一个基于移动 Agent 防止双重消费的离线电子支付模型及协议*)

A Model and Protocols of Off-line Electronic Payment Preventing Double-spending Based on Mobile Agents

温 涛[1] 王济勇[2] 刘积仁[3]

(东北大学东软信息技术学院 大连116023)[1]

(东北大学信息学院计算机网络通信工程研究所 沈阳110004)[2](东北大学软件中心 沈阳110004)[3]

Abstract Because it is quite unsatisfactory that in anonymous off-line payment schemes the multiple spending of coins can only be detected but not prevented, a model and protocols of off-line electronic payment system preventing double-spending and based on Mobile Agents are presented in this paper, which improve the off-line payment scheme based on hardware observer[1]. Because the hardware device called Observer in [2] is replaced by the software object of Mobile Agents which is called Mobile Observer, thus customers don't need to worry about the bottle-neck and vulnerability owing to all the interactions to a single device. This paper discusses the life recycle of the Mobile Observer and the security problems of the Mobile Agents system. In addition, this model presents a recovery mechanism for the failure of the customer end system. Hence, the security, robustness, practicality of the model are higher than any one of the previous systems.

Keywords Off-line electronic payment, Mobile Agent, Mobile Observer, Double-spending

1 引言

随着基于 Internet 的电子商务发展,电子支付因其比传统支付系统具有操作简便、运行成本低廉和资金周转迅速等优点而成为未来电子商务发展的趋势和必然。目前,国际上电子支付主要基于两种模式:预付模式(prepaid model)和后付模式(pay-later model)。其中,预付模式主要采用基于智能卡的电子现金(e-cash)支付;而后付模式主要采用基于信用卡的电子支付[3]。

匿名电子支付系统可以用掩饰签名方案实现。当顾客要提款时,银行为顾客掩饰地签名一个消息(通常是一个随机数)。银行的签名使得这个消息成为一个合法的具有一致值的币值。顾客能够在给商店的支付中使用这个电子货币。由于掩饰签名方案的属性,银行没有关于电子货币的信息(除了它的币值)。因此,支付是匿名的和不可连结的。

在在线系统中,双重消费能够通过银行检查以前的存款记录来防止。这要求所有的存款记录都要保留(至少在银行公开密钥的合法期内);在离线系统中,双重消费不能被防止,但是设计一个系统允许在一笔钱被多次消费时,撤消顾客的匿名性是可能的。确保顾客的标识(身份)被合适地编码在签名的消息中,并且使顾客在支付阶段回答一个质询消息,通过这种方法顾客的身份能够从两个不同的质询中计算出来。作为选择,文[4]中提出的匿名撤消机制可以被使用,但是,在离线系统中,双重消费只能检测不能防止,相当令人不满意。

随着计算机网络的迅速发展,分布式计算越来越成为当今计算机技术的关键研究领域,其主要目标在于实现跨平台资源的透明互操作机制和协同计算。移动 Agent 是一独立计算机程序,它可以自主地在异构的网络上,按照一定的规程迁移,寻找合适的计算资源、信息资源或软件资源,利用这些资源同处一台主机或网络的优势,处理或使用这些资源,代表用户完成特定的任务[5]。移动 Agent 改变了传统的分布式系统的设计和实现。客户/服务器模式和移动代码模式相比,这种新的分布式计算模式具有如下优点:(1)节省带宽,减轻网络负载;(2)提高响应速度;(3)均衡负载;(4)重构组件;(5)易于理解且方便地编程范例。

为此,本文提出了一个基于移动 Agent 的离线电子支付模型及协议,它既满足匿名性和匿名性可撤消的要求,又能防止双重消费,还解决了与单个设备交互带来的系统瓶颈和脆弱性问题。

