移动商务环境中基于交易票据的自动信任协商协议

刘百灵 雷 超 李延晖
(华中师范大学信息管理学院 武汉 430079)

摘 要 针对移动商务环境下使用现有信任协商方案存在的计算开销大的问题,提出一种基于交易票据的自动信任协商协议。首先,协商双方依据交易票据评估对方的信任度,然后根据信任度动态地调整访问控制策略来进行协商,最后双方交换信任证,协商双方根据交易票据和验证权证减少信任证验证次数,从而完成协商过程。经证明,基于交易票据的自动信任协商协议能够有效减少计算开销。

关键词 移动商务,自动信任协商,协商效率,信任度评估

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.10.030

Automated Trust Negotiation Protocol Based on Transactional Receipt in Mobile Commerce Environment

LIU Bai-ling LEI Chao LI Yan-hui
(School of Information Management, Central China Normal University, Wuhan 430079, China)

Abstract It is difficult to use trust negotiation in the mobile environment since existing trust negotiation mechanisms have large computational overhead. To address this problem, a transaction receipt-based mobile trust negotiation protocol was proposed. Firstly, both sides of the negotiation evaluate each other's trust degree based on the transaction receipt. Secondly, they dynamicly adjust the access control policy on the basis of the evaluated trust degree. Finally, they enter into the digital certificate exchanging process, in which the number of certificate authentication is reduced by taking advantages of transaction receipt and authentication ticket. The experiments show that this protocol can effectively reduce computational overhead.

Keywords Mobile commerce, Automated trust negotiation, Negotiation efficiency, Trust degree evaluation

1 引言

移动商务是一种新兴的电子商务模式,它依托移动通信网络,使用手机、掌上电脑和笔记本电脑等移动终端设备进行各类商务活动和商业信息交互[1]。移动商务克服了传统商务在时间和空间上的局限性,使用户可以随时随地访问和获取信息和服务,是一个市场需求很大的综合信息服务领域。但我国移动商务应用程度较低,接受程度不高[2,3]。很多学者指出,缺乏消费者信任是影响电子商务发展的重要因素之一[4,5],而移动商务作为电子商务的一个子集,消费者对其缺乏信任也成为其发展的障碍[6-8]。

目前,国内外关于电子商务环境下信任的研究比较多,而对移动商务环境下消费者信任的研究较少[6,15]。建立移动商务用户信任比传统电子商务中的信任更加困难。相对于传统电子商务环境,移动商务环境更具开放性和跨域性,各种服务和用户均是高度动态变化的,服务请求者和服务提供者在很多情况下是彼此陌生的,同时,随着无线网络应用的不断拓展,用户个人资料被泄露的机会明显增加,因此用户信息安全面临严重的威胁;相对于传统电子商务终端设备PC机,移动终端界面较小且分辨率低,键盘的功能有限,使得用户的信息浏览和交易操作都不方便,且移动终端设备的计算能力也受到限制,通信带宽成本较高。因此需要一种灵活、自动、高效的信任建立机制来解决跨域的陌生交易主体之间信任建立的问题。

自动信任协商(Automated Trust Negotiation, ATN)[9]被认为是解决跨域陌生实体之间信任建立的一种有效方法。协商双方通过交替披露访问控制策略和数字信任证以在陌生主体之间逐步建立信任关系[10,11]。将信任协商引入移动商务以辅助用户与移动服务提供商建立信任,具有以下优势:

(1)满足移动用户的多样化和个性化需求。移动商家和消费者都能够通过访问控制策略制定个人信息披露规则和交易服务规则等。同时由于信任建立是双向的,这种交互协商行为能增强用户感知的交互性,增加移动用户的信任。

(2)在保证个人敏感信息安全的前提下,提高移动商家和消费者的交易机会。信任协商通过双向协商建立信任,即消费者也可以要求移动商家提供一些必要信息以决策是否满足消费者信息披露规则,实现个人敏感信息保护。

(3)信任的建立基于陌生交易主体的相关属性,而非其身份。

到稿日期:2015-08-21 返修日期:2015-12-28 本文受国家自然科学基金项目(71571082,71101061),中央高校基本科研业务费项目(CCNU14Z02016,CCNU15A02046)资助。

刘百灵(1983-),女,博士,副教授,主要研究方向为自动信任协商、信息隐私,E-mail:bl_liu@mail.ccnu.edu.cn;雷 超(1989-),男,硕士,主要研究方向为自动信任协商;李延晖(1974-),男,博士,教授,主要研究方向为电子商务。

