为后续的业务控制提供会话和 EDP 表机制。对特殊资源进行请求的时候，通过对特殊资源功能 SRF 发出请求。

3 SSF 模型设计

通过对 SCF 和 CCF 功能的研究，分析了它们之间的区别和联系，本文建立以下的 SSF 模型。模型以独立的 TOPO 和 DPHANDLER 两大模块区分并处理 SCF 和 CCF 向下向上的命令，对公有的属性集中在 SESSION 模块中处理。本模型的中心思想是以单点控制为核心(同一 DP 点的控制权只属于一个业务)。以 EDP 表、TDP 表和 CDP 表为手段，完成对单业务的触发、业务的控制、多业务的冲突、多业务的触发问题的解决。根据 EDP/TDP/CDP 表的属性分别放在 SESSION 和 DPHANDLER 子模块中管理。另外，对外消息的分发统一到独立的功能模块 IH(Interface Handler)(图 2)。

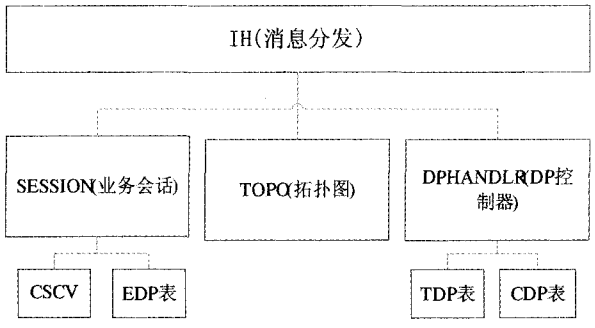


图 2 SSF 的模型内部结构

IH：各资源的创建及销毁者，外部消息分发接口。

SESSION：每个业务实例 SLI(SCF 侧的一个具体业务)的映射，CSCV/EDP 表的所有者。

CSCV：维护 CS 的上下对应视图，保持 CS 的状态迁移关系，是一个状态机。

EDP 表：一个动态的表数据，事件检出点表。

TOPO：对 SCF 关注 DP 点跳转的控制，并保存 CCF 侧的 CVS 图。

DPHANDLER：DP 点消息上报单元，TDP 的所有者。

TDP 表：一个静态的表数据，触发检出点表。

CDP 表：一个静态的表数据，冲突检出点表。

DP 上报流程：DP 事件产生后，上报给 DPHANDLER，DPHANDLER 顺序检查 TDP 和 CDP 表。如果两个表都满足对应的触发条件，则上报给 SESSION，并给 DP 点相应的命令。SESSION 通过判断 CS 的状态，并对比 EDP 的数据，在满足条件的情况下上报 DP 信息给 SCF。

SCF 下发事件：一个事件发送到 SESSION。SESSION 首先判断 CS 的状态，在合理的情况下，修改 CVS 图，然后发送命令给 TOPO。TOPO 分析命令后，将信令上发送到 BCSM，让 DP 迁移状态、特殊资源请求发送给专用资源功能 SRF。

以下将对 SSF 子模型的具体功能和原理进行描述。

(1)EDP 表、TDP 表、CDP 表

EDP 表和 TDP 表是从半呼叫模型中 DP 点的四个类型分离而来。DP 的配置是为了通知 SLI 遇到了 DP，从而使 SLI 可以影响随后的呼叫处理。如果 DP 没有配置，则 SSF/CCF 继续原来的呼叫处理而不涉及到 SCF。DP 点有以下类型：

a)触发检出点－请求(TDP-R)；

b)触发检出点－通知(TDP-N)；

c)事件检出点－请求(EDP-R)；

d)事件检出点－通知(EDP-N)。

EDP 表保存了 SLI 呼叫中相应 DP 点的动态关注状态。EDP 表的配置如下：SCF 下放“配置 EDP 表”命令并动态添加到表中，并且每个 EDP 表的信息是配置在对应 LEG 上面的。如果 LEG 不存在了，则删除其对应的 EDP 表信息。EDP 表的运用如下：DP 点上报信息后，在 SESSION 部分检测 EDP 表。如果是 EDP-R，则让对应 DP 点悬置在当前状态不迁移；如果是 EDP-N，让 DP 点按照默认 DP 迁移流程运行。EDP 表的创建如下：IH 创建 SESSION 时，SESSION 自动创建了一个空的 EDP 表，其实就是一个空的容器(表 1)。

表 1 EDP 表

字段	说明
DP 号	主叫端和被叫端统一编号共 19 个
类型	是 EDP-R 或者 EDP-N
LEG 号	此表配置所在腿的腿号
触发条件	这条腿出发 DP 点的上报条件