2 一个基于移动 Agent 的离线电子支付的模型及协议

本文提出的基于移动 Agent 的离线电子支付的模型是用一个称为移动发现者 MO 的移动 Agent 软件对象代替 Chaum 等[6]提出的称为发现者的硬件设备,使其完成与硬件发现者相同的功能,模型如图1。下面的要求保证了顾客的隐私:

·除了顾客,移动发现者 MO 不能跟任何人通信。特别是,移动发现者 MO 不能与银行建立一个潜在的通道。

·即使银行控制了一个移动发现者 MO 并读取了存储在其中的所有信息,银行也必须不能跟踪支付。

·顾客每次提款创建的移动发现者 MO 的私人/公开密钥对是相同的。

图1中出示了移动发现者 MO、顾客、银行和商店之间的通信。由于每个顾客的移动发现者 MO 是唯一的(实际上是在时间上,每个顾客同时可以对应多个移动发现者 MO,但它们的私人/公开密钥对总是相同的),银行能够用(i)连结(ii)和(iii)。为了满足上面提到的条件,通信(iv)一定不能连结通信(i)和通信(iii)。

*) 本文研究得到国家863高科技项目基金资助(编号:863-306-ZT05-05-5)。温 涛 博士,教授,主要研究领域:计算机网络、网络安全。王济勇 博士生,主要研究领域:计算机网络安全、数据融合。刘积仁 博士,教授,博士生导师,主要研究领域:分布式多媒体技术、网络安全。

本模型的主要思想是，一个电子货币由三个主要部件组成，即满足 $z_p=h_p^x$ 的序对(h_p,z_p)，其中 x 是银行的私人密钥；以这个事实为证据的一个签名（记为 W）；另一个签名（记为 V）用于保证匿名性是可撤消的。签名 W 由银行给出，签名 V 由顾客给出。为了得到匿名性，签名 W 的发布必须使用掩饰签名方案：在提款阶段顾客发送给银行一个随机化了（掩饰）的序对(h_w,z_w)，银行基于这个序对计算相应于 W 的签名，顾客将这个签名转换成签名 W。这通过提款协议的一个子协议 P_o来实现。如果托管人能够连结序对(h_p,z_p)和(h_w,z_w)，他就能撤消电子货币的匿名性。

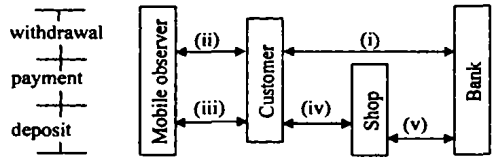

图1　顾客需要移动发现者的帮助来执行提款和支付事务。对于每个电子货币，移动发现者仅参与一次支付事务，因此一个电子货币的多重消费能防止。

2.1　系统建立

2.1.1　*符号及基本定义*　为了建立一个基于移动 Agent 的离线电子支付系统模型，本文中假设整数、代数群元素和文本串都存在二进制的标准表示，且 $a\|b$ 表示用 a 和 b 的二进制串表示的连接。

$c[i]$表示串 c 从右端数的第 i 位。符号$(c_i)_{i\in S}$表示 c_i 的顺序列表，其中 i 是集合 S 中的元素。符号 $Pr_i(.)$表示元组的第 i 投影，如 $Pr_i((x_1,\cdots,x_n))=x_i$。

表达式 $\varepsilon\in_R X$ 表示从有限集 X 中根据一致分布随机选择 ε。

为了建立该模型，本文定义了如下两个 SPK（signatures based on proofs of knowledge）。

定义1　序对$(c,s)\in\{0,1\}^t\times Z_q$ 满足：

$c=H(S\|V\|m)$，其中 $S=g\|y$ 且 $V=g^sy^c$

是消息 $m\in\{0,1\}^*$ 关于代数群元素 y 以 g 为底离散对数的一个 SPK，记为：

$SPKLOG\{(a):y=g^a\}(m)$。

如果（密钥）$x=\log_g y$ 的值知道，就能够计算 $SPKLOG\{(a):y=g^a\}(m)$，过程如下：

1. 选择 $r\in_R Z_q$；
2. 计算 $t=g^r$；
3. 计算 $c:=H(g\|y\|t\|m)$，然后 $s:=r-cx(\mathrm{mod}q)$。