交易双方之间的信任关系是通过属性信息的逐步交换而建立的，这种基于属性信息的动态信任建立方式适合开放跨域的移动商务环境中陌生交易主体之间的信任建立。

(4)协商过程无需人工干预。整个信任协商过程利用协商代理在协商策略算法的控制下自动完成，适用于界面较小且键盘功能有限的移动终端设备。

因此信任协商能够解决开放的移动商务环境中大量陌生交易主体间的信任建立问题。在协商交互过程中，双方根据各自的访问控制策略，交换属性证书并进行有效性验证。访问控制策略越复杂，交换的证书可能会越多，为验证证书有效性而进行的公钥密码运算的次数也越多，会带来较大的计算开销，其不适合用于包含大量资源受限的移动终端设备的移动商务环境中。

为此，提出了一种基于交易票据的自动信任协商协议，该协议分为3个阶段：1)寒暄阶段。主要任务是协商双方评估对方的信任度，其中移动服务商根据用户提供的交易票据计算其信任度。2)信任序列生成阶段。协商双方通过评估信任度动态调整访问控制策略，之后根据协商策略逐步协商，生成信任证披露序列。3)信任证交换阶段。协商双方根据信任证披露序列交换信任证，并通过交易票据和验证权证减少信任证有效性验证次数。该协议利用交易票据，既能根据信任度优化访问控制策略，同时也能减少信任证有效性验证次数，最大限度地减少了协商带来的计算开销。

本文第2节主要介绍自动信任协商的概念及相关工作；第3节提出基于交易票据的自动信任协商协议；第4节通过实验对协议性能进行分析；最后总结全文。

2 相关工作

本节主要介绍自动信任协商的概念和相关工作研究的进展。

2.1 自动信任协商

自动信任协商通过逐步请求和披露信任证以在陌生实体之间建立信任，被视为一种在跨安全域的陌生实体间建立信任的有效方法。Winsborough等人[9]将自动信任协商抽象定义为构造一条信任证披露序列。假设 $ClientCreds$ 是资源请求方的数字证书，$ServerCreds$ 是资源提供方的数字证书，则证书披露序列可以描述为：$\{C_i\}_{i\in[0,2n+1]}=C_0,C_1,\cdots,C_{2n+1}$，其中 $n\in N$，$C_{2i}\subseteq ClientCreds$，$C_{2i+1}\subseteq ServerCreds$。其中证书集合 C 满足 $C=ClientCreds\cup ServerCreds$。

如图1[16]所示，Alice和Bob是两个协商实体，其中Alice向Bob请求服务。此次协商的证书披露序列为：{*BBB Credential*, *VISA Card*, *Service*}。

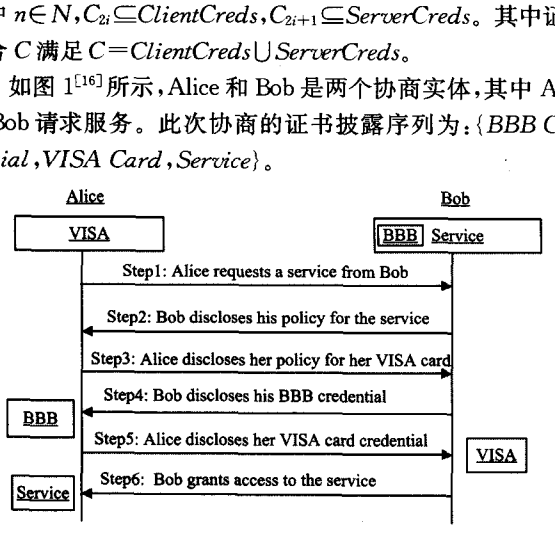


图1 Alice与Bob的协商过程

2.2 代表性的相关工作

在自动信任协商的研究中，考虑了协商效率提升的代表性工作有Trust-X[17,18]，它开创了利用历史协商信息提高协商效率的新思想，例如对某服务进行交易成功后，交易双方彼此颁发TrustTicket，在某期限之内他们要对同样的服务再次进行交易时，可通过出示双方曾经颁发的TrustTicket快速建立信任，而无需使用协商策略算法。此外，将通过逐步协商而建立信任的协商信息缓存，以便当同样的交易被请求时可以直接利用缓存的信息加快信任建立的速度。

鲁宏伟等[19]提出了有穷自动机协商策略DFANS，确保协商过程中没有与协商无关的信任证披露。DFANS利用OSBE方案[20]处理回环依赖问题，增加了额外的计算开销，在协商双方访问控制策略允许的情况下，总能够保证协商成功。

