SUPANET中的虚通道切换方式研究

高 雨 曾华燊 窦 军

(西南交通大学信息科学与技术学院 成都 610031)

摘 要 以一种新的单物理层用户数据传输与交换平台体系结构(Single physical layer User-data transfer & switching Platform Architecture,SUPA)为研究背景,针对Internet与SUPA互联时由移动节点引起的虚通道切换问题,提出了两种基本的虚通道切换方式和一种混合的虚通道切换方式,并对每种虚通道切换方式进行了特点分析和仿真实验。仿真实验结果表明,混合切换方式的综合性能明显好于其他两种基本切换方式。

关键词 SUPANET,虚通道,切换方式

中图法分类号 TP393.03 **文献标识码** A

Research on Virtual Tunnel Handover Method in SUPANET

GAO Yu ZENG Hua-shen DOU Jun

(School of Information Sciences and Technologies, Southwest Jiaotong University, Chengdu 610031, China)

Abstract Based on a new architecture called SUPA (Single physical layer User-data transfer & switching Platform Architecture) and the virtual tunnel handover problem which is caused by mobile node when Internet interconnected with SUPA network, this paper proposed two basic virtual tunnel handover methods and a mixed virtual tunnel handover method, then analyzed characteristics of each handover methods. Simulation results show that the mixed method is better than other basic methods.

Keywords SUPANET, Virtual tunnel, Handover method

随着互联网应用向多媒体化、移动化发展,现有Internet面临着高速交换、服务质量保障、网络安全和移动性问题的挑战。为了解决上述问题,四川省网络通信技术重点实验室根据对OSI/RM和Internet体系结构问题的分析,为进一步发挥"带外信令"思想的优势,提出了以面向以太网物理帧时槽交换(Ethernet-oriented Physical Frame Timeslot Switching, EPFTS)技术[1](本文简称PFTS技术)为基础的单物理层用户数据传输与交换平台体系结构[2;3](Single physical layer User-data transfer & switching Platform Architecture, SUPA),使用SUPA体系结构的网络被称为SUPANET。

在解决高速交换和服务质量(Quality of Service, QoS)保障问题上,SUPANET在用户数据平台(U-Platform)以物理帧为交换单元,根据QoS调度算法[4-6],在物理层进行高速的数据交换;通过信控管理平台(S&M-Platform)[7]的信令机制[8-11],在U-Platform建立端到端的虚通道(Virtual Tunnel, VT),并在相关交换节点上预留时槽资源,从而使得物理层能够为上层提供可度量的、可控制的、面向连接的端到端QoS保障服务。

在解决从现有的Internet向下一代Internet平滑过渡问题上,实验室提出了"首先以SUPA体系结构为基础建立能够应对上述挑战的Internet骨干通信子网,把现有各类网络视为接入网络,保持与现有网络,特别是Internet的互联互通性,待各类技术成熟后再逐步向用户端延伸"的BSF-OES (Backbone Substrate First, Outwards Expansion Second)策略[12]。但该策略首先需要解决SUPANET与Internet的互联互通问题[13]。鉴于Internet应用的移动化趋势,移动性问题是SUPANET与Internet互联时需要考虑的主要问题之一。

由于SUPANET采用面向连接的虚通道方式传递用户数据,传统的Internet移动性管理技术(如移动IP[14])不能直接解决SUPANET内部的数据通道切换问题[15]。因此,有必要研究Internet移动终端引起的SUPANET虚通道切换问题。

本文针对上述虚通道切换问题,在SUPANET的虚通道机制基础上,首先提出了两种基本的虚通道切换方式,分析了每种基本切换方式的特点,进而提出了一种混合的虚通道切换方式,并通过仿真实验证明了混合虚通道切换方式具有更好的切换性能。