定义2　序对$(c,s)\in\{0,1\}^t\times Z_q$ 满足：

$c=H(S\|V\|m)$，其中 $S=g\|h\|y\|z$ 且 $V=g^sy^c\|h^sz^c$

是消息 $m\in\{0,1\}^*$ 基于代数群元素 z 以 h 为底离散对数和代数群元素 y 以 g 为底离散对数的知识证明和两个离散对数相等的签名，记为：

$SPKLOGEQ\{(a):y=g^a\wedge z=h^a\}(m)$

如果知道 $x=\log_g y$ 的值且 $\log_g y=\log_h z$ 成立，就能计算签名 $SPKLOGEQ\{(a):y=g^a\wedge z=h^a\}(m)$，过程如下：

1. 选择 $r\in_R Z_q$；
2. 计算 $t_1=g^r$ 和 $t_2=h^r$；
3. 计算 $c:=H(g\|y\|y\|z\|t_1\|t_2\|m)$，然后 $s:=r-cx(mod\ q)$。

2.1.2　*系统建立*　为了建立一个基于移动 *Agent* 的离线电子支付系统，银行选择一个序为素数 q 的有限群 G，使得在 G 中计算离散对数是不可行的。现在选择 $q\approx2^{170}$被证明是安全的除非这个群有特殊的结构。三个元素 g,g_1 和 g_2由公开可验证的随机机制来保证任何一个对其它两个中的任何一个的离散对数都是未知的。最后，银行选择密钥 $x\in_R Z_q$ 并计算公开密钥 $y=g^x$。银行公布 G,g,g_1,g_2和 y。

托管人随机地选择它的私人密钥 $\tau\in Z_q^*$ 并计算和公布相应的公开密钥 $y_T=g_2^\tau$。

2.2　移动发现者参与的子协议 P_o 的设计

该子协议 P_o的基本思想是，顾客和移动发现者 MO 共享一个值 a，使得他们中的任何一个单独都不能知道 a。具体实现方法是，用积 $\hat{a}a(\mathrm{mod}\ q)$来代替 a，其中 $\hat{a}$ 由移动发现者 MO 选择（保持机密），a 由顾客选择。对于在线系统[2]中涉及到 a 的所有计算，在子协议 P_o中必须有移动发现者 MO 的协同才能完成。而且，在从银行提取一个电子货币期间，顾客必须向银行证明值 a 确实与移动发现者 MO 共享。因此，移动发现者 MO 能够防止双重消费。令 $\tilde{\omega}$ 和 $y_o=g_1^{\tilde{\omega}}$分别表示移动发现者 MO 的私人密钥和公开密钥。

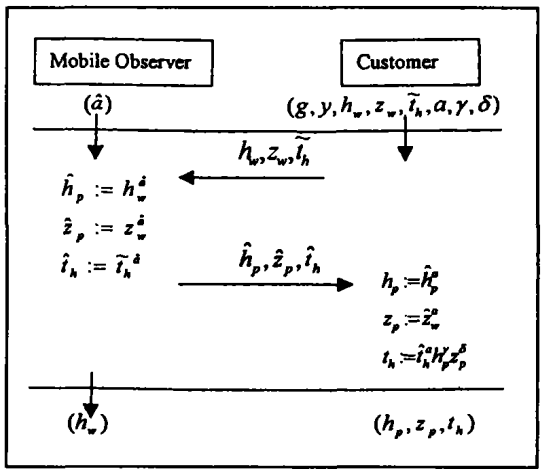

图2　基于移动发现者的系统

本文提出的子协议 P_o是对文[2]中子协议 P 的修改，如图2，参数 a 出现在 h_p,z_p 和 t_h 的计算中。移动发现者 MO 知道的值$(h_w,z_w$ 和 $\tilde{t}_h)$银行都知道，因此，没有将信息泄露给移动发现者 MO。在结果协议 P_o 中，参数 $\hat{a}a$ 代替了协议 P 中 A 的输入 a,h_p,z_p 和 t_h 的计算必须由顾客和移动发现者 MO 联合完成。