李建欣等[21]引入了基于契约的信任协商方法，即在协商的初期双方确立契约，若无法达成契约，则尽早终止无法进行的协商，避免不必要的后续协商过程。

李建利等[22]提出了基于有穷自动机的自动信任协商策略，构造有穷自动机状态转化图对相应的访问控制策略进行图形化表示，在谨慎策略的基础上加入记忆链结构，以减少协商双方的交互次数，提高协商效率。

汪秋云等[23]提出了基于属性披露的移动信任协商方案，协商双方根据对对方信任度的评估，预先选择性地显露证书中的某些敏感属性，之后再根据协商策略多次交换属性加密密钥，逐步向对方显示自己的属性。该方案基本解决了在移动商务环境下进行信任协商造成的计算开销大的问题。

目前，国内外关于传统电子商务环境下的消费者信任研究较多，而对移动商务信任的研究较少，尤其缺乏将自动信任协商用于移动商务环境方面的研究。上述协商策略都在一定程度上提高了协商效率，但均没有考虑在资源受限的环境下信任证有效性验证的计算开销。

3 基于交易票据的信任协商协议

3.1 基本概念

移动商务环境中，移动用户的历史交易信息能够在一定程度上反映该用户的信任度。因此本策略主要通过合理利用移动用户的历史交易信息来提高信任协商的效率。相关定义如下。

定义1(证书 c) 证书 c 定义为一个四元组$\langle CredInfo, AttrInfo, SigInfo, KeyInfo\rangle$，其中，$CredInfo$ 是信任证属性集合{$CredName, CredID, Issuer, ExpirationDate$}，分别表示该信任证的证书名、证书ID号、颁发者、有效期；$AttrInfo$ 单个是信任证属性的集合{$(AttrName_1, AttrValue_1)$, $(AttrName_2, AttrValue_2)$,…}。$SigInfo$ 包含信任证的签名信息，验证信任证的真实性和完整性。$KeyInfo$ 是信任证的公钥信息。

移动用户与移动服务提供商通过信任协商逐步建立信任，并成功进行交易。当交易结束时，移动服务提供商给移动用户签发一张交易票据，该票据注明本次交易的一系列信息，定义如下。

定义2(交易票据，transaction receipt，tr) tr 定义为一个五元组$\langle tranID, AttrInfo, CredList, SigInfo, KeyInfo\rangle$，其中，$tranID$ 是交易号，用来标识某一交易；$AttrInfo$ 是交易

属性集合{*issuer*, *subject*, *category*, *price*, *date*, *rating*}，分别表示该交易票据的颁发者、拥有者、交易种类、交易价格、交易时间以及服务提供商对用户此次交易的评价；*CredList* 表示交易过程中移动用户披露的信任证 ID 号和颁发者的哈希值集合{$hash(CredID_1 | issuer_1 | n_1)$, $hash(CredID_2 | issuer_2 | n_2)$, …}，其中 $n_i(i \in N)$ 表示随机数。*SigInfo* 包含颁发者的签名信息，例如签名算法、数字签名等。*KeyInfo* 是交易票据颁发者的公钥，用于验证该交易票据的签名信息。

交易票据中只包含信任证的哈希，一方面，信任证的哈希能唯一识别该信任证；另一方面，用这些哈希值识别已经通过认证的信任证，即使交易票据披露，也可以保证其中信任证内容的安全，同时不会增加密码算法那样昂贵的负担。

为了更好地保护隐私，如果协商方认为某些信任证属于拥有敏感[10]，那么这类信任证将不会出现在交易票据中。

在协商过程中，移动用户会选取合适的交易票据发送给移动服务提供商，移动服务提供商收到交易票据后验证交易票据的颁发者是否为可信实体，例如交易票据的颁发者与移动服务提供商是否处在同一个虚拟组织域(Virtual Organization, VO)等。若为可信实体，则移动服务提供商信任该交易票据，否则该交易票据失效。