EDP 表相关命令：

ARMEDP：由 SCF 下发配置一组表的命令，由四个字段和成一个唯一的表项。

DISARMEDP：由 SCF 下发的清空 EDP 表命令。

EDPRREPORT：EDP-R 的上报命令，每个表项成功上报后删除。

EDPNREPORT：EDP-N 的上报命令，每个表项成功上报后删除。

EDP 表体现了一种“关系”。当遇到一个配置的 DP，并且满足 DP 标准，则 SSF 可以通过“关系”传递信息流。如果 SCF 通过这个“关系”可以影响呼叫处理，则认为这个“关系”是“控制”关系；如果 SCF 通过这个“关系”不能影响呼叫处

理，则认为这个“关系”是一个“监视”关系。当对应 LEG 所存在 BCSM 的 EDP-R 数目 N≥1 时，是一种“控制”关系，否则当 EDP-N 数目 N≥1 是一种“监视”关系。

TDP 表是主要作用于补充业务初始触发的。TDP 表的配置如下：从网管侧读得静态信息，信息加载后就不会改变。TDP 表的运用如下：当 DP 上报后，DPHANDLER 检查 TDP，如果对应的 DP 点在 TDP 表中有相应的表项，则触发对其应业务。TDP 表的创建如下：在一个呼叫建立起来后，就马上创建 TDP 表，其实就是一个空的容器(表 2)。

表 2　TDP 表

字段	说明
DP 号	主叫端和被叫端统一编号共 19 个
类型	TDP-R 或者 TDP-N
优先级	多个 DP 点上报后的优先选择
触发条件	DP 上报的条件
补充业务号	对应的补充业务

TDP 表相关命令：

ARMTDP：由网管侧一次性导入所有数据。

SELECTEDP：根据 DP 点的上报，查询表项。

TDPRPROCESS：TDP-R 处理函数。

TDPNPROCESS：TDP-N 处理函数。

由于一个 DP 在同一个呼叫中可能被配置为一个 TDP 和/或 一个 EDP，因此 BCSM 应该在 DP 处理期间应用下面一组规则以保证单点控制：

规则 1：对于任何 DP，一个规定的触发条件一次只能触发一个业务逻辑程序实例 SLI。

规则 2：对于任何 DP，处理通知 EDP-N 和 TDP-N 具有高于处理请求 EDP-R 和 TDP-R 的优先级。如果多个通知存在，当所有的通知都被处理完时，才处理 EDP-R 和 TDP-R。

规则 3：如果一个 DP 同时被配置为 EDP 和 TDP，由于 EDP 是在一个已经存在的 SSF-SCF 关系中配置的，EDP 处理的优先级高于 TDP 处理的优先级。

规则 4：如果一个 DP 同时被配置为 EDP-R 和 TDP-R，则 EDP-R 先处理；EDP-R 处理的结果是结束控制关系，则允许 TDP-R 处理(表 3，参看中国智能网设备业务交换点 SSP 技术规范)。

表 3　EDP/TDP 处理的组合

流称	TDP 类型	EDP 类型	存在的关系	处理
1	未配置	未配置	不介意	继续
2	TDP-R	未配置	不存在	启动 DP 请求
3a	TDP-R	未配置	控制	继续(忽略 TDP)
3b	TDP-R	未配置	监视	启动 DP 请求
4	TDP-N	未配置	不介意	单向 DP 通知，启动检视关系。
…	…	…	…	…

CDP 表是实现上图 EDP/TDP 处理的组合，它的存在从根本上避免了不可并发的业务、不可嵌套的业务出现和实现单点控制。

CDP 的相关命令：

GETRESULT：获得存在的关系。

GETPROCESS：分别调用相应的处理，可以直接从 EDP 或者 TDP 表调用接口完成。

(2)DPHANDLER

一旦触发呼叫，IH 立刻建立 DPHANDLER，并把 TDP 和 CDP 表建立好。处理 DP 点的上报，根据 CDP 表中的数据，按照上述规则把 DP 的信息上报给 SESSION，同时维护两个表 TDP 和 CDP。

(3)SESSION

SESSION 是和一个具体的业务实例对应的功能单元。当补充业务触发后，IH 会自动建立 SESSION，并自动构件一个包含一条主动 LEG 和一条被动 LEG 的 CS。这里的 LEG 不用维护状态信息，CS 在空闲状态。SESSION 要保存 CS 的状态，由 CSCV 类的状态机模式来维护(图 2)。

