基于主从代理协作的多重数字签名机制的研究*)

王海艳[1] 黄海平[1] 王汝传[1,2] 李明远[1]
(南京邮电学院计算机科学与技术系 南京210003)[1]
(信息安全国家重点实验室(中国科学院研究生院) 北京100039)[2]

摘 要 多移动代理协作的多重数字签名在移动代理技术领域,特别是电子商务领域,有着广阔的应用前景。本文鉴于移动代理的安全问题,针对"主从代理协作"这一新兴概念,提出了一种基于ElGamal密码系统和ElGamal密码系统在DSS(数字签名标准)中变换形式的多重数字签名方案,并通过一个具体的商务案例分析其安全性和有效性,得出了若干结论。

关键词 移动代理,主从代理协作,多重数字签名,ElGamal密码系统

The Research of Multi-Signature Mechanism Based on Cooperation of Master Agent and Slave Agents

WANG Hai-Yan[1] HUANG Hai-Ping[1] WANG Ru-Chuan[1,2] LI Ming-Yuan[1]
(Department of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003)[1]
(State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing 100039)[2]

Abstract Multi-signature based on cooperation of multi-mobile agents has the wide prospect on mobile agent technique application especially on E-commerce. Aiming at a new concept Cooperation of master agent & slave agents, this paper proposes a new kind of multi-signature mechanism based on ElGamal cryptography and its variant form in DSS (Digital Signature Standard) for the serious security problems. Then it makes the analysis for the security & validity of the mechanism and draws some conclusions through a detailed E-commerce example.

Keywords Mobile agent, Cooperation of master agent and slave agents, Multi-signature, ElGamal cryptography

1 引言

移动代理技术在分布式网络计算中有着广泛的应用和扩展潜力。然而,这一技术的优势在当前的Internet中并未得以完整的体现,"安全性问题"仍是移动代理技术推向商用的瓶颈。对此,许多研究者提出了各种各样的安全策略,其中讨论得最为激烈亦最难解决的仍是"恶意主机或恶意的执行平台对代理的攻击"。在诸多安全保护方案中,"利用多移动代理协作进行多重数字签名"将是本文要探讨的核心内容。

在引入正题之前,先简要介绍当前研究者关于此的一些研究成果。其实"多重数字签名"这一概念,在Shamir及Blakley提出的门限方案(Threshold Scheme)[1,2]中已经有所体现,近来的研究者将其巧妙地应用于移动代理领域,尤其多见于电子商务领域,已成为研究的热点,见参考文[3,4];而不基于门限方案的其它多移动代理的签名机制(例如基于RSA的多移动代理的商务联合签名机制)可参看文[5,6]。

2 背景知识

2.1 多移动代理中主代理的强弱定义

源主机在多移动代理协作中扮演着重要的角色:作为移动代理的初始创建者,它根据任务的要求把多移动代理之间的体系结构定义为两种模式——对等模式与主从模式。一般而言,多移动代理协作签名均需要有一个主代理(Master Agent)和若干从代理(Slave Agent,之间是对等模式)统一协调工作。下面将阐述主代理的强弱定义。

强定义:源主机创建主代理,而主代理驻留于可信任的主机节点或服务器,根据任务的性质和网域的环境创建从代理并把任务和数据委派给从代理,从代理(并行或串行)移动到指定目的地利用委派的数据完成任务后将结果返回给主代理。

弱定义:源主机创建主代理和若干从代理,并把任务委派给主从代理,在远程网域内,由主代理指挥协同各从代理共同执行源主机的任务。

强弱主代理之间最显著的区别在于:前者具有创建从代理的功能,并能依据任务性质和执行环境自主地将数据与任务分配给由它创建的从代理,一般情况下,它携带着源主机的机密信息或关键数据驻留于可信任的节点,本身并不参与具体任务的执行;而后者不具备创建从代理的功能,也不予从代理分派任务,它充当了指挥调度的角色,自身也参与任务的执行;强主代理比弱主代理具有更高的构件要求和开发难度。

本文介绍的基于主从多移动代理协作的多重数字签名采用的是"弱主代理"的形式。

2.2 密钥体制与密钥分割

提及密钥体制,最广为人知的莫过于DES对称密钥体制

*)本课题得到国家自然科学基金(60173037)、江苏省自然科学基金(BK2003105)、国家高科技项目八六三(2002AA776032)、江苏省计算机信息处理技术重点实验室基金(kjs03061)资助。王海艳 讲师,硕士,在读博士,主要研究方向为计算机软件、计算机网络、信息安全、移动代理等;黄海平 硕士研究生,主要研究方向是计算机网络、计算机软件在通信中的应用和信息安全等;王汝传 教授,博士生导师,主要研究方向是计算机软件、计算机网络、信息安全、移动代理和虚拟现实技术等;李明远 硕士研究生,研究方向为计算机网络和信息安全等。