定义 3(信任度) 假设移动服务提供商接收并信任某一交易票据 *tr*，移动服务商根据 *tr* 确定移动用户的信任度。用户信任度计算公式定义为：

$$w=(\frac{1}{2}r+\frac{1}{2}p)\times d \tag{1}$$

其中，r 表示交易票据的颁发者对用户的交易评价 *tr. AttrInfo. rating*，*tr. AttrInfo. rating* 越高，表明移动用户的历史交易行为越好，移动服务提供商对移动用户的信任度 w 越高；p 表示移动用户与该交易票据的颁发者在先前的交易过程中的交易价格 *tr. AttrInfo. price*，交易金额的大小直接反映了历史交易的重要程度，交易金额越大，则移动服务提供商对移动用户的信任度 w 越高；同时考虑到时间衰减因素，用户如果长时间没有网络行为或者协商行为，则不能再完全根据用户之前的网络行为计算用户的信任度，此时需要降低用户的信任度，因此 d 表示交易票据上的交易日期和用户注册日期的差值，差值越小，表示交易时间距离当前时刻越远，*tr. AttrInfo. rating* 和 *tr. AttrInfo. price* 的可信度越小，w 也就越小。综合考虑交易票据 *tr* 的 *tr. AttrInfo. rating* 和 *tr. AttrInfo. price*，两种属性都应该被重视，因此将交易票据中交易评价和交易价格两种属性对信任度的权重各设置为 0.5。由此可知，当移动用户拥有多张交易票据可供选择时，移动用户应该选择 *tr. AttrInfo. date* 距离当前时刻最近且 *tr. AttrInfo. rating* 和 *tr. AttrInfo. price* 都最高的交易票据。

为了节省移动终端的计算资源，同时移动服务商在移动用户中具有一定的信任度，例如对于电信、移动这种信誉度比较高的移动服务商，用户可以选择部分或完全信任该服务商。因此移动双方协商结束后，仅移动服务提供商给移动用户颁发交易票据。

在证书交换阶段，为减少信任证有效性验证次数，提出验证权证，定义如下。

定义 4(验证权证，authentication ticket, at) *at* 定义为一个四元组(*ticket_info*, *sigalg*, *validity*, *sig*)，其中 *ticket_info* 存储信任证集合的哈希值、使用的哈希算法和 *at* 的颁发者；*sigalg* 显示 *at* 使用的签名算法；*validity* 表示验证权证的有效期；*sig* 表示该权证颁发者对 *ticket_info* 中各哈希值的连接进行的数字签名。

当移动服务提供商发送的信任证出现在验证权证时，移动用户由于信任验证权证的颁发者，就不需要对此信任证进行数字签名验证。因此，*at* 的颁发者必须是权威的协商者，所谓权威的协商者是指某个实体拥有某个范围内的成员的管理角色，并为其他移动服务商提供安全服务，例如大学、银行以及政府等。因为信任证的哈希值能够唯一识别该信任证，所以每个验证权证只包含信任证的哈希值，用这些哈希值识别已经通过认证的信任证，即使披露验证权证，也可以保证其中信任证内容的安全，同时不会增加密码算法那样过重的负担。

3.2 移动信任协商协议

基于交易票据的自动信任协商协议的整个协商过程分为 3 个阶段：寒暄阶段、信任序列生成阶段和信任证交换阶段。假设 Alice 和 Bob 分别为移动用户和移动服务提供商，协议的具体算法描述如下。

(1)寒暄阶段

当 Alice 向 Bob 提交某一资源的访问请求时，首先触发寒暄阶段，资源申请者 Alice 与资源拥有者 Bob 开始交互协商。

寒暄阶段的主要目的是协商参与者确定对方的信任度。移动服务提供商根据收到的交易票据 *tr*，利用式(1)计算移动用户的信任度，而移动用户根据移动服务提供商的信誉来评价其信任度。寒暄阶段具体算法如下。

算法 1 移动用户端算法描述 CalculateTrustDegree_Client(R, TR)

输入：移动用户对移动服务端的原始请求资源 R 和移动用户拥有的本地交易票据集合 TR

输出：移动服务端的信任度 std 和交易票据 tr

```
1. send R to the Server;//向服务端发送原始请求 R
  //客户端主观判断服务提供商的信任度 std
2. determine the Server's trust degree std;
3. receive a message m from Server;
4.   tr'=NULL;
5.   if(m is greeting message){
6.     Search_transactionReceipt(greeting message.ServerHash_issuer,greeting message. transaction_category);
7.   }
8.   send tr' to the Server;
9.   return std;
10.  End of CalculateTrustDegree_Client Search_transactionReceipt (greeting message. ServerHash_issuer,greeting message. transaction_category);
1. Minimum=199999;
2. ctd'=0;
3.   For each tr in TR{
     //利用服务端发送过来的哈希算法对交易票据的颁发者哈希
```

```
4.  Hash_issuer=tr. AttrInfo. issuerusing greeting message. hash_
    algorithm;//检查客户端拥有的交易票据的颁发者的哈希值和
    交易票据的种类与服务端发送过来的值是否相等
5. if(Hash_issuer==greetingmessage. ServerHash_issuer&&tr. At-
   trInfo. category==greetingmessage. transaction_category){
6.  calculate client trust degree ctd;
7.  if (ctd>ctd')
8.  tr'=tr;
9.        }
10.  }
11.  if (tr'!=NULL)
12.    return tr';
13.  return NULL
14.  End of Search_transactionReceipt
```

算法 2 移动服务端算法描述 CalculateTrustDegree_Server(*Server_trust_entity*,*hash_algorithm*)

