公平的移动小额支付协议

樊利民　　廖建新
(北京邮电大学网络与交换技术国家重点实验室　北京　100876)

摘　要：为了实现具有完全公平性和非单元支付功能的小额支付协议，该文首先提出了双 PayWord 链(DPWC)的概念和非单元支付的实现机制。利用 DPWC，并基于数据业务管理平台(DSMP)提出了一种新的公平的移动小额支付协议(FMMP)。该协议由注册、支付、仲裁、结算和注销 5 个子协议组成。分析结果表明，该协议能提供支付的完全公平性和非单元支付功能，并且具有安全、高效和不可否认的特点。

关键词：小额支付；公平性；PayWord
中图分类号：TN929.5　　**文献标识码**：A　　**文章编号**：1009-5896(2007)11-2599-04

Fair Mobile Micropayment Protocol

Fan Li-min　　Liao Jian-xin
(*State Key Laboratory of Networking and Switching Technology*,
Beijing University of Posts and Telecommunications, *Beijing* 100876, *China*)

Abstract: In order to realize the micropayment protocol with both full fairness and non-unit payment function, the concept of Double PayWord Chain(DPWC) and the realization mechanism of non-unit payment are presented first in this paper. Using DPWC, a new Fair Mobile Micropayment Protocol(FMMP) based on Data Service Management Platform(DSMP) is developed. The new protocol consists of 5 subprotocols: registration, payment, arbitration, settlement and cancellation. Full fair payment and non-unit payment can be provided by FMMP. In addition, FMMP has characteristics of security, efficiency and nonrepudiation.

Key words: Micropayment; Fairness; PayWord

1　引言

移动数据业务的快速发展，对以移动终端作为支付途径的移动小额支付提出了巨大的市场需求，并且已有大量的文献对移动环境下的小额支付进行了研究。在众多的研究方案中，有一类方案[1−4]是基于PayWord链[5]思想的，包括分割PayWord链[6]和非平衡单向二进制树(UOBT)[7]技术等。这类方案的优点是协议效率高，但还存在一些严重的缺点，如无法保证支付的完全公平性、无法实现非单元支付、无法防止用户的恶意消费和恶意欺诈等。这些缺点使得这类方案仅能应用于每笔交易金额比较微小的微支付业务领域，而且仅适合于后付费移动用户，对于预付费用户还存在较大的风险。对于大多数的小额支付业务，由于每笔的交易金额已经不是微不足道(比如：几元、十几元到几十元)，保证支付的完全公平性是必要的，因此上述这类基于PayWord链的方案需要进行改造。

目前，移动运营商提出了以数据业务管理平台(DSMP)[8]为核心的业务网络，来加强移动数据业务的可运营性，而且在移动梦网上已有相关设备[9]在运行。SP(Service Provider，业务提供商，以下同)提供的每项业务或每件信息商品，DSMP都要进行统一的编号。本文基于DSMP提出了一种新的移动小额支付协议，新协议使用了本文后面提出的双PayWord链的概念，分成了注册、支付、仲裁、结算和注销 5 个子协议，实现了支付的完全公平性和非单元支付功能，并具有安全、高效、和不可否认性等特点。

2　双 PayWord 链的概念及非单元支付的实现

自PayWord链[5]概念提出之后，人们对其进行了广泛的扩展研究[4,6,7,10−12]，这些研究主要是为了解决支付的公平性、灵活性、效率和安全等问题。本文提出了双PayWord链(Double PayWord Chain , DPWC)的概念，利用该概念来实现支付的公平性和非单元化，以满足小额支付业务的要求，具体说明如下。

双 PayWord 链由等长度($N+1$)的两条 PayWord 链组成，一条定义为主链 $\{w_{mN}, w_{mN-1}, \cdots, w_{mi}, \cdots, w_{m1}, w_{m0}\}$，一条定义为从链 $\{w_{sN}, w_{sN-1}, \cdots, w_{si}, \cdots, w_{s1}, w_{s0}\}$，$(w_{m0}, w_{s0})$ 是双 PayWord 链的根。主链和从链可以使用相同的强抗碰撞单向杂凑函数，但要求 w_{mN} 和 w_{sN} 一定要不同。每一对杂凑值

2006-03-24 收到，2006-10-08 改回
国家杰出青年科学基金(60525110)，国家 973 计划项目(2007CB307103)，新世纪优秀人才支持计划(NCET-04-0111)，高等学校博士学科点专项科研基金(20030013006)资助课题