1 SUPANET的虚通道机制

SUPANET由SUPA终端、PFTS交换节点、PFTS边界节点以及SUPA网关节点构成。SUPANET通过SUPA网关节点与Internet互联,如图1所示。SUPA网关是一个双协议栈的节点,对Internet而言,它相当于一个Internet路由

到稿日期:2009-06-16 返修日期:2009-08-31 本文受国家自然科学基金(NGI体系结构-SUPA及其核心技术研究,No. 60773102)资助。

高 雨(1982-),男,博士生,主要研究方向为下一代网络体系结构等,E-mail:gaoyu666@gmail.com;曾华燊(1945-),男,教授,博士生导师,主要研究方向为网络体系结构等;窦 军(1963-),男,副教授,主要研究方向为网络体系结构等。

器，对于 SUPANET 而言，它相当于一个 SUPA 端系统。

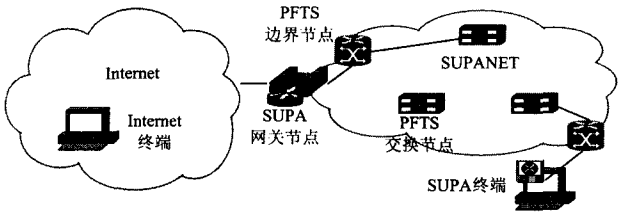

图 1　SUPANET 与 Internet 互联示意图

1.1　虚通道概述

虚通道(VT)是一对 SUPA 网关节点之间的端到端数据传输通道，它可以看成在一个波长的数据传输容量内划分的子信道。面向以太网物理帧(Ethernet-oriented Physical Frame，EPF)是 PFTS 中的标准数据传输和交换单元，单个 EPF 的传输时间被称为基本时槽(Timeslot)，用户数据在 SUPA 网关(或 SUPA 终端)处被封装到 EPF 中，经过相应的 VT，传输到目的 SUPA 网关(或 SUPA 终端)。

一条单向的虚通道，通过一组有序的虚线路标识符(Virtual Line Identifier，VLI)来进行唯一标识。如图 2 所示，1->6->8->2 和 6->7->3->3 分别是两个 SUPA 网关之间的两条方向相反的虚通道，这一对虚通道可以承载这对网关节点之间的某一个业务或某一类业务的数据。