2.3　移动发现者参与提款和支付协议

本文提出的由移动发现者 MO 参与的提款协议如图3。鉴别之后，顾客和移动发现者 MO 联合计算 h_w 和 d。然后他们联合创建两个 SPK，$u_1=SPKLOG\{(a):\frac{h_w}{g_2}=y_o^a\}$和 $u_2=SPKEQ\{(a):\frac{h_w}{g_2}=g_1^a\wedge y_\tau=d^a\}$。顾客和移动发现者 MO 执行计算签名 u_1和 u_2的协议是相应于两个签名 $u_1'=SPKLOG\{(a):\hat{h}_w=y_o^a\}$和 $u_2=SPKEQ\{(a):\hat{h}_w=g_1^a\wedge y_T=d^a\}$的交互式协议，这也是一个诚实验证者的零知识协议。使用这个协议顾客能够计算签名 u_1和 u_2。签名 u_2的计算与文[2]中在线方案 u 的计算相同，同时向银行证实了 d 计算的正确性。签名 u_1向银行证实了移动发现者 MO 确实参与到了协议中，因为 $\log_{(h_w/g_2)}y_o$（由于 u_1）和 $\log_{g_1}h_w/g_2$（由于 u_2）的知识暗示着 $\log_{g_1}y_o(=\tilde{\omega})$的知识，即移动发现者 MO 的密钥。银行知道移动发现者 MO 不会偏离协议，因为它知道顾客单独不能知道 $\log_{(h_w/g_2)}g_1$的值。