和 RSA 公钥密码体制。在文[5]中，Boyd 便提出了一种基于 RSA 的多重数字签名机制，多移动代理的商务联合签名机制[6]也是以 RSA 作为密钥体制。而本文的密钥体制基于 ElGamal 密码系统[7,8]，采用这种形式，能使签名方案更加简单、密钥计算易于实现。鉴于 DSS(数字签名标准)规范，我们还将采用其一种变体形式，来实现原始 ElGamal 密钥系统到 DSS 规范的过渡。

密钥分割的思想也不同于常见的(t,n)门限方案，虽然该方案有着许多不可比拟的优点：t 值的变化可使安全级别灵活改变，多个移动代理共享密钥，可以在没有认证中心的情况下，利用各自的子密钥进行计算，子密钥可以是一次性的，也可以被重复地使用等等。但是基于门限方案的密钥分割算法大多过于复杂，采用了大量多项式或者指数函数的形式。而本文采用的密钥分割算法对商业应用有两个极为重要的优点：简单性和普遍性，因为仅使用了加法和乘法，用普通的标准公钥密码技术便可实现(例如 RSA)，不需要额外设计新的算法。

3 基于主从代理协作的 ElGamal 多重数字签名机制

3.1 算法的基本实现

前文已经提及，该签名算法基于 ElGamal 密码体制。而签名的形式也有两种区分，即多个移动代理是串行签名还是并行签名。3.1.1节将分别对这两种签名形式进行算法描述，而3.1.2节则实现了该算法从原始 ElGamal 密码系统到 DSS 规范的过渡。

3.1.1 *基于 ElGamal 密码体制的主从代理串/并行签名*

以下是算法的基本步骤：

公开长期(恒定)公钥：$\langle g,p,T\rangle$，分割私钥：S，此处有 $g^S \bmod p=T$；

对预签名信息 m，随机选择整数 S_m，计算 $g^{S_m} \bmod p=T_m$ 并生成$(m|T_m)$的摘要 d_m；

对摘要进行签名 $X=S_m+d_m S \bmod (p-1)$；

验证签名 $g^X=T_m T^{d_m} \bmod p$。

(1)主从代理协作的串行签名。ElGamal 密码体制采用一对私钥而并非 RSA 体制的单一私钥形式。第一个私钥是长期(恒定)私钥，而第二个私钥是短期(周期)私钥，对于 n 个移动代理，可用乘法和加法将私钥对分割如下：

分割长期(恒定)私钥：$S=S_1 * S_2 * \cdots * S_n$；(主代理拥有 S_n)

分割短期(周期)私钥：$S_m=S_{m_1}+S_{m_2}+\cdots+S_{m_n}$；(主代理拥有 S_{m_n})

对于预签名的信息摘要 d_m，采用串行签名的形式，从代理1利用 S_1和 S_{m_1}对其进行签名可得 $X_1=S_{m_1}+d_m S_1 \bmod (p-1)$，签完后从代理1将 X_1传送给从代理2；同理，从代理2利用 S_2和 S_{m_2}继续对 X_1进行签名，得到 $X_2=S_{m_2}+X_1 S_2 \bmod (p-1)=S_{m_2}+S_2 S_{m_1}+d_m S_1 S_2 \bmod (P-1)$；以此类推，最后签名由从代理$(n-1)$传到了主代理手中，主代理将产生最后的完整签名 $X_n=\sum_{t=1}^{n} S_{m_t}+d_m \prod_{t=1}^{n} S_t \bmod (P-1)+\sum_{t=1}^{n-1}[S_{m_t}[\prod_{k=t+1}^{n} S_k-1]] \bmod (p-1)$。

然而，该签名 X_n 与我们所期待的签名 $X=S_m+d_m S \bmod (p-1)$却不尽相同，它们两者之间的差距在于：$X_n-X=\sum_{t=1}^{n-1}[S_{m_t}[\prod_{k=t+1}^{n} S_k-1]] \bmod (p-1)$。容易发现等式的右端仅由一些常数项和子密钥组成，它们的数值在源主机发送多移动代理之前就能精确地计算出来，因此并不影响主从代理协作完成签名任务，主代理只需将 X_n 稍加变化便能得到正确的签名 X。