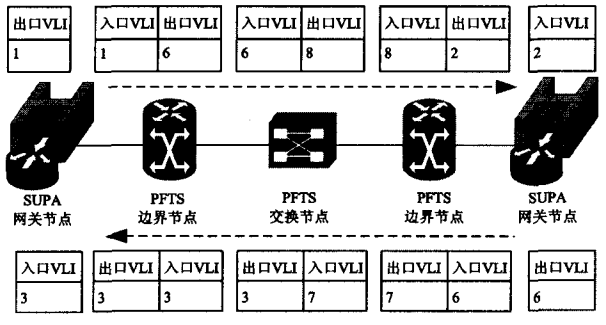

图 2　虚通道示意图

1.2　虚通道的建立

虚通道的建立方法有单向单独建立和双向同时建立两种[11]，本文只以双向同时建立这种方式为例。

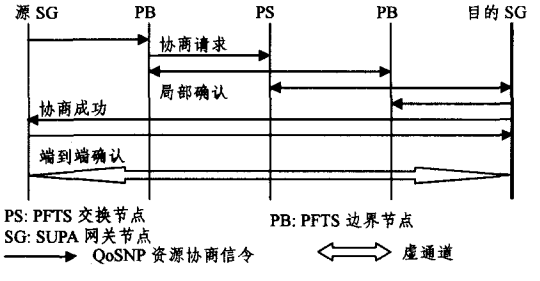

图 3　虚通道建立示意图

如图 3 所示，SUPA 网关收到来自 Internet 的业务连接请求后，将根据业务流的目的地址和相关 QoS 参数信息，按照 QoS 路由算法提供的最优路径，利用服务质量协商协议(QoS Negotiation Protocol，QoSNP)[10,11]的资源协商预留功能向路径上的 PFTS 边界节点和 PFTS 交换节点逐跳转发“协商请求消息”，逐跳协商并预留时槽资源，并利用“局部确认消息”在相邻节点间分发 VLI，填写虚线路交换表(如图 4 所示)，建立 VLI 映射关系，直到目的 SUPA 网关。若整条路径协商成功，目的 SUPA 网关将向源 SUPA 网关发送端到端的“协商成功消息”，收到该消息后，源 SUPA 网关再向目的 SUPA 网关发送“端到端确认消息”。最终在一对 SUPA 网关之间建立起一对用于双向通信的虚通道，并将相关信息填入 SUPA 网关的虚通道信息表(如图 5 所示)。

入口 VLI	出口 VLI	时槽总数	出口端口号与波长号

图 4　PFTS 交换节点中的虚线路交换表

虚通道编号	虚通道类型	时槽总数	出口 VLI	出口端口号与波长号

图 5　SUPA 网关处的虚通道信息表

虚通道建立好后，业务流数据被封装成 EPF 帧在物理层进行交换转发，其帧结构如图 6 所示，EPF 帧头的 VLI 字段决定了该 EPF 属于哪个虚通道，优先级字段标识该 EPF 所属虚通道的优先级。

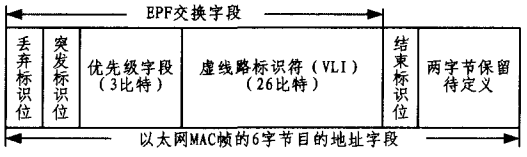

图 6　EPF 交换字段格式与意义示意图

1.3　虚通道的拆除

如果需要拆除某个虚通道并释放其占用的资源，SUPA 网关节点将使用 QoSNP 的资源释放功能释放该虚通道预留的全部资源，并删除各节点上关于该虚通道的 VLI 映射关系，彻底拆除该虚通道，其流程与虚通道建立流程类似。

2　虚通道的基本切换方式

如图 7 所示，假设两个 Internet 终端：移动节点(Mobile Node，MN)和对端节点(Correspondent Node，CN)，正通过 SUPANET 进行通信。当 MN 在位置 1 时，用户数据通过旧 SUPA 网关(O-GW)和对端 SUPA 网关(C-GW)之间的虚通道 VT1 进行传递。当 MN 从位置 1 移动到位置 2 后，用户数据需要切换到新 SUPA 网关(N-GW)和对端 SUPA 网关(C-GW)之间的虚通道 VT2 进行传递。

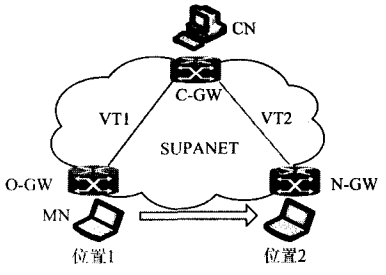

图 7　虚通道切换示意图

从 VT1 到 VT2 的切换过程称为虚通道切换，基本的切换方式可分为虚通道重建和虚通道延伸两种。

2.1　虚通道重建

虚通道重建(Virtual Tunnel Rebuilding，VTR)切换方式的基本思想是：在 N-GW 和 C-GW 之间重新建立一条虚通道，替代 C-GW 与 O-GW 之间的原始虚通道。