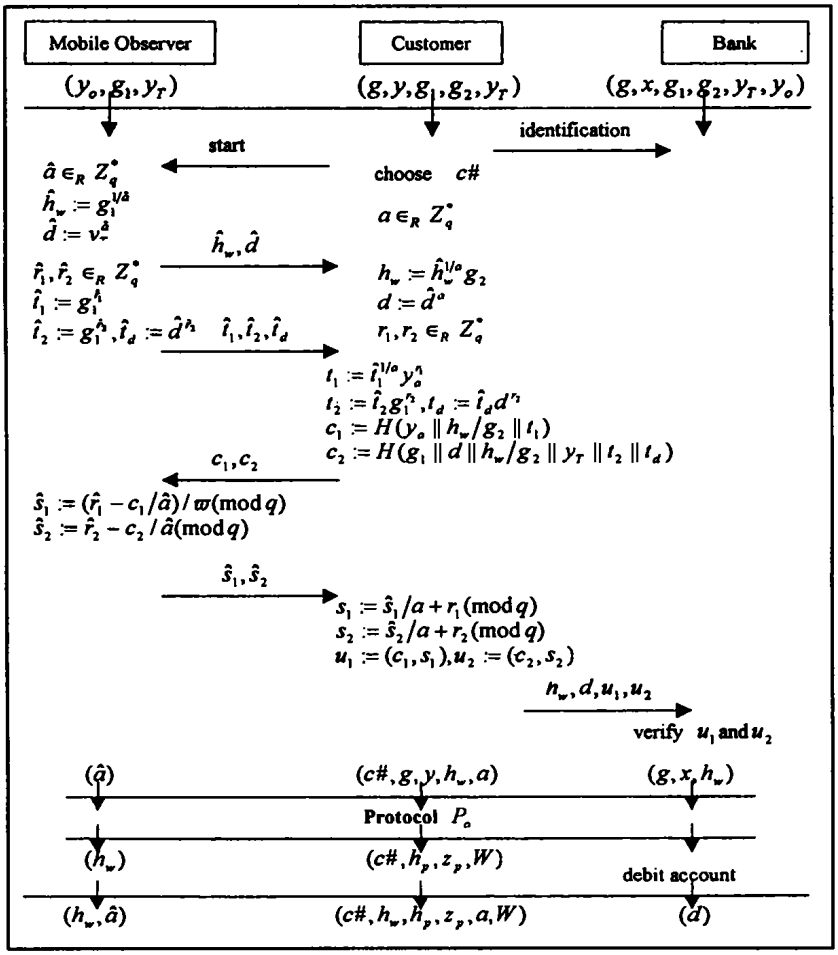

图3　带有移动发现者的离线系统提款协议

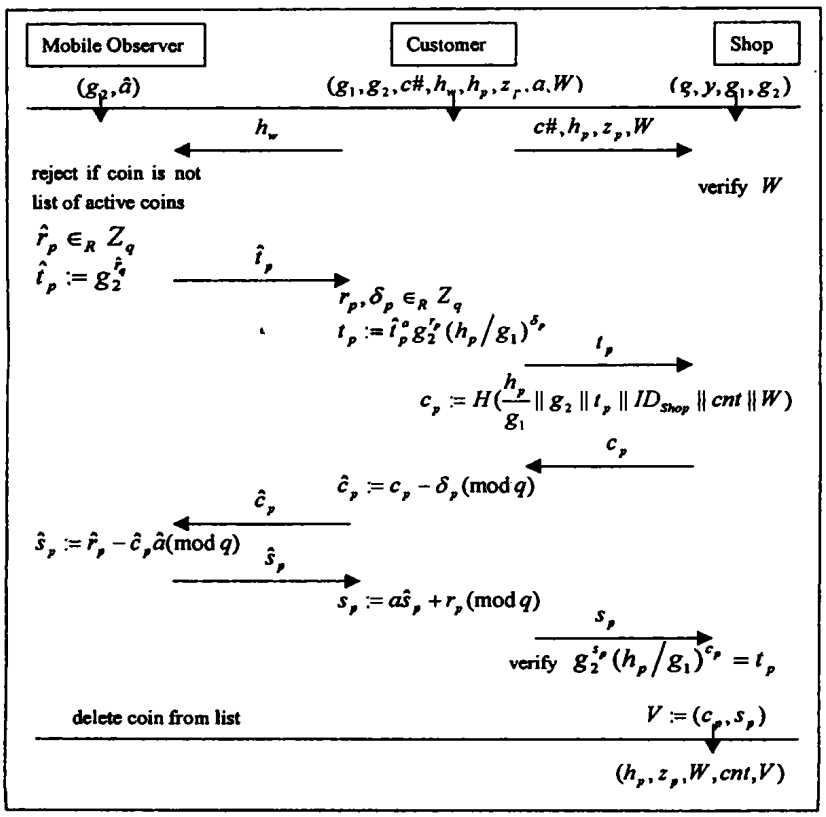

图4　基于移动发现者离线系统中的支付协议

下面的式子证明了图3的提款协议中签名 u_1 和 u_2 的计算确实是合法的。有下式成立：

$$y_o'^{r_1}\left(\frac{h_w}{g_2}\right)^{c_1}=y_o'^{r_1/a+r_1}\hat{h}_w^{c_1/a}=y_o^{(r_1-c_1/\hat{a})/\hat{a}a+r_1}\hat{h}_w^{c_1/a}=y_o^{r_1}g_1'^{r_1-c_1/\hat{a}}\hat{h}_w^{c_1/a}$$
$$=y_o^{r_1}g'^{r_1/a-c_1/(\hat{a}a)}g_1'^{r_1/(\hat{a}a)}=y_o^{r_1}g_1'^{r_1/a}=y_o^{r_1}\hat{t}_1^{1/a}=t_1$$