输入:移动服务端信任的实体名单 Server_trust_entity 和哈希算法 hash_algorithm

输出:客户端的信任度 ctd

```
//服务端收到客户端的请求信息
1. receive a message m from Client
2.  if(m is a request for R)
3.  send the greeting message containing ServerHash_issuer and hash_
    algorithm about the list of Server_trust_entity and transaction_
    category to the client//将服务端信任的实体的哈希值和哈希算
    法以及此次交易的种类发送给客户端
4.  if(m is a tr)//如果服务端收到的是客户端的交易票据
5.    If(tr. AttrInfo. issuer∈Server_trust_entity&&tr. AttrInfo.
      category==greeting message. transaction_category)//检验客
      户端发送的交易票据的颁发者是否是可信实体,以及交易票
      据的种类与此次交易是否相同
6.    calculate the client's trust degree ctd;//服务端根据交易票据
      计算客户端的信任度
7.    return ctd;
8.  End of the CalculateTrustDegree_Server
```

(2)信任序列生成阶段

Bob 根据第一阶段计算出的 Alice 的信任度,动态确定访问控制策略,相关分析如下:

$$\begin{cases} s \leftarrow (c_1 \cap c_2 \cap c_3) \cup (c_4 \cap c_5 \cap c_6), & \text{if } w \in [0, w_1) \\ s \leftarrow (c_1 \cap c_2) \cup (c_4 \cap c_5), & \text{if } w \in [w_1, w_2) \\ s \leftarrow c_1 \cup c_4, & \text{if } w \in [w_2, 1) \end{cases}$$

s 是 Bob 的本地资源,c_1,c_2 是 Alice 的本地资源,w 表示 Bob 评估的 Alice 的信任度值。w_1 和 w_2 是移动服务商设定的信任度的中间阈值,可由移动服务商根据需要来设定。

当 $w \in [0, w_1)$ 时,Bob 对 Alice 的信任度最低,当且仅当 Alice 披露了 c_1,c_2 和 c_3 或者 c_4,c_5 和 c_6,Bob 才会披露资源 s;

当 $w \in [w_1, w_2)$ 时,Bob 对 Alice 的信任度居中,只要 Alice 披露了 c_1,c_2 或者 c_4,c_5,Bob 就会披露资源 s;

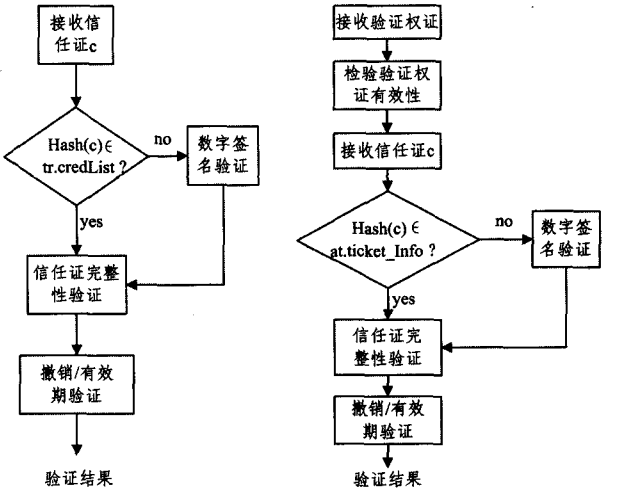
当 $w \in [w_2, 1)$ 时,Bob 对 Alice 的信任度最高,只要 Alice 披露了 c_1 或者 c_4,Bob 就会披露资源 s。

类似地,Alice 同样会根据自己对 Bob 的信任度评估动态地确定访问控制策略。当 Alice 向 Bob 请求某一资源 s 时,Bob 根据寒暄阶段计算的 Alice 的信任度,动态地确定资源的访问控制策略,假设 Alice 的信任度为 $w \in [w_1, w_2)$,Bob 会向 Alice 请求资源 c_1,c_2 或者 c_4,c_5,Alice 收到 Bob 对资源 c_1,c_2 或者 c_4,c_5 的请求后,同样会根据寒暄阶段计算的 Bob 的信任度确定资源 c_1,c_2 或者 c_4,c_5 的访问控制策略,然后 Alice 确定向 Bob 请求什么样的资源才能满足 c_1,c_2 或者 c_4,c_5 的访问控制策略,如此重复下去直至协商完成,最后生成信任证披露序列:$\{C_i\}_{i \in [0,2n+1]} = C_0, C_1, \cdots, C_{2n+1}$,其中,$n \in N$,$C_{2i} \in C_{Alice}$,$C_{2i+1} \in C_{Bob}$。