1. 切换过程

(1)如图 8 所示，N-GW 收到切换请求消息后，向 C-GW 发起虚通道建立请求(流程如 1.2 节所述)，建立虚通道 VT2。

(2)当 VT2 建立成功后，将 MN 与 CN 间的用户数据切换到 VT2 上。

(3)C-GW 向 O-GW 发起虚通道拆除请求，拆除 VT1，释放相应资源。

(4)下一次连续切换流程同上。

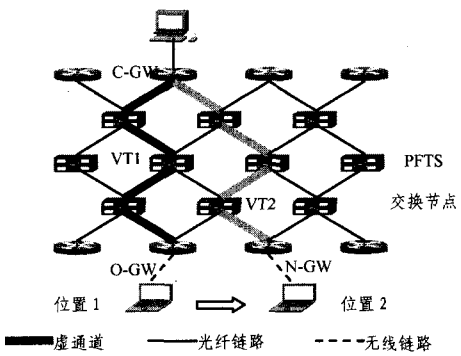

图 8 VTR 切换方式示意图

2. 切换性能分析

(1)切换时延

在不考虑虚通道建立失败的情况下，VTR 需要进行一次端到端的 QoSNP 双向协商流程，其切换时延主要取决于 QoSNP 双向协商所经历的节点数(或跳数)，假设协商所经节点数为 n，第 i 次连续切换的切换时延可表示为：

$$T_i = 3 \times n_1 \times t$$

其中，n_1 是 N-GW 到 C-GW 的最佳路径跳数，t 是 QoSNP 消息的每跳传输和处理时延。

(2)切换后的 QoS 保障

由于 QoSNP 利用 QoS 路由算法寻找 QoS 最优的路径建立 VT，而 VTR 利用 QoSNP 进行了端到端的 VT 重建，因此新 VT 的 QoS 参数(时延、抖动、数据率)是当前的最优选择。

(3)技术复杂度

沿用已有的 QoSNP 协议和虚通道机制，技术复杂度低。

(4)超前操作的支持程度

超前操作是指在 MN 离开当前网络前(即在 O-GW 管辖内)开始虚通道切换操作。VTR 由于是由 N-GW 发起新 VT 而建立请求，因此基本不支持超前操作。

2.2 虚通道延伸

虚通道延伸(Virtual Tunnel Extension，VTE)切换方式的基本思想是：O-GW 和 C-GW 之间的虚通道继续使用，在 O-GW 和 N-GW 之间建立一条新的虚通道，与原有虚通道一起构成切换后的数据传输通道。

1. 切换过程

(1)如图 9 所示，O-GW 收到切换请求消息后，向 N-GW 发起虚通道建立请求，建立虚通道 VT2。

(2)VT2 建立成功后，在 O-GW 处建立 VT1 和 VT2 的映射关系，对 MN 与 CN 间的用户数据进行中转。

(3)下一次连续切换时，按同样的原则建立 VT3，MN 与 CN 间的用户数据通过 VT1，VT2 和 VT3 进行传递。

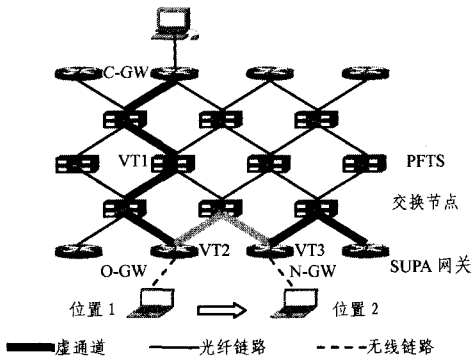

图 9 VTE 切换方式示意图

2. 切换性能分析

(1)切换时延

在不考虑虚通道建立失败的情况下，VTE 需要进行一次相邻 SUPA 网关之间的 QoSNP 双向协商流程，切换时延取决于相邻网关间的跳数，连续切换时的切换时延相对固定，第 i 次连续切换的切换时延可表示为：

$$T_i = 3 \times n_2 \times t$$

其中，n_2 是 N-GW 到 O-GW 的最佳路径跳数，t 是 QoSNP 消息的每跳传输和处理时延。

(2)切换后的 QoS 保障

由于 VTE 采用虚通道不断延伸的方式，切换后的端到端时延不是最优，并会随着切换次数的增加而增大，甚至最终无法满足业务的需求，因此，VTE 方式不适合于连续切换次数较多的场景。