因此 u_1 的验证方程成立。对于 u_2，这里仅证明 $d'^{r_2}y_T'^{c_2}$ 成立。$g_1'^{c_2}\left(\frac{h_w}{g_2}\right)^{c_2}=t_2$ 的证明与此类似。因为有下式成立 $d'^{r_2}y_T'^{c_2}=d'^{r_2/a+r_2}y_T'^{c_2}=d^{r_2}d'^{(r_2-c_2/\hat{a})/a}y_T'^{c_2}=d^{r_2}\hat{d}'^{r_2-c_2/\hat{a}}y_T^{-c_2}=d^{r_2}\hat{d}^{r_2}y_T^{-c_2}y_T'^{c_2}=d^{r_2}\hat{t}_d=t_d$，所以验证 u_2 的方程也是成立的。

在创建这两个签名的过程中，很重要的一点是，由顾客使用随机值 r_1 和 r_2 来完成的额外的随机化过程（掩饰过程）。为防止银行得到值 $\hat{s}_1$ 和 $\hat{s}_2$，使用 s_1 和 $\hat{s}_1$（或者 s_2 和 $\hat{s}_2$）计算出 a，因为当移动发现者 MO 返回到银行或者当银行知道移动发现者 MO 随机数发生器的种子时，这种情况可能发生。

在提款协议结束时，移动发现者 MO 和顾客都保存 h_w，为了以后在本文提出的支付协议（如图4）中鉴别电子货币。

除了移动发现者 MO 和顾客联合计算签名 V 以外，顾客和移动发现者 MO 之间的通信不能与商店和顾客之间的通信连结是至关重要的。这样才能保证无论是银行还是移动发现者 MO 都不会得到关于相应于提款和支付事务的有用信息。这是通过随机化（掩饰）t_p，c_p 和 s_p 来实现的。顾客与移动发现者 MO 之间的协议是相应于 $SPK,V'=SPKLOG\{(a):(\frac{h_t}{g_1})^{1/a}=g_2^a\}$ 的交互式协议，因此这也是个诚实验证者的零知识协议。使用这个协议，顾客能够计算签名 V。既然移动发现者 MO 对于给定 h_w 和 $\hat{a}$ 仅执行这个协议一次，顾客不能双重消费一个电子货币。

在本文提出的支付协议结束时，商店将拥有签名 $V=SPKLOG\{(a):h_p/g_1=g_2^a\}(ID_{Shop}\|cnt\|W)$。

图4中协议的正确性的证明如下：

$$g_2'^{a}\left(\frac{h_t}{g_1}\right)^{c_p}=g_2^{(ar_p-\hat{c}\hat{a}a+r_p)}\left(\frac{h_t}{g_1}\right)^{c_p}=\hat{t}_p^{a}g_2^{(r_p+\theta_p\hat{a}a)}=\hat{t}_p^{a}g_2^{r_p}\left(\frac{h_t}{g_1}\right)^{\theta_p}=t_p$$

因此，V 的验证方程成立。这里，使用的事实是 $h_p=g_1g_2^{\hat{a}a}$。

3 移动发现者的生命期分析

本文提出的移动发现者 MO 是一个移动 Agent 对象，必然有一定的生命期。与文[2]中使用的硬件设备不同，移动发现者 MO 不可能总是存在于顾客能够使用的机器上。因此，本文要讨论的问题是由谁来创建移动发现者 MO，移动发现者 MO 与顾客交互时应处的位置以及每个移动发现者 MO 在生命期内所担负的责任。

移动发现者 MO 是由银行来创建，在顾客有提款请求时，完成对顾客的认证（执行相应的鉴别协议），如果认证成功，银行创建一个移动发现者 MO。移动发现者 MO 携带对应于这个顾客的私人密钥 x_o，并被传送到顾客所在的本地机器，与顾客交互。与文[2]中硬件设备发现者不同，每个移动发现者 MO 对应一个未消费电子货币。在顾客的本地机器与顾客交互的过程和硬件设备发现者相同。一旦对应的电子货币消费掉，此移动发现者 MO 自行销毁。