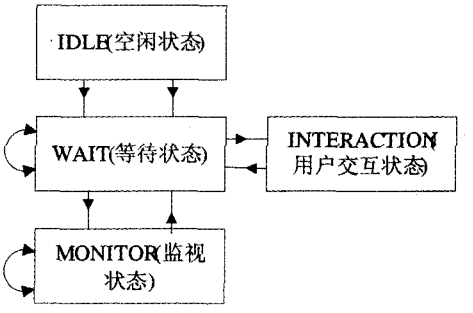


图 2　CS 的状态

SESSION 维护 CCF 侧的 CVS 图和 SCF 侧的 CVS 图，同时保存两套 CS 号和 LEG 号并维护 EDP 表。每一个 SESSION 和一个 SLI 对应。当 CCF 侧同一个 BCSM 有多个业务触发后，在 SCF 侧不加区分，看作是两个独立的 BCSM；而在 SESSION，则要把 SCF 侧和 CCF 侧的连接正确对应起来，这样就把多业务并行问题解决了。此模型根据系统的性能可以同时触发多个 SESSION，也就是多个 SLI 并行处理(图 3)。

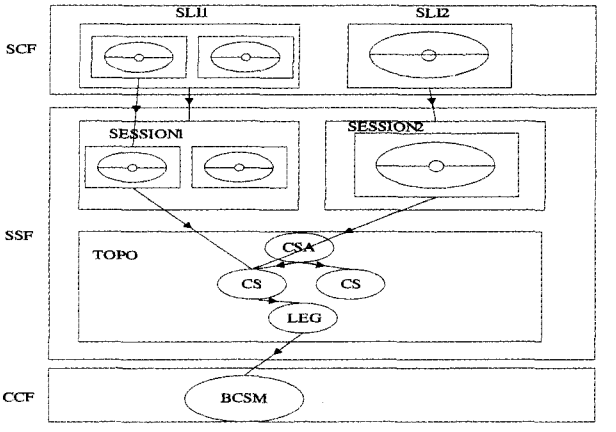


图 3　SESSION 映射图

(4)TOPO

TOPO 是完成解释 SCF 下放命令，并让 DP 按照业务的需求跳转的功能单元，并保存了 CCF 所看到的 CVS 图，由类 CS 保存。TOPO 在呼叫刚开始建立时初始化，初始的时候保存一个 CS，并有两条在虚态下的 LEG(注意：在 TOPO 中 CS 不用再保留状态)。以 SCF 下发的“事件”中的断腿命令为例子 DISLEG：SESSION 判断 CS 状态等信息，下发断脚消息给 TOPO。根据 CS2 规范的规定，TOPO 下发 GOTOPIC 命令让没有进入“中间呼叫点”的 DP 点进入。如果已经进入，保持状态不迁移。

(下转第 74 页)

这里只是对最简单情况进行一下仿真演示。由于加解密的速度非常快，因此在实际应用中，规则半径通常要取 $r>10$ 以上，以达到实用的安全强度。

4.2 安全性分析

安全性分析中很重要的一项就是研究明文或密文改变一位后密文和明文的变化。通常采用改变一位明文编码后最终密文的改变结果与原来的加密结果进行比较，如果相同则用"-"表示，不同则用"#"表示。表 6～7 给出在相同明文中的相同扰乱引起的误差传播过程的比较。

表 6 耦合单触发元胞自动机中的误差传播

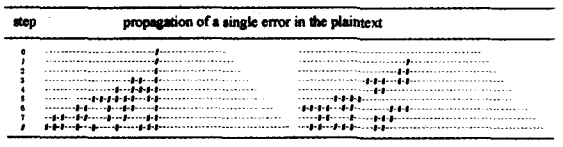
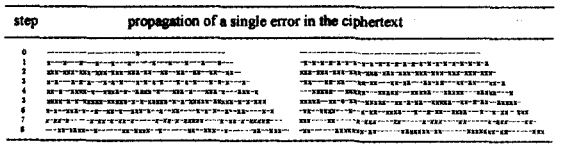


表 7 耦合双触发元胞自动误差传播



从表 6～7 可以看出，这种方法可以大大提高对密文的扰乱程度，只要几步就可以使误差扩展到整个密文，避免密文中的相似性问题，从而能够抵抗差分分析方法攻击。

在加密和解密过程中，密钥采用 CA 系统本身，当半径 $r=4$ 时，密钥空间达 $2^{2^{2r-1}}\times 2^{2^{2r-1}}\approx 1.16\times 10^{77}$。在相同的规则半径下，远远大于目前所见文献中提到的本类方法的密钥空间[10]。而且密钥空间随着规则半径 r 的增大呈指数增长。因为 CA 的并行特性，其加解密速度较快，在实际应用中，规则半径应选取 $r>10$，蛮力攻击变得不可能，系统在计算上是安全的。对同一明文加密，由于每次引入不同的随机数，因此每次得到的密文是不同的，但是解密后得到的明文却是相同的，很难得到唯一的明文密文对，因而可以抵抗已知明文和已知密文的攻击。