(3)技术复杂度

在沿用已有的 QoSNP 协议和虚通道机制的同时，需要在 SUPA 网关增加虚通道之间的映射表，并管理该映射关系。MN 与 CN 通信结束后，需要依次拆除多个虚通道。

(4)超前操作的支持程度

由于 VTE 由 O-GW 发起，且扩展虚通道建立好后，只要不改变 O-GW 的映射表，MN 仍然能通过 O-GW 收发数据，当 MN 确认进行切换前，只需告知 O-GW 改变映射表，就可以实现快速的虚通道切换，因此 VTE 对超前操作的支持程度很高。

3 先扩后建的虚通道切换方式

从表 1 可知，两种基本切换方式各有优势，VTR 的主要问题在于切换时延较大，不支持超前操作；而 VTE 的主要问题是切换后端到端时延较大，且随着节点的连续切换而不断增大。因此，我们吸取这两种基本切换方式各自的优点，提出了一种混合的虚通道切换方式——先扩后建(Extension First Rebuilding Second，EFRS)方式。

表 1 两种基本切换方式的比较

切换方式	切换时延	端到端时延	技术复杂度	超前操作
VTR	大	最优	较小	不支持
VTE	小	非最优	较大	支持

EFRS 方式的基本思想是：先在 O-GW 和 N-GW 之间建立新的扩展虚通道，与 O-GW 和 C-GW 之间的旧虚通道一起构成切换后的数据临时传输通道；MN 切换到 N-GW 后，再

在 N-GW 和 C-GW 之间重新建立一条新虚通道，替代之前的临时传输通道。

1. 切换过程

(1)如图 10 所示，O-GW 收到切换请求消息后，向 N-GW 发起虚通道建立请求，建立虚通道 VT2。

(2)VT2 建立成功后，在 O-GW 处建立 VT1 和 VT2 的映射关系，对 MN 与 CN 间的用户数据进行中转。

(3)MN 移动到 N-GW 的管辖后，N-GW 在通过 VT1＋VT2 转发用户数据的同时，向 C-GW 发起虚通道建立请求，建立虚通道 VT3。

(4)新虚通道 VT3 建立成功后，C-GW 和 N-GW 将 MN 与 CN 间的用户数据切换到 VT3 上传输。

(5)N-GW 发起虚通道拆除消息，拆除 VT1 和 VT2，释放相应资源。

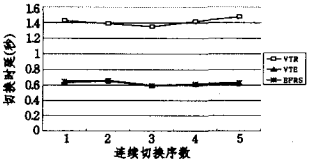

图 10　EFRS 切换方式示意图

2. 切换性能分析

(1)切换时延与丢包数

由于 N-GW 到 C-GW 之间的端到端新虚通道是 MN 切换后才发起的，因此，EFRS 的实际切换时延与 VTE 类似。连续切换时的切换时延相对固定，第 i 次连续切换的切换时延可表示为：

$$T_i = 3 \times n_3 \times t$$

其中，n_3 是 N-GW 到 O-GW 的最佳路径跳数，t 是 QoSNP 消息的每跳传输和处理时延。

(2)切换后的 QoS 保障

从 MN 切换成功到 VT3 建立成功之间，端到端时延不是最优，但 VT3 建立成功后，与 VTR 切换后的端到端时延相类似，全局最优。

(3)技术复杂度

在沿用已有的 QoSNP 协议和虚通道机制的同时，需要在 SUPA 网关增加虚通道之间的映射表，并管理该映射关系。VT3 建立后，需要依次拆除 VT2 和 VT1。

(4)超前操作的支持程度

与 VTE 类似，EFRS 由 O-GW 发起，因此对超前操作的支持程度很高。

4　仿真实验与结果分析

仿真实验的网络拓扑结构如图 11 所示，CN 通过 CGW 与 SUPANET 互联，MN 首先通过 GW1 与 CN 通信。在移动过程中，MN 分别接入到 GW2，GW3……GW6 管辖的子网，每次更换网关，都将引起 SUPA 网关之间虚通道的切换。