(w_{mi}, w_{si}), $i = 1,2,\cdots,N$，构成一个支付单元，代表一个支付单位。用户进行小额支付交易时，先把支付单元的主链杂凑值 w_{mi} 和序号 i 发给 SP，等交易成功结束后，用户再把支付单元的从链杂凑值 w_{si} 发给 SP，从而实现类似分割 PayWord 链所提供的支付的部分公平性。至于如何实现支付的完全公平性，本文是通过再附加一个仲裁链来实现的，这将在后面协议的详细描述中进行说明。

在实现了支付的完全公平性的基础上，非单元支付功能的实现机制如下。假设 (w_{mi}, w_{si}) 是用户已花出的最后一个支付单元。当某笔小额支付交易的金额是 v 个支付单位时，用户就可先把 $w_{m(i+v)}$ 和 $i+v$ 发给 SP，等交易成功结束后，再把 $w_{s(i+v)}$ 发给 SP，从而实现非单元支付功能。

3 协议的描述和说明

在本文的协议描述中，数据业务管理平台DSMP的私钥是SK_D；业务提供商SP的标识是$\mathrm{ID_{SP}}$，私钥是SK_SP；移动用户U的标识是$\mathrm{ID_U}$，数字证书是CertU，对应的私钥是SK_U；$\{M\}_{\mathrm{S}}$表示用私钥SK对消息M进行签名；$X||Y$表示消息X和Y的连接；$A\rightarrow B$: x表示A把消息x发给B；假定在协议执行之前，DSMP已有用户和SP的数字证书，SP已有DSMP的数字证书。对于用户和SP来说，DSMP可看成是TTP(Trusted Third Party，可信第三方)，用户和SP在DSMP上都开设有专门的小额支付交易账户。

3.1 注册子协议

注册子协议的主要功能是用户向 DSMP 注册双 PayWord 链，作为与 SP 进行小额支付交易的支付凭据。具体如图 1 所示，包括 4 步。

第 1 步　用户选择一个二元组 (w_{mN}, w_{sN})，构造一个长度为 $N+1$ 的双PayWord链，根据需要，定义每个支付单位的实际值为 P，然后对$\mathrm{ID_U}||w_{m0}||w_{s0}||N||P||\mathrm{ID_{SP}}$签名后发给DSMP，表示请求注册一个面向某个SP的双PayWord链，用于与该SP的小额支付交易。

第 2 步　DSMP 收到用户的注册请求后，首先对用户的签名进行验证，然后检查用户账户里是否还有 $N\times P$ 数量的可用资金(对于后付费用户，可以是信用额度，以下略)，如果没有，则返回注册失败的消息给用户，并说明原因；如果还有，则 DSMP 冻结用户账户里的 $N\times P$ 数量的资金，然后给这个双PayWord链分配一个唯一的序列号SN，并确定两个时限值 T_1 (使用期限)和 T_2 (结算期限)。其中 T_1 是SP能接收用户该双PayWord链的最后期限，T_2 是DSMP对该双PayWord链进行结算的最后期限，所以 T_2 应至少比 T_1 延时一个结算周期。然后DSMP把消息$\mathrm{SN}||\mathrm{ID_U}||w_{m0}||w_{s0}||N||P||\mathrm{ID_{SP}}||\mathrm{CertU}||T_1||T_2$进行签名后，发给SP，作为结算承诺。

(1) U→DSMP：$\{\mathrm{ID_U}||w_{m0}||w_{s0}||N||P||\mathrm{ID_{SP}}\}_{\mathrm{SK\_U}}$
(2) DSMP→SP：$\{\mathrm{SN}||\mathrm{ID_U}||w_{m0}||w_{s0}||N||P||\mathrm{ID_{SP}}||\mathrm{CertU}||T_1||T_2\}_{\mathrm{SK\_D}}$
(3) SP→DSMP：$\{\mathrm{SN}||h_1(\mathrm{SN}||\mathrm{ID_U}||w_{m0}||w_{s0}||N||P||\mathrm{ID_{SP}}||\mathrm{CertU}||T_1||T_2)\}_{\mathrm{SK\_SP}}$
(4) DSMP→U：$\mathrm{SN}||R||T_1$