(2)主从代理协作的并行签名。基于 ElGamal 密钥体制的并行签名，对于 n 个移动代理，私钥对的分割有如下形式：

分割长期(恒定)私钥：$S=S_1+S_2+\cdots+S_n$；(主代理拥有 S_n)

分割短期(周期)私钥：$S_m=S_{m_1}+S_{m_2}\cdots+S_{m_n}$；(主代理拥有 S_{m_n})

对于预签名的信息摘要 d_m，主从代理利用各自的子密钥对并行签名如下：

$X_1=S_{m_1}+d_m S_1 \bmod (p-1)$，$X_2=S_{m_2}+d_m S_2 \bmod (p-1)$，$\cdots$，$X_n=S_{m_n}+d_m S_n \bmod (p-1)$；

各个从代理再将各自的签名 X_t 传送给主代理，由主代理合并这些签名，最后得到：

$$X=\sum_{t=1}^{n} X_t=\sum_{t=1}^{n} S_{m_t}+d_m \sum_{t=1}^{n} S_t \bmod (p-1)=S_m+d_m S \bmod (p-1)$$

该签名与我们预期得到的签名是完全一致的。

3.1.2 *ElGamal 密码体制向 DSS 规范的过渡* 限于篇幅，本文不再赘述 DSS 的细节以及子密钥的具体产生过程。特别指出，原始的 ElGamal 密钥体制与 DSS 中的 ElGamal 版本有一个重要的区别：

在 DSS 中，对于预签名的摘要 d_m，签名的等式为：$X=S_m^{-1}(d_m+S_{T_m}) \bmod q$，其中，$S_m^{-1}$ 是$(S_m \bmod q)$的乘法逆元。因此，我们不再对 S_m 进行密钥分割，而是对 S_m^{-1} 进行密钥分割。

(1)主从代理协作的串行签名(DSS 规范)

对于 n 个移动代理，密钥分割如下：

分割长期(恒定)私钥：$S=S_1+S_2+\cdots\cdots+S_n$；(主代理拥有 S_n)

分割短期(周期)私钥(乘法逆元)：$S_m^{-1}=S_{m_1} * S_{m_2} * \cdots * S_{m_n}$；(主代理拥有 S_{m_n})

签名的过程与3.1.1(1)所描述的串行多重签名基本相同，只是最后主代理得到的数字签名 $X_n=\prod_{t=1}^{n} S_{m_t}(d_m+\sum_{t=1}^{n} S_t T_m) \bmod q-T_m \sum_{t=1}^{n-1}(\prod_{k=1}^{t} S_{m_k-1})(\prod_{r=t+1}^{n} S_{m_r}) S_{t+1}$，显然这与我们所期待的正确的数字签名是不符合的，两者之间的差距在于：$X-X_n=T_m \sum_{t=1}^{n-1}(\prod_{k=1}^{t} S_{m_k}-1)(\prod_{r=t+1}^{n} S_{m_r}) S_{t+1}$，等式的右端仍是仅由一些常数项和子密钥组成，与3.1.1(1)同理，主代理只需将 X_n 稍加变化便能得到正确的签名。

(2)主从代理协作的并行签名(DSS 规范)

对于 n 个移动代理，私钥对的分割有如下形式：

分割长期(恒定)私钥：$S=S_1+S_2+\cdots+S_n$；(主代理拥有 S_n)

分割短期(周期)私钥：$S_m^{-1}=S_{m_1}+S_{m_2}+\cdots+S_{m_n}$；(主代理拥有 S_{m_n})

对于预签名的信息摘要 d_m，主从代理利用各自的子密钥

对并行签名的形式如下：

$X_1=S_{m_1}(d_m+S_1T_m) \bmod q, X_2=S_{m_2}(d_m+S_2T_m) \bmod q, \cdots, X_n=S_{m_n}(d_m+S_nT_m) \bmod q$；

各个从代理再将各自的签名 X_i 传送给主代理，由主代理合并这些签名，最后得到：$X'=\sum_{i=1}^{n}S_{m_i}(d_m+\sum_{i=1}^{n}S_iT_m) \bmod q - T_m\sum_{i=1}^{n}\sum_{\substack{k=1\\k\neq i}}^{n}S_{m_i}S_k$，遗憾的是这一签名 X 与我们所期待的签名有一些常数项和子密钥数值因子的差距，$X-X'=T_m\sum_{i=1}^{n}\sum_{\substack{k=1\\k\neq i}}^{n}S_{m_i}S_k$，然而得到正确的签名只需要源主机事先计算，签名完毕后由主代理进行调整即可。