每次发生虚通道切换时，分别采用 VTR，VTE 和 EFRS 方式进行虚通道切换。记录得到的切换时延和切换后虚通道端到端时延分别如图 12 和图 13 所示。

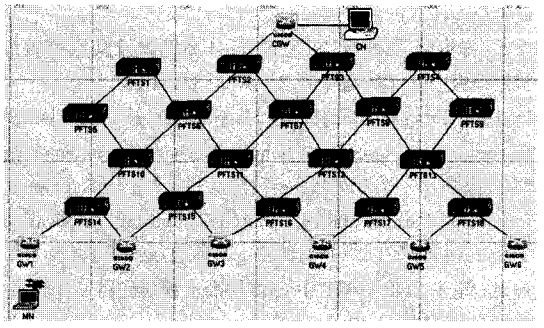

图 11　仿真试验的网络拓扑结构

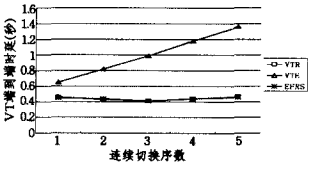

图 12　切换时延

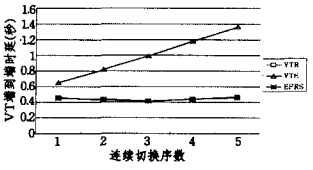

图 13　虚通道端到端时延

从图 12 中可以看出，EFRS 的切换时延与 VTE 相当，且明显小于 VTR；从图 13 中可以看出，EFRS 的虚通道端到端时延与 VTR 相当，且明显小于 VTE。可见 EFRS 的综合性能优于 VTR 和 VTE。

结束语　在 Internet 与 SUPANET 互联的背景下，针对 Internet 节点移动带来的 SUPANET 虚通道切换问题，本文提出了两种基本的虚通道切换方式和一种混合的虚通道切换方式，并对每种虚通道切换方式进行了特点分析和仿真实验。结果表明，EFRS 切换方式的综合性能明显好于其他两种基本切换方式。

本文只研究 SUPANET 域内的虚通道切换方式和性能，并没涉及节点移动时发生的二层切换和三层切换问题，但在实际网络化境下，二层切换和三层切换是虚通道切换的前提。因此，在未来的工作中，将进一步研究 EFRS 切换方式与快速移动 IPv6(FMIPv6)协议的兼容性问题。

参 考 文 献

[1] Zeng Huaxin, Xu Dengyuan, Dou Jun. On Physical Frame Time-slot Switching over DWDM[C]// PACAT03. IEEE press, Aug. 2003: 286-291

[2] Zeng Huaxin, Dou Jun, Xu Dengyuan. Single physical layer U-plane Architecture (SUPA) for Next Generation Internet[R]. Comprehensive Report on VoIP and enhanced IP Communications Services. IEC Publications, 2004: 197-227

[3] 曾华燊，窦军，汪海鹰. 论“单物理层的用户数据传输平面体系结构网络”——SUPANET[J]. 计算机应用，2004，24(6)：1-5

[4] 许登元，张新有，刘文杰. 物理帧时槽交换中改进的 DWRR 调度算法[J]. 西南交通大学学报，2005，40(6)：735-739

[5] Guo Zirong, Zeng Huaxin. Simulation and analysis of weighted fair queueing algorithms in OPNET[C]// 2009 International Conference on Computer Modeling and Simulation (ICCMS 2009). Macau: IEEE press, 2009: 114-118