结论 本研究基于元胞自动机之间状态演化的互动性，以及触发元胞状态值与规则半径对演化状态的支配性，构造出耦合双触发元胞自动机的加密系统。解决了通常触发元胞自动机的加密算法中误差传播小而且是单向的相似性问题，同时大大提高密钥空间。分析表明，这样不仅具有抵抗穷举法的蛮力攻击和已知明文、已知密文的攻击的能力，同时具有抵抗差分分析的能力。

参 考 文 献

1 Lai C. High-speed cellular-automata based block cipher and fault tolerant public-key cryptosystems: [M. Sc.]. Regina: The University of Regina, Canada, 2000

2 Wolfram S. A New Kind of Science. Illinois: Wolfram Media, Inc, 2002. 1192

3 Martin del Rey A. A Novel Cryptosystem for Binary Images. Studies in Informatics and Control, 2004, 13(1): 5～14

4 Li H, Zhang C N. A Cellular Automata Based Reconfigurable Architecture for Hybrid Cryptosystems. Computer Journal, 2004, 47(3): 320～328

5 Seredynski F, Bouvry P, Zomaya A Y. Cellular automata computations and secret key cryptography. Parallel Computing, 2004, 30(5-6): 753～766

6 Oliveira G M B, Coelho A R, Monteiro L H A. Cellular automata cryptographic model based on bi-directional toggle rules. International Journal of Modern Physics C, 2004, 15(8): 1061～1068

7 Gutowitz H A. Method and apparatus for encryption, decryption and authentication using dynamical systems. USA, 1994. 34

8 Chopard B, Droz M. 物理系统的元胞自动机模拟. 祝玉学，赵学龙译. 北京：清华大学出版社，2003

9 赵学龙. 耦合触发元胞自动机在数据加密中的应用. 信息与控制，2005,34(6):746～752

10 张传武，沈野樵，彭启琮. 细胞自动机反向迭代加密技术研究. 计算机学报，2004，27(1)：125～129

（上接第 44 页）

4 SSF 模型测试

本模型的建立从理论上实现了灵活业务和基本呼叫的分离，并且以简约的模型使业务控制效率不会在 SSF 这一层受到制约。在试验中，以此模型建立 SSF，作为以高级业务功能为代表的 ACP 和以基本业务为代表的 BCP 的中间层，形成 ACP-SSF-BCP 的整体模型，成功地完成了各项补充业务，在呼叫效率上也达到了试验的目的。下面的图例说明了实现的补充业务中消耗在 SSF 这一层所需要花费的微秒值(图 4)。

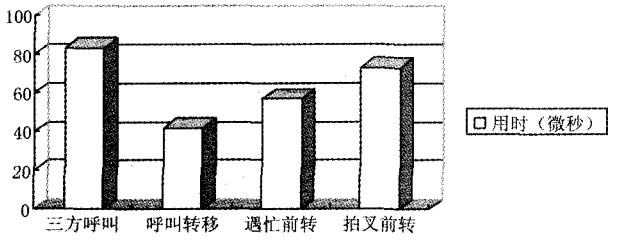


图 4 业务效率图

结论 软交换是下一代通信网络的核心控制设备，其中又以呼叫模块为其核心。在半呼叫为核心的网络中，上述的 SSF 模型很好地完成了 SCF 和 CCF 之间的桥梁作用。以单点控制为核心，以上下两条命令流程为建立模型基础，清晰简约地解决了 SSF 所面临的多种问题，并以 TDP 表的方式解决了单业务的触发问题，以 EDP 表的方式解决了业务的控制问题，以 CDP 表的方式解决了多业务的冲突问题，最后以 SESSION 为子模块的设计解决了多业务的并发问题。经过实践的证明，这样的 SSF 模型是一种合理的、可靠的设计。

参 考 文 献

1 Lu Huilan. Network evolution in the context of the global information infrastructure. Communications Magazine, 1998, 36(8): 98～102

2 Huitema C. An architecture for residential Internet telephony service. IEEE Network, 1999, 13(5): 50～56

3 Rosenberg J. Session initiation protocol. RFC3261, Intrnet Engineering Task Force, June 2002

4 Cuervo F. *Megaco Protocol Version 1. 0. RFC3015*, November 2000

5 Ong L, Rytina I, Garcia M. Framework Architecture for Signaling Transport. RFC2719, Internet Engineering Task Force, October 1999

6 中华人民共和国邮电部.《中国智能网设备业务交换点(SSP)技术规范》