3.2 基于主从代理协作多重数字签名的商务案例分析

假定源主机创建了三个移动代理——主代理、从代理1和从代理2。源主机为其委派任务，要求三个代理分别到三台远程主机 Host1、Host2和 Host3寻求某种型号手机的报价，找出报价最优的那台主机并与之签订购买协议。显然，要产生源主机合法的数字签名，源主机必须对其私钥(对)进行分割，并分派给三个移动代理。对于如何寻求报价本文不进行另外的阐述，假定 Host1对该型号手机的报价是最优的，那么协议的签订将在 Host1进行。鉴于串行和并行两种多重数字签名的形式，分别对其进行描述如下：

(a)主从代理串行签名的商务案例分析

如图1所示，具体的执行步骤按小圈中数字的次序进行。

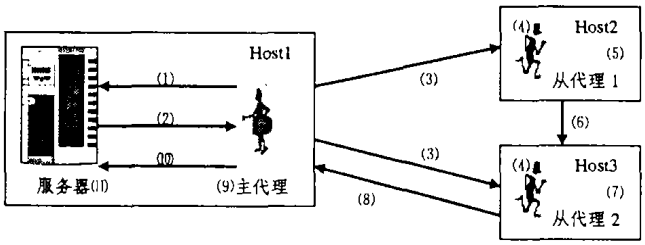

图1 主从代理协作串行签名的商务案例

(1) 主代理向 Host1索要某种型号手机的报价信息、购买协议和数字签名；

(2) Host1提供给主代理报价信息、购买协议和它的数字签名；

(3) 主代理将 Host1的报价信息、购买协议、数字签名分别传送给从代理1和从代理2；

(4) 从代理1和从代理2将分别验证签名的有效性；

(5) 验证无误后，从代理1用其子密钥对对购买协议进行签名，得到 X_1；

(6) 从代理1将签名 X_1 传送给从代理2；

(7) 同理，从代理2再对 X_1 进行签名得到 X_2；

(8) 从代理2将签名 X_2 传送给主代理；

(9) 主代理利用它的密钥信息和调整算法最终产生完整的签名 X；

(10) 主代理将签名 X 提交给主机 Host1；

(11) Host1用源主机公布的公开密钥验证签名的合法性，验证通过，则协议生效。

(b)主从代理并行签名的商务案例分析

如图2所示，具体的执行步骤按小圈中数字的次序进行。

(1)(2)(3)(4)的执行内容与(a)中的(1)(2)(3)(4)的执行内容完全相同；

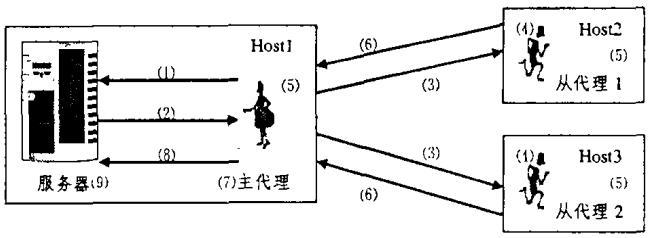

图2 主从代理协作并行签名的商务案例

(5)从代理1、从代理2、主代理分别利用各自的子密钥对产生签名 X_1、X_2和 X_3；

(6)从代理1和从代理2分别将 X_1和 X_2发送给主代理；

(7) 主代理利用调整算法合并签名，得到最终的签名 X；

(8)(9)的执行内容与(a)中的(10)(11)的执行内容完全相同。

3.3 安全性和有效性分析

(1) ElGamal 签名的安全性基于求离散对数的难题，要想从源主机的公开密钥推导出私有密钥对是极其困难的；

(2) 主代理向 Host1索要的报价信息、购买协议和数字签名可作为日后 Host1抵赖交易发生的凭证；

(3) 让从代理来验证 Host1的数字签名增加了安全性，因为主代理受控于 Host1，很有可能受到 Host1的“欺骗”；

(4) 恶意主机可能会窃取移动代理所携有的密钥信息，然而，由某个代理的子密钥信息推导出主密钥是极为困难的，除非窃取了所有的子密钥信息；

(5) 代理之间的及时通信也确保了签名过程的安全性；

(6) 任何人只需拥有源主机的公开密钥便能验证签名的合法性；

(7) 从最终的签名或某一代理的签名，无法推导出源主机的主密钥对或代理的子密钥对，这同样面临求解离散对数的困难；

(8) 只有所有真实子密钥对到齐时才能得出正确的签名，任何伪造或篡改密钥对的作弊行为均无法得到有效的合法签名。

结论 基于 ElGamal 密钥体制的主从代理协作串/并行签名的算法，通过上述的电子商务案例体现了其具体的运作过程。由3.3节的安全性和有效性分析可以证明，“主从代理协作的签名机制”的确为移动代理的安全问题提供了一种较好的安全策略和保护方案。尤其对于并行复杂的任务，多个移动代理的协作不但能保证安全性还能提高运作效率。然而，本文提供的方案仍然存在一些缺陷，如串行签名无法检测签名作弊者(是从代理1或 Host2作弊还是从代理2或 Host3作弊)，而且恶意主机的合谋攻击将有可能泄露源主机的所有子密钥对，并因此而泄露主密钥，下一步工作的重点将对这些潜在的安全隐患作进一步深入研究和探讨。

参 考 文 献

1 Shamir A. How to Share a Secret. Comm. ACM, 1979, 22:612～613

2 Blakley G R. Safeguarding Cryptographic Keys. Proc. NCC, AFIPS Press, Montvale, 1979,48:313～317