[6] 李季，曾华燊，郭子荣. 基于时槽预定的加权公平调度策略[J]. 软件学报，2007，18(10)：2605-2612

[7] 李季，曾华燊，许登元. CICQ 交换机中一类服务可保障的调度策略研究[J]. 计算机研究与发展，2007，44(11)：1873-1880

[8] 窦军，曾华燊，陈文佳. SUPANET 信控管理平台的 UNI 和 NNI

研究[J]. 计算机科学,2009,36(4):112-115
[9] 窦军,曾华燊,汪海鹰. NGI/NGN 体系结构及其服务质量保障机制研究[J]. 计算机科学,2008,35(3):31-33
[10] Dou Jun, Zeng Huaxin, Wang Haiying. Single User-Plane Architecture and its QoS Provisioning Mechanisms in Signaling and Management (S&M) Planes[C]// The 5th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 04). Singapore, Dec. 2004:429-440
[11] 赵君,高雨. SUPANET 中 QoS 协商流程研究[J]. 计算机科学,2004,31(8 增刊):21-24
[12] Zeng Huaxin, Gao Yu, Xia Yu. On NGN architecture and evolution strategy[C]// First ITU-T Kaleidoscope Academic Conference-Innovations in NGN: Future Network and Services. Geneva: IEEE press, May 2008:337-342
[13] Gao Yu, Zeng Huaxin. A New Mechanism supporting QoS and Mobility in SUPANET[C]// 2008 International Symposium on Computer Science and Computational Technology (ISCSCT 2008). Vol. 1, Shanghai: IEEE press, December 2008:771-776
[14] Johnson D, Perkins C, Arkko J. Mobility Support in IPv6 RFC 3775 [DB/OL]. [2004-6-10]. http://www.ietf.org/rfc/rfc3775.txt
[15] Gao Yu, Zeng Huaxin, Wang Haiying. Research on Mobility Management in DDQP Mechanism of SUPANET[C]// 2009 International Conference on Communications and Mobile Computing (CMC 2009). Kunming: IEEE press, January 2009:216-221

(上接第 76 页)

5 改进方案的安全性和性能分析

在 BSZ 模型中[5],将理想的动态群签名方案应满足的安全特性归纳为 4 点:1)正确性。群成员所生成的签名验证有效,打开算法能正确地揭示签名者的身份并且给出可接受的证明;2)匿名性。对于一个指定消息的签名,如果敌手不能判定是由他所选择的两个成员中哪一个成员所签署,则方案满足匿名性;3)可跟踪性。敌手若不能生成一个 GM 就不能揭示其身份的签名,或者 GM 可以揭示其身份但是不能给出一个可接受的证明;4)抗陷害性。如果一个成员没有生成某个签名,敌手就不能给出一个证明来认定该成员生成了此签名。基于此安全模型,对改进方案的安全性分析如下。

正确性:$u_1=g^{r_2}r_1^{-r_1 2^{T-j}}y^{u_2 r_1} \bmod n$ 的正确性由原方案保证。而 $u_3^{r_2}=u_1^{[k+(e_u+x_u)u_2r_1]}g^{k_1[k+(e_u+x_u)u_2r_1]}=u_1^{Eu_2r_1+a[k+x_uu_2r_1]+k_1}u_1^{-k_1}g^{k_1[k+(e_u+x_u)u_2r_1]}=u_1^{Eu_2r_1+a[k+x_uu_2r_1]+k_1}g^{-kk_1}g^{k_1[k+(e_u+x_u)u_2r_1]}=u_1^{Eu_2r_1+r_3}g^{r_4} \bmod n$。

匿名性:首先,在强 RSA 问题和离散对数假设下,从两个不同的签名出发,判断密钥 e_u 的相关性等同于求解离散对数问题 $C_{p,0}^{2^T}=g^{e_u}g^{x_u}y \bmod n$,判断 $C_{u,j}$ 的相关性等同于求解强 RSA 问题 $C_{u,i}=C_{u,i-1}^2 \bmod n$。其次,由于随机值 k_1 和 k 分别通过 $r_2=k+(e_u+x_u)u_2r_1$,$r_4=k_1(e_u+x_u)u_2r_1$ 和 $r_3=a(k+x_uu_2r_1)+k_1$ 对密钥成分 (e_u+x_u) 和 x_u 进行了随机化,任何对密钥成分 (e_u+x_u) 和 x_u 的求解或比较也是不可行的。因此,在改进方案中,不仅签名 $(u_1,u_2,u_3,r_1,r_2,r_3,r_4)$ 的每一成分都与随机数进行了绑定,而且任何对密钥成分的求解和比较是不可行的,从而改进方案的匿名性仍然成立。