若在协商寒暄阶段 Alice 拒绝发送交易票据,Bob 无法获得有效的交易票据来计算出 Alice 的信任度,Bob 默认 Alice 的信任度 $w=0$。

(3)信任证交换阶段

在此阶段,协商双方根据生成的信任证披露序列逐步向对方披露信任证,从而完成协商。在披露信任证的过程中,如果信任证 $c \in C_{2i}$ 的哈希值出现在 tr 里,由于 Bob 信任 $tr.AttrInfo.issuer$,因此只需检查 c 的完整性、有效期和撤销状态,省略了对数字签名的验证。当 $c \in C_{2i+1}$ 的哈希值出现在 at 里,则 Bob 会在披露 c 的同时也披露 at。当 Alice 收到 at 时,首先利用 at 的公钥检验其合法性,如果合法,那么 Alice 同样只需检查 c 的完整性、有效期和撤销状态,省略了对数字签名的验证,如图 2 所示。



(a)移动服务端信任证交换阶段的工作原理　(b)移动客户端信任证交换阶段的工作原理

图 2

协商完成后,Bob 会根据 Alice 的协商行为签发此次交易的交易票据 tr'。

4 实验

4.1 实验环境

本实验在一台内存为 1GB、操作系统为 Android4.3 的华为手机 C8815 上进行。将提出的自动信任协商协议与传统的自动信任协商协议作比较,协商策略模块均采用基于有穷自动机的信任协商策略。

实验模拟了 15 个移动客户端分别与 100 个移动服务商进行自动信任协商,其中每个移动客户端拥有 15 个资源,每

个移动服务商拥有 40 个资源。协商双方的访问控制策略都是随机生成的。由于对任意的访问控制策略 $Policy$，其形式都可转化为 $c \leftarrow policy = D_1 \vee \cdots \vee D_m$，其中 $D_i = S_{i1} \wedge \cdots \wedge S_{in}$ 表示 $Policy$ 的一个子句，S_{ij} $(0<i<m, 0<j<n)$ 表示资源 c 的一个元策略。因此当 $m=3, n=3$ 时协商双方每个资源生成最复杂的访问控制策略，当 $m=3, n=2$ 时协商双方对应资源生成较复杂的访问控制策略，当 $m=3, n=1$ 时协商双方对应资源生成最简单的访问控制策略。传统的自动信任协议中由于不涉及信任度，因此协商双方都选择最复杂的访问控制策略来保护自己的敏感资源。而在基于交易票据的信任协商协议中，由于信任度的两个中间阈值 w_1, w_2 由移动服务商自己设定，在这里取三等分点，即 $w_1=1/3, w_2=2/3$。协商双方根据评估对方的信任度依次选择合适的访问控制策略保护自己的敏感资源。由于移动客户端对服务端的评估采取主观判断的方式，因此实验中假设客户端对前面 33 个移动服务端评估的信任度 $w \in (0, w_1)$，对第 34－66 个移动服务端评估的信任度 $w \in (w_1, w_2)$，对第 67－100 个移动服务端评估的信任度 $w \in (w_2, 1)$。而移动服务端对客户端的评估主要取决于客户端提供的交易票据 tr。实验假设每个移动服务端拥有 15 个信任的实体名单，且实体名单都是随机生成的。每个移动服务端拥有 2～6 个验证权证 at，每个 at 包含的信任证不少于 2 个。每次协商完成后移动服务商都会给移动用户颁发交易票据 tr。每次协商的交易评价取值在 0～1 之间，交易价格取值 0～1000，然后将其折算到 0～1。每分钟模拟 1 次协商，实验记录了在相同环境下两种协商策略各个阶段所消耗的计算开销。

4.2 实验结果

图 3 显示了当移动服务端对客户端评估的信任度不同时两种协商策略消耗的平均时间。由图 3 可知，传统的自动信任协商协议的协商时间不会随着信任度的提高而变化，因为每次协商中，双方的访问控制策略都是固定的，与信任度无关。而基于交易票据的自动信任协商协议随着信任度的提高，双方的访问控制策略都会变简单，协商时间和信任证交换所消耗的时间都会逐渐变短。

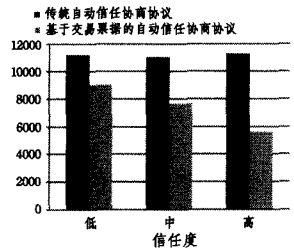
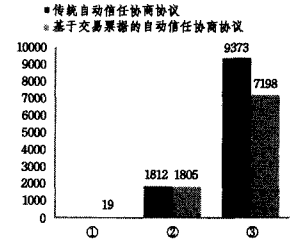
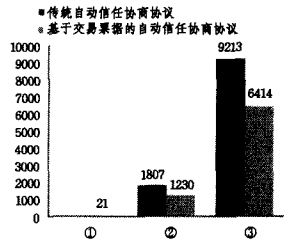