3 Harn L, Lin H Y, Yang S. Threshold Cryptosystem with Multiple Secret Sharing Policies. IEE Proc. Comput. Digit. Tech. 1994, 141(2):142～144

4 杨波，马文平，王育民. 一种新的密钥分割门限方案及密钥托管体制. 电子学报，1998，10:1～3

5 Boyd C. Some Applications of Multiple Key Ciphers. LNCS 330, Advances in Cryptology, EUROCRYPT'88 Proceedings, 1988

6 Ye Yiming, Yi Xun. Coalition Signature Scheme in Multi-agent System. In: 11th Intl. World Wide Web Conf. Honolulu, Hawaii, USA, May 2002
7 Elgamal T. A Public Key Cryptosystem and A Signature Scheme Based on Discrete Logarithms. IEEE Trans Inform. Theory, 1985, 31:469～472
8 Chang Y S, Wu T C, Huang S C. EIGamal-Like Digital Signature and Multi-signature Schemes Using Self-certified Public Keys. The Journal of System and Software, 2000, 50(2): 99～105
9 伊丽江,白国强,肖国镇.代理多重签名:一类新的代理签名方案.电子学报,2001,4:569～570
10 Roth V. Mutual Protection of Cooperating Agents. In:Jan Vitek and Christian Jensen, eds. Secure Internet Programming: Security Issues for Mobile and Distributed Objects, vol. 1603 of Lecture Notes in Computer Science, pp275～285
11 王汝传,徐小龙.移动代理安全机制的研究.计算机学报,2002,25(12):1294～1301
12 王汝传,赵新宁.基于网络的移动代理系统安全模型研究和分析.计算机学报,2002,26(4):477～483
13 王汝传,孙开翠.基于 JavaCard 的移动代理安全模型研究.通信学报,2003,24(11):27～33
14 Miao C, Wei R. Secret Sharing for Mobile Agent Cryptography. Communication Networks and Services Research Conference, Session B2, 2003. 93～100
15 Tate S R, Xu K. Mobile Agent Security Through Multi-Agent Cryptographic Protocols. In:The 4th Intl. Conf. on Internet Computing, 2003

(上接第78页)

4.4 DMABMA 中的缓存失效策略

缓存(Cache)技术在传统的分布式系统中得到广泛应用,但移动计算环境具有低带宽、易断连、低电源容量的特性,使得移动客户的缓存管理要充分考虑频繁断连带来的问题,因此,缓存管理协议应能优化利用有限带宽、容忍断连、有效使用电能,并对无线网络提供不同 QoS 的适应性。

Imielinski 和 Barbara 等人提出的"缓存失效报告技术"[7],能较好地适应移动计算环境的特点,但是存在若客户较长时间断线会令整个缓存失效的问题,其可伸缩性较差,而在我们 DMABMA 的体系结构中,由于移动代理技术的引入,能更好地解决这些问题。

我们在文[8]提出了一种"基于移动代理的缓存失效策略",如图4所示,每个移动主机,都在本机有一个数据缓存区;除此之外,在该主机所在的无线网络内,都有一个连接在固定网络上的移动服务支持站 MSS,MSS 上有 n 个移动代理(Mobile Agent)负责分别管理该网络内相应的 n 个 MH 的缓存副本,该副本称为本地缓存(Home Cache)。