可跟踪性:由于打开算法与原方案同,方案的可跟踪性仍然成立。

抗陷害性:在离散对数和强 RSA 问题假设下,由方案的匿名性求解签名密钥是不可行的。而如果签名密钥是安全的,攻击者选择满足条件的参数 (r_1',r_2',r_3',r_4'),设 $u_1'=g^{r_2'}r_1'^{-r_1'2^{T-j}}y^{u_2'r_1'} \bmod n$,$u_3'^{r_2'}\equiv u_1'^{Eu_2'r_1'+r_3'}g^{r_4'} \bmod n$,$u_2'=H(u_1',m)$。在离散对数和强 RSA 问题假设下,求解 u_1',u_2',u_3' 是不可行的,因此攻击者不能伪造一个合法的群签名。

可撤销性:(u_3,r_3,r_4) 可以作为"e_u 整除当前 E 值"的知识证明。由于验证 (u_3,r_3,r_4) 的合法性密钥 e_u 和签名使用的密钥 e_u 是一致的(利用了同一参数 r_2),并且两个验证关系相互绑定,如果成员 U 被撤销,则他此后的签名也只能使用自己的密钥成分 e_u 做合法性检验,而此时的密钥 e_u 一定不满足 $ae_u=E$。

结束语 在大量的群签名方案的设计中,成员撤销问题的解决备受关注。本文分析了陈少真等人提出的群签名方案中成员取消算法的缺陷,否定了文献[7]给出的第 2 种群成员撤销方法,并在陈方案的基础上给出了一个可撤销成员的改进方案。新方案中群管理者只需做一次除法运算就可以撤销一个成员,而成员密钥不需要改变,且签名和验证过程独立于现有的成员个数和撤销成员个数。因此,改进方案克服了原方案存在的安全缺陷,提高了群签名协议的执行效率,是一个实用的群签名方案。

参 考 文 献

[1] Chaum D, van Heyst E. Group signatures[C]// Advances in Cryptology—EUROCRYPT '91. Berlin: Springer-Verlag, 1991:257-265
[2] Ateniese G, Tsudik G. Some open issues and new directions in group signature schemes[C]// Financial Cryptography (FC'99). Berlin: Springer-Verlag, 1999:196-211
[3] Song D X. Practical forward secure group signature schemes[C]// Proc. of the 8th ACM Conf on Computer and Communications Security (CCS 2001). New York: ACM Press, 2001:225-234
[4] Atenies G, Camenisch J, Joye M, et al. A practical and provably secure coalition-resistant group signature scheme[C]// Advances in Cryptology—CRYPTO 2000. Berlin: Springer-Verlag, 2000:255-270
[5] Bellare M, Shi H, Zhang C. Foundations of group signatures: research interests are cryptography and the case of dynamic groups[C]// CT2RSA 2005. Berlin: Springer-Verlag, 2005:136-153
[6] Camenisch J, Lysyanskaya A. Dynamic accumulators and application to efficient revocation of anonymous credentials[C]// Proc. of Crypto 2002. Berlin: Springer Verlag, 2002:61-76
[7] 陈少真,李大兴. 有效取消的向前安全群签名体[J]. 计算机学报,2006,29(6):998-1003
[8] 陈泽文,王继林,黄继武,等. ACJT 群签名方案中成员撤消的高效实现[J]. 软件学报,2005,16(1):151-157