移动发现者 MO 除了具有移动性和每个移动发现者 MO 对应一个活动的电子货币，它还具有文[2]中硬件设备发现者的所有属性，因此，它能够防止双重消费。

4 一个新的基于移动发现者电子支付系统的恢复机制

本文提出的基于移动发现者 MO 的离线电子支付系统与基于硬件设备发现者的系统都面临一个顾客端系统瘫痪后恢复的问题，即如果移动发现者 MO 或者硬件设备发现者所在的机器突然瘫痪，如何处理丢失的所有活动电子货币。但是硬件设备瘫痪的机率要比软件对象小得多，因此，本文提出的模型中的系统恢复需要特殊对待。这种系统恢复的解决方案是，对于每个由银行发行的电子货币都设定一个生命期限，如果在期限内没有被花费掉，就被视为无效，这样由于顾客本地机器瘫痪造成的电子货币丢失，在这些电子货币的生命期限过后，会自动加到相应顾客的帐户上。

5 安全属性分析

本文提出的模型同样具有基于硬件设备发现者离线电子支付模型[2]的如下安全属性：1）支付是不可连结的和匿名的；2）电子货币是不能伪造的；3）双重消费能够检测；4）可撤消的匿名性；5）顾客不能被错误地被指控为双重消费；6）商店能验证电子货币的合法性。

引入了移动 Agent 对象作为移动发现者 MO，又引发了另外的安全问题。但是，由于本文提出的模型使用的移动 Agent 除了 CPU 和内存资源外无需其它资源，在这种情况下，利用文[8]中的安全体系结构模型，本模型的安全性能够得到保障。

最后，对于基于移动发现者 MO 的系统，与文[2]中基于硬件设备发现者的系统相同，是否不能侵犯顾客隐私（即使以后当银行控制了它）还有待于证明。这在文[2]中进行了讨论。

结论 本文提出的基于移动 Agent 的离线电子支付模型实际上是一种半离线的电子支付模型，因为提款结束时存在一个银行创建的软件对象，它能够在支付时与用户交互。这种软件对象是文[2]中使用的发现者硬件设备的软件实现，基于的理论和实现技术上二者基本上相同，因此本模型不仅具有基于硬件设备发现者模型的所有安全属性，还解决了由于单个硬件设备而引起的系统瓶颈和脆弱性问题。对于本模型引入移动 Agent 而引发的安全问题和顾客端系统瘫痪问题，本文也给出了具体的解决方案。与基于硬件设备发现者的模型一样，本模型中顾客的隐私不受侵犯还有待于证明。

参考文献

1 Camenisch J ,et al. Efficient group signature for large groups. In: Proc. CRYPTO'97, Springer-Verlag, 1997. 410～424
2 Camenisch J,Maurer U,Stadler M . Digital payment systems with passive anonymity-revoking trustees. Journal of Computer Security,1997,5(1):69～89
3 Asokan N,et al. The State of the Art in Electronic Payment Systems. IEEE Computer, 1997(Sep.):28～35
4 an Camenisch. An efficient and generalized group signatures. In: Proc. EUROCRYPT 97, pages 465 ～ 479, Springer-Verlag, 1997. Lecture Notes in Computer Science No. 1223
5 陶先平，吕建，董桓，李新. 流动 agent：一种未来的分布计算模式. 计算机科学，1999,26 (2):1～4
6 Chaum D . Achieving electronic privacy. Scientific American, August 1992. 96～101
7 Cramer R J F,Pedersen T P. Improved privacy in wallets with observers. In Tor Helleseth, editor, Advances in Cryptology --- EUROCRYPT'93, volume 765 of Lecture Notes in Computer Science, Springer-Verlag, 1994. 329～343,
8 王济勇，温涛，李春光. 一个基于 Java 的 Mobile Agent 安全体系结构模型. 计算机工程与应用，2000,10