图 3　两种协商策略随信任度不同所消耗的时间对比

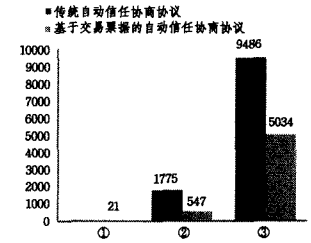
图 4 对比了不同信任度情况下两种协商协议在各个协商阶段的消耗时间。其中①、②、③分别代表寒暄阶段、信任序列生成阶段、信任证交换阶段。由图 4 可知两种策略的协商时间主要消耗于信任证交换阶段。在基于交易票据的自动信任协商协议中，由于寒暄阶段消耗的时间太少，因此基本可以忽略不计，当协商双方披露的信任证出现在交易票据和验证权证中时，由于此类信任证不需验证数字签名，只需检查信任证的完整性和有效期，因此传统的自动信任协商协议比基于交易票据的信任协商协议消耗的时间更多。随着信任度的提升，协商双方的访问控制策略逐渐变得简单，信任序列生成阶段生成的信任证会减少，同时考虑到当协商双方披露的信任证出现在交易票据和验证权证中时不需要验证数字签名，信任证交换阶段消耗的时间也会随着信任度的升高逐渐降低。



(a)信任度较低时，两种协商策略各个阶段的消耗时间对比



(b)信任度居中时，两种协商策略各个阶段的消耗时间对比



(c)信任度较高时，两种协商策略各个阶段消耗时间对比

图 4

图 5 显示了单个用户分别与 100 个移动服务端进行协商时信任度的增长趋势，其中每个值选取连续 10 次协商服务端对客户端评估的信任度的平均值。由图 5 可知，单个用户的信任度增长总体上呈线性增长趋势，随着协商次数的增多，服务端对客户端的信任度会较高。

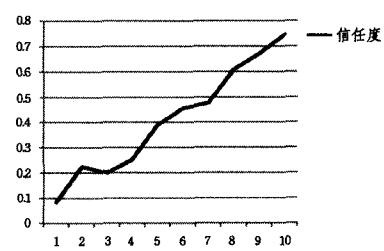


图 5　100 次协商中单个用户信任度上升趋势

结束语　针对移动商务环境下计算资源有限的特点，提出了基于交易票据的自动信任协商协议，通过利用信任度动态调整访问控制策略，同时运用交易票据和验证权证有效减少了验证信任证带来的巨大计算开销。实验表明，所提出的协议在一定程度上克服了现有信任协商方案的弊端，能极大提高信任协商的效率。

参 考 文 献

[1] Yuan Y F, Wang Y W, Xu Z C, et al. Mobile Commerce [M]. Beijing: Tsinghua University Press, 2006(in Chinese)
袁雨飞，王有为，胥正川，等. 移动商务[M]. 北京：清华大学出版社，2006

[2] Zhou T, Lu Y B, Zhang J L. A study on acceptance behavior of mobile commerce user based on perceived walue and trust [J]. Chinese Journal of Management, 2009, 6(10): 1407-1412(in Chinese)
周涛，鲁耀斌，张金隆. 基于感知价值的移动商务用户接受行为研究[J]. 管理学报，2009，6(10)：1407-1412

[3] Hu R B, Yang D L, Qi R H. Recommended trust evaluation model in mobile commerce based on combination evaluation model [J]. Operations Research and Management Science, 2010, 19(3): 85-93(in Chinese)
胡润波，杨德礼，祁瑞华. 移动商务中基于综合评价的推荐信任评估模型[J]. 运筹与管理，2010，19(3)：85-93

[4] Hoffman D L, Novak T P, Peralta M. Building consumer trust online [J]. Communications of the ACM, 1999, 42(4): 80-85

[5] Turban E. Electronic Commerce: A Managerial Perspective[M]. Beijing: Electronic Industry Press, 2002(in Chinese)
Turban E. 电子商务——管理新视角(第二版)[M]. 北京：电子工业出版社，2002

[6] Zhou T, Lu Y B. The impact of privacy concern on mobile commerce users' adoption behavior [J]. Chinese Journal of Management, 2010, 7(7): 1046-1051(in Chinese)
周涛，鲁耀斌. 隐私关注对移动商务用户采纳行为影响的实证分析[J]. 管理学报，2010，7(7)：1046-1051