图 1　注册子协议

第 3 步　SP收到结算承诺后，对签名进行验证，无误后对消息$\mathrm{SN}||h_1(\mathrm{SN}||\mathrm{ID_U}||w_{m0}||w_{s0}||N||P||\mathrm{ID_{SP}}||\mathrm{CertU}||T_1||T_2)$进行签名，然后返回DSMP，表示可以接受用户的双PayWord链作为支付凭据。其中 h_1 表示一强抗碰撞单向杂凑函数。

第 4 步　DSMP 收到 SP 的消息后，向用户返回双 PayWord 链的 SN 和用户账户的当前可用资金 R 以及最后使用期限 T_1，表示用户注册成功。

3.2 支付子协议

支付子协议包括 3 步，如图 2 所示。对于SP出售的商品，都有在DSMP注册的唯一的标号$\mathrm{ID_G}$。

(1) U→SP: $\{\mathrm{SN}||w_{m(i+v)}||i+v||\mathrm{ID_G}\}_{\mathrm{SK\_U}}$
(2) SP→U: 标号为$\mathrm{ID_G}$的商品
(3) U→SP: $\mathrm{SN}||w_{s(i+v)}$

图 2 支付子协议

第 1 步　用户打算购买标号为$\mathrm{ID_G}$的商品，该商品的价格为 v 个支付单位即 $v\times P$，则用户对$\mathrm{SN}||w_{m(i+v)}||i+v||\mathrm{ID_G}$进行签名后，作为交易请求，发给SP。其中，$(w_{mi}, w_{si})$ 是用户已花出的最后一个支付单元。

第 2 步　SP收到用户的交易请求后，对签名进行验证。根据序列号SN查找与该双PayWord链对应的结算承诺，然后对 $w_{m(i+v)}$ 进行检查，无误后，向用户发送标号为$\mathrm{ID_G}$的商品。

第 3 步　用户成功收到商品后，向 SP 发送消息$\mathrm{SN}||w_{s(i+v)}$给 SP。每次交易后，SP 都要保存最新的支付记录，已防止用户的重复消费。

3.3 仲裁子协议

在支付子协议中，若用户试图欺诈而导致 SP 没有正确接收到 $\mathrm{SN}||w_{s(i+v)}$，则 SP 就可以启动仲裁子协议，恢复支付的公平性。仲裁子协议包括 3 个步骤，如图 3 所示。

(1) SP→DSMP: $\{\{\mathrm{SN}||w_{m(i+v)}||i+v||\mathrm{ID_G}\}_{\mathrm{SK_U}}||$标号为$\mathrm{ID_G}$的商品$\}_{\mathrm{SK_SP}}$
(2) DSMP→SP: $\{\mathrm{SN}||w_{a(i+v)}||i+v||w_{a0}\}_{\mathrm{SK\_D}}$
(3) DSMP→U: $\mathrm{SN}||i+v||$标号为$\mathrm{ID_G}$的商品

图 3 仲裁子协议

第 1 步

(1)U→DSMP: SN
(2)DSMP→SP: $\{\mathrm{SN}\}_{\mathrm{SK\_D}}$
(3)SP→DSMP: $\{\mathrm{SN}||w_{si}$ (或 $w_{ai})||i||h_2(\{\mathrm{SN}\}_{\mathrm{SK\_D}})\}_{\mathrm{SK\_SP}}$
(4)DSMP→U: $\mathrm{SN}||R$

SP 把收到的用户签名的交易请求{SN||$w_{m(i+v)}$ || $i+v$ ||$\mathrm{ID_G}$}$_{\mathrm{SK_U}}$和对应的商品签名后一起发给DSMP。

第 2 步　DSMP 根据 SN 检索对应的双 PayWord 链的有关信息，然后生成一个等长度的杂凑链{$w_{aN}, w_{aN-1}, \cdots, w_{ai}, \cdots, w_{a1}, w_{a0}$}，叫做仲裁链。根据交易请求中的 $w_{m(i+v)}$，DSMP 从仲裁链中找到对应序号的杂凑值 $w_{a(i+v)}$，然后把 SN|| $w_{a(i+v)}$ || $i+v$ || w_{a0} 签名后发给 SP。$w_{a(i+v)}$ 的作用是在后面的结算子协议中替代 $w_{s(i+v)}$，实现 SP 与 DSMP 的结算。