对于一个具体的 MSS 而言,在它的覆盖范围内有 n 个移动主机(MH_i, $1\leqslant i\leqslant n$),对于任一个 i,都有一个相应的移动代理 MA_i 维护其 HC_i,此 HC_i 是对应 MH_i 的缓存副本。HC_i 由一系列的记录清单组成的,每个记录是一个三元组(x, TS, $invalid\_flag$)。其中 x 表示数据项,TS 是服务器在失效报告中提供时戳(Time-Stamp),$invalid\_flag$ 是失效标记,缺省值为 FALSE。

因为本方案的失效报告的传送是异步的,失效报告先缓存在 MA_i 中,当移动主机与 MSS 连接时才由 MA_i 传送报告给 MH_i。若失效项已发给 MH_i 但没收到确认,$invalid\_flag$ 被标记为 TRUE。

每个移动主机维护本机的经常被访问缓存数据项,在回答任何应用查询之前,它首先检查数据的一致性状态。具体过程如下:当 MSS 收到来自服务器的失效报告,MSS 通过和 MA 协商决定哪些 MH 集合需要这些数据并发送给它们。MH 收到失效信息,它使本机缓存中的相应数据项失效。当 MH 从应用层收到查询请求,检查缓存数据的有效性,如果数据项有效,在本地就可以满足查询;否则,向 MSS 中的 MA 发送上行查询,MA 再向服务器提出此请求,当 MA 从服务器收到请求数据后,先增加到 HC 中,再发送给 MH。

4.5 DMABMA 的优势

DBABMA 模型将移动代理划分为两个部分:MA_i 和 MA_i,它们都驻留在 MSS 上,MA_i 可与固定网络的服务器直接交互,MA_i 可与无线网络的移动主机 MH 直接交互。该结构最大的好处是通过移动代理的插入把移动计算环境分成了两大部分:传统的分布式网络部分和无线网络部分;这样针对不同的网络环境可以选择更合适的方法和技术解决相应的问题,增加了系统的可用性。

该模型可以很好地支持移动计算环境的断接性。由于 MA 存在于固定网络之中,即使 MH 处于断接状态,MA 仍然可利用固定网络的高带宽与 Server 交互执行任务;在 MH 上的局部数据缓存可以在一定程度上满足在断接情况下客户的数据需求,缓存的命中丢失可以由 MA 和 MH 联合进行处理,一旦再次连接成功就可以解决命中丢失问题;同样在断接状态,服务器端对客户的要求也可以在 MA 处进行缓存等待处理,直到再次成功连接。

该模型通过两种 MA 的共同协作来优化无线链路的使用,从而使不同的应用获益。它解决了 Client/Agent/Server 模型只能优化从固定网络到移动主机的数据传输,而不能优化从移动主机到固定网络的数据传输的问题;也解决了 Client/Intercept/Server 模型的每个应用都要求在服务器端和客户端开发相应的软件的问题;较好地满足了系统的动态可伸缩性的要求。

总结 本文提出了一种基于移动代理的数据管理体系结构 DMABMA,该结构与数据复制、数据广播和缓存技术相结合,能较好地适应移动计算环境的特殊要求,满足我们的设计目标,具有较强的可用性、可伸缩性和收敛性。

参 考 文 献

1 Coulouris G, Dollimore J, Kindberg T. Distributed Systems: Concepts and Design(Third Edition). Pearson Education, 2001
2 Imielinski T, Badrinath B R. Mobile wireless computing: challenges in data management. Communication of ACM, 1994, 37(10): 18～28
3 Dunham M H, Helal A. Mobile computing and databases: anything new? ACM SIGMOD Record, 1995, 24(4): 5～9
4 李东,冯玉才,王元珍.适于移动数据库的客户用及务器体系结构研究.计算机应用研究,2001(4):32～34
5 Gray J, Helland P. The dangers of replication and a solution. In: Proc. ACM SIGMOD Record, 1996, 25(2): 173～182
6 Anindya D, Debra E V, Aslihan C, Vijay K. Broadcast Protocals to support efficient retrieval from database by mobile users. ACM TODS, 1999, 24(1)1: 1～79
7 Barbara D, Imielinski T. Sleepers and Workaholics: Caching Strategies in Mobile Environments. In: Proc. of the1994 ACM-SIGMOD intl. conf. on Management of Data, May 1994. 1～12
8 吴劲,卢显良,任立勇.在移动计算环境中基于移动代理的缓存失效方案.计算机科学,2003,30(4):82～84