[7] Lu Y B, Deng Z H, Zhang S T. The acceptance of mobile micropayment service: an empirical research based on trust-TAM [J]. China Journal of Information Systems, 2007, 1(1): 46-59(in Chinese)
鲁耀斌，邓朝华，章淑婷. 基于 Trust-TAM 的移动商务服务消费者采纳研究[J]. 信息系统学报，2007，1(1)：46-59

[8] Siau K, Shen Z. Building customer trust in mobile commerce[J]. Communications of the ACM, 2003, 46(4): 91-95

[9] Winsborough W H, Seamons K E, Jones V E. Automated trust negotiation [C]// Proceedings of 2000 DARPA Information Survivability Conference and Exposition. Hilton Head, USA, Jan. 2000: 88-102

[10] Li J X, Huai J P, Li X X. Research on automated trust negotiation [J]. Journal of Software, 2006, 17(1): 124-133(in Chinese)
李建欣，怀进鹏，李先贤. 自动信任协商研究[J]. 软件学报，2006，17(1)：124-133

[11] Liao Z S, Jin H, Li C S, et al. Automated trust negotiation in its development trend [J]. Journal of Software, 2006, 17(9): 1933-1948(in Chinese)
廖振松，金海，李赤松，等. 自动信任协商及其发展趋势[J]. 软件学报，2006，17(9)：1933-1948

[12] Deng C H, Lu Y B. Research on mobile commerce trust establishment framework based on VFT [J]. Science and Technology Management Research, 2008(3): 680-683(in Chinese)
邓朝华，鲁耀斌. 基于 VFT 的移动商务信任构建框架研究[J]. 科研管理研究，2008(3)：680-683

[13] Zhang Y, Chen H J, Jiang X H, et al. A survey of trust management for e-commerce systems [J]. Acta Electronica Sinica, 2008, 36(10): 2011-2020(in Chinese)
张宇，陈华钧，姜晓红，等. 电子商务系统信任管理研究综述[J]. 电子学报，2008，36(10)：2011-2020

[14] Winslett M, Lee A J, Perano K J. Trust negotiation: authorization for virtual organizations [C]// Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research. Knoxville, USA, 2009: 1-4

[15] Lin J B, Lu Y B, Zhang J L. An Empirical Study on Consumers' Trust of Mobile Stock Based on TAM Theory [J]. Journal of Management Science, 2009, 22(5): 61-71(in Chinese)
林家宝，鲁耀斌，张金隆. 基于 TAM 的移动证券消费者信任实证研究[J]. 管理科学，2009，22(5)：61-71

[16] Li J L, Deng X, Wang Y M. Security and efficiency negotiation model [J]. Computer Science, 2015, 42(6): 378-392(in Chinese)
李建利，邓潇，王艺谋. 一种高效安全的自动信任协商模型[J]. 计算机科学，2015，42(6)：378-392

[17] Bertino E, Ferrari E, Squicciarini A C. Trust-X: a peer to peer framework for trust negotiations [J]. IEEE Transaction on Knowledge and Data Engineering, 2004, 16(7): 827-842

[18] Squicciarini A, Bertino E, Ferrari E, et al. PP-Trust-X: a system for privacy preserving trust negotiations [J]. ACM Transactions on Information and System Security, 2007, 10(3): 1-48

[19] Lu H W, Liu B L. DFANS: A Highly Efficient Strategy for Automated Trust Negotiation[J]. Computers & Security, 2009, 28(7): 557-565

[20] Li N H, Du W L, Dan B. Oblivious Signature-Based Envelope [C]// Proceedings of the 22nd ACM Symposium on Principles of Distributed Computing (PODC 2003). New York: ACM Press, 2003: 182-189

[21] Li J X, Huai J P. COTN: A Contract-Based Trust Negotiation System [J]. Chinese Journal of Computers, 2006, 29(8): 1290-1299(in Chinese)
李建欣，怀进鹏. COTN：基于契约的信任协商系统[J]. 计算机学报，2006，29(8)：1290-1299

[22] Li J L, Liu B, Deng X. Finite Automaton Based Strategy for Automated Trust Negotiation [J]. Journal of Chinese Computer Systems, 2013, 34(6): 1000-1220(in Chinese)
李建利，刘博，邓潇. 基于有穷自动机的自动信任协商策略[J]. 小型微型计算机系统，2013，34(6)：1000-1220

[23] Wang Q Y, Jiang W B, Wang H. Scheme of Attribute-Based Disclosure Mobile Trust Negotiation [J]. Telecommunication Science, 2013(10): 103-107(in Chinese)
汪秋云，蒋文保，王鸿. 基于属性披露的移动信任协商方案[J]. 电信科学，2013(10)：103-107