第 3 步　DSMP把SN|| $i+v$ ||标号为$\mathrm{ID_G}$的商品发给用户。

在支付子协议中，若 SP 想进行欺诈，那么 SP 不可能从用户得到 SN|| $w_{s(i+v)}$；根据仲裁子协议，SP 也不可能既得到 SN|| $w_{a(i+v)}$ || $i+v$ || w_{a0}，而又不发送正确的商品，所以 SP 不能欺诈成功。

3.4　结算子协议

在预定的结算时间，SP 把所有需要结算的双 PayWord 链的 SN，对应从链(或仲裁链)的最后一个杂凑值 w_{si} (或 w_{ai}) 和序号 i 签名后发给 DSMP，进行结算。如图 4 所示。DSMP 保留上次的结算记录，以防止 SP 的重复结算。结算成功后，DSMP 把相应的资金从用户账户的冻结部分扣除并划帐到 SP 的账户里。对于已过结算期限 T_2 的双 PayWord 链，DSMP 自动把这些双 PayWord 链进行注销，并告知用户。

SP→DSMP: {SN|| w_{si} (或 w_{ai})|| i ||.....} $_{\mathrm{SK\_SP}}$

图 4　结算子协议

3.5 注销子协议

在双 PayWord 链未被 DSMP 自动注销之前，用户可随时通过注销子协议，注销掉还未花出的支付单元，具体如图 5 所示。

第 1 步　用户向 DSMP 发送一个已注册的双 PayWord 链的 SN，启动注销子协议。

第 2 步　DSMP 根据 SN，查找到对应的 SP，然后对 SN 签名后，发给 SP。

第 3 步　SP根据SN，查找到对应从链(或仲裁链)的最后一个杂凑值 w_{si} (或 w_{ai})，然后对SN|| w_{si} (或 w_{ai})|| i || h_2 ({SN}$_{\mathrm{SK\_D}}$)签名后发给DSMP。其中，h_2 是强抗碰撞单向杂凑函数。此步之后，SP可以拒绝接收来自用户的该双PayWord链的新的支付单元。

第 4 步　DSMP 根据 w_{si} (或 w_{ai})和 i 算出用户账户可用资金的当前值 R，并返回用户消息 SN|| R，表示注销成功。

图 5 注销子协议

4　协议分析

4.1 支付的完全公平性

首先由于采用了双 PayWord 链的结构，交易进行时用户可先把主链的杂凑值发给 SP，等用户接收到正确的商品后，再把从链相应的杂凑值发给 SP，只要能保证支付子协议正常执行，那么支付就是完全公平的。

第二，由于在交易请求中，通过用户的签名把主链的杂凑值与商品的标号$\mathrm{ID_G}$进行了绑定，所以当支付子协议不能正常执行时(比如用户故意不把从链相应的杂凑值发给SP)，那么SP就可以启动仲裁子协议，作为TTP的DSMP就可利用仲裁链来保证支付的完全公平性。

4.2 协议的安全性

协议的安全性由以下几个方面得到了保障。

(1)根据注册子协议，用户必须先注册一个双 PayWord 链，然后才能使用，同时 DSMP 会冻结用户相应的资金；根据支付子协议，用户的交易请求要经过签名，这两方面就保证了用户无法恶意消费、欠费和欺诈。

(2)由于每个双 PayWord 链都是与用户和 SP 身份同时绑定的，所以即使被别的用户或 SP 窃取，也是无法使用的。

(3)每次交易后，SP 都会保存双 PayWord 链(或仲裁链)的最新杂凑值，并且每个双 PayWord 链都有唯一的 SN，所以用户是无法重复消费的。

(4)每次结算后，DSMP 也会保存双 PayWord 链(或仲裁链)的最新杂凑值，并且每个双 PayWord 链都有唯一的 SN，所以 SP 也是无法重复结算的。

4.3 协议的效率

协议的效率可从 DSMP 和用户的角度进行分析如下：

(1)对于DSMP，在支付子协议正常进行时，只有用户和SP之间的交互，DSMP并不参与交易的流程，因此DSMP实际是一种离线的TTP[13]；而对于注册、结算、仲裁和注销等 4 个子协议，DSMP可以非在线执行，以上两点使DSMP避免成为系统性能的瓶颈。

(2)对于用户终端，构造一个双PayWord链的计算量与构造一个等数目支付单元的分割PayWord链[6]的计算量，完全是相同的。

(3)由于实现了非单元支付，用户和 SP 之间的交互次数可以减少很多。

4.4 支付和交易的不可否认性

通过注册子协议，用户对所有使用的双 PayWord 链都先经过了注册；PayWord 链的单向性，保证了只由用户才能生成正确的支付单元，这两方面保证了用户对每一次支付的不可否认。通过支付子协议，用户对每次交易请求都进行了签名，另外通过仲裁子协议，保证了当支付子协议不能正常

完成时，用户对交易的不可否认。

5 结束语

本文提出了一种新的公平的移动小额支付协议，该协议包括注册、支付、仲裁、结算和注销等 5 个子协议。该协议实现了支付的完全公平性和非单元支付功能，并且具有安全、高效和不可否认的特点，完全适用于移动小额支付的场合。本文提出的双PayWord链的概念可以扩展到非平衡单向二进制树(UOBT)[7]或并列PayWord链[11]中去，既实现带面额信息的支付，又提供支付的公平性，从而适应于更广泛的支付领域。

参 考 文 献

[1] 万仁福, 李方伟, 朱江. 一种适应于移动环境的认证和支付协议[J]. 电子与信息学报, 2005, 27(3): 498–501.
Wan Ren-fu, Li Fang-wei, and Zhu Jiang. An efficient authentication and payment protocol for mobile communication[J]. *Journal of Electronics & Information Technology*, 2005, 27(3): 498–501.

[2] 李明柱, 李志江, 杨义先. 移动通信增值服务认证和支付研究[J]. 通信学报, 2003, 24(4): 123–127.
Li Ming-zhu, Li Zhi-jiang, and Yang Yi-xian. Research on authentication and payment of mobile communication VAS[J]. *Journal of China Institute of Communication*, 2003, 24(4): 123–127.

[3] 姬东耀, 王育民. 移动计算环境中的认证与小额支付协议[J]. 电子学报, 2002, 30(4): 495–498.
Ji Dong-yao and Wang Yu-min. An authentication and micropayment protocol for mobile computing network[J]. *Acta Electronica Sinica*, 2002, 30(4): 495–498.

[4] Patil V and Shyamasundar R K. E-coupons: An efficient, secure and delegable micro-payment system[J]. *Information Systems Frontiers*, 2005, 7(4/5): 371–389.

[5] Rivest R and Shamir A. Payword and MicroMint: two simple micro-payment schemes[C]. Proceedings of 1996 International Workshop on Scurity Protocols, Cambridge, 1996, LNCS 1189, 1997: 69–87.

[6] Buttyan L. Removing the financial incentive to cheat in micropayment schemes[J]. *IEE Electronics Letters*, 2000, 36(2): 132–133.

[7] Yen S, Ho L, and Huang C. Internet micropayment based on unbalanced one-way binary tree[C]. Proc. CrypTEC'99, Hong Kong, July 1999: 155–162.

[8] 中国移动通信集团公司. 数据业务管理平台设备规范[S]. V1. 0.0, 2003.
China Mobile Communications Corporation. Mobile Data Service Management Platform Equipment Specification[S]. V1.0.0, 2003.

[9] 郑炜. MISC 平台的架构和基本功能[J]. 中国数据通信, 2004, (8): 20–22.

[10] Yang Zongkai, Lang Weimin, and Tan Yunmeng. A new fair micropayment system based on hash chain[C]. Proc. EEE'04, Taipei, 2004: 139–145.

[11] 李明柱, 李志江, 杨义先, 钮心忻. 基于 PayWord 的 WWW 微支付模型[J]. 北京邮电大学学报, 2002, 25(2): 23–27.
Li Ming-zhu, Li Zhi-jiang, Yang Yi-xian, and Niu Xin-xin. WWW micropayment model based on PayWord[J]. *Journal of Beijing University of Posts and Telecommunications*, 2002, 25(2): 23–27.

[12] Lin I, Hwang M, and Chang C. The general pay-word: A micro-payment scheme based on n-dimension one-way hash chain[J]. *Designs, Codes, and Cryptography*, 2005, 36(1): 53–67.

[13] 卿斯汉.电子商务协议中的可信第三方角色[J]. 软件学报, 2003, 14(11): 1936–1943.
Qing Si-Han. TTP roles in electronic commerce protocols[J]. *Journal of Software*, 2003, 14(11): 1936–1943.

樊利民： 男，1971 年生，博士生，研究方向为移动商务.

廖建新： 男，1965 年生，博士，教授，博士生导师，研究方向为移动通信.