普适计算环境下信任管理模型的研究

徐文拴 辛运帏 卢桂章 陈秋双
(南开大学信息技术科学学院 天津 300071)

摘 要 普适计算环境下,各种资源、设备、应用以及环境均是高度动态变化的,因此如何衡量实体间的信任关系成为了一个十分重要的问题。传统的安全和认证方法基于可信第三方,而在动态的普适计算环境下,可信第三方的设置是不现实的,也是不可行的。基于以上问题,提出了一个新的普适计算信任管理模型,该模型集成了信誉和风险分析机制,考虑了多种相关因素,可以有效建立和度量各实体间的信任关系。相关仿真结果证明,该模型是行之有效的。

关键词 普适计算,信任,信誉,风险分析,信任管理

Research on the Trust Management Model for Pervasive Computing

XU Wen-shuan XIN Yun-wei LU Gui-zhang CHEN Qiu-shuang
(College of Information Technical Science, Nankai University, Tianjin 300071, China)

Abstract In pervasive computing environment, various resources, devices and applications are frequently changeable. Therefore, how to measure the trust relationship between entities has become an important problem. Those traditional authentication and security solutions are mostly based on the third trusted party, however, it is infeasible to set the third trusted entities in dynamic pervasive computing environment. Based on the status quo, a novel trust management model was presented , several essential factors were considered. A reputation module and a risk analysis module were integrated in the model, by which it can establish and measure the trust relationship between various entities effectively. The simulation results prove that the model is feasible and effective. It is applicable in dynamic pervaisve computing environments.

Keywords Pervasive computing, Trust, Reputation, Risk analysis, Trust management

1 引言

当前,普适计算环境下信任建模机制的研究是普适计算领域中的一个研究热点,也是一个难点。普适计算环境下,各种资源、设备、应用以及环境均是高度动态变化的,通过普适计算信任模型的建立,可以在各动态变化的实体间建立相应的信任关系,从而可以根据不同的信任值确定不同的访问策略。

目前,关于普适计算信任模型的研究工作有很多[1,4-16],这些研究考虑了信任关系建立的一些相关因素,信任模型的建立主要依赖于历史交互经验、时间以及其它实体的直接推荐等。而另外一些比较重要的因素,如风险分析机制、多跳信任推荐等,却较少考虑。

2 相关工作

文献[4]提出的信任模型利用模糊数字来表示信任,利用模糊规则计算和模糊控制领域中的方法来制定信任措施。类似地,PTM[8]使用模糊逻辑来表达信任关系,使用一个数学和一个概率信任变化模型减小环境的不确定性。

R. He 等在文献[5-7]中提出了一种基于云理论对信任建模的方法,考虑了信任传播和信任聚合问题,并提出了相关的处理方法。

在文献[12]中,W. Yuan 等则提出了一个基于朴素贝叶斯分类器的信任模型,可以在不同的环境中动态做出决策。

以上模型均侧重于基于不同理论方法对信任机制进行建模。在特定的情况下,这些信任模型可能具有较好的效果。然而,由于模型中均未考虑信誉、风险分析机制等一些关键因素,因此是不全面的。

D. Xiu 等在文献[11]中提出的动态信任模型的信任策略包括访问控制及 PKI 技术、信任商议(trust negotiation)、信任委托(trust delegation)、基于信誉的信任、基于上下文和本体的信任以及安全的数据流和信息隐私等方面,但文中并未详细讨论如何实现这个模型。

文献[13]提出了一个基于信任的访问控制模型,基于时间和以往交互历史以及推荐关系进行信任计算,进而设置信任阈值来决定是否允许访问。文献[14]认为信任系统包括个

到稿日期:2008-03-20 本文受天津市应用基础研究计划(自然科学基金)项目(06YFJMJC00200),天津市科技发展计划项目(06YFGZGX05900)资助。

徐文拴 博士研究生,主要研究方向为普适计算、信息自动化,E-mail:xuws@robot.nankai.edu.cn;**辛运帏** 博士,教授,主要研究方向为普适计算、信息加密技术;**卢桂章** 教授,博士生导师,主要研究方向为信息自动化、智能机器人系统;**陈秋双** 教授,博士生导师,主要研究方向为供应链管理与物流系统优化、先进生产计划与调度理论、CIMS。

人交互经验和信誉系统，讨论了信誉系统可能存在的一些问题并提出了相关的解决方法，但文中并没有给出具体的实现方法。文献[15]基于信任值矢量提出了一个信任模型，信任值的计算考虑了信誉、时间、历史交互经验等因素。同样，这些模型也未考虑风险分析机制。

SSRD+[16]是对 SSRD 模型[1]（MARKS 中间件[3]中的资源发现模块 SAFE-RD[2]的一部分）的改进和扩展，增加了一个风险模型，但该模型中的风险评价机制是比较简单的。

在最近的研究中，文献[9]提出了一个基于信誉的信任模型，将信任关系分为直接信任和推荐信任，并提出了一种多跳推荐协议。文献[10]则重点讨论了信任模型的建立，尤其是推荐信任的计算方法，但并未给出具体的实现结果。

在本文中，我们提出了一种集成信任、信誉、风险分析和决策机制的信任管理模型，信任模块中考虑了时间和历史交互经验等相关因素，信誉模块中包含了多跳信任推荐机制，风险分析模块中集成了较为全面的风险度量策略。

3 一个新的普适计算信任管理模型

一个完整的信任管理模型应该包括信任模块、信誉模块、风险分析模块和决策模块。其中，信任模块完成实体间信任关系的建立和度量；信誉模块可以给出一个实体的信誉度量，用于信任关系的建立；如果实体间没有信任关系或者信任关系达不到信任阈值的要求，就要利用风险分析模块给出风险评估；决策模块包含于各个模块之中，用于做出最终的决策，是接受或是拒绝实体的访问请求。

3.1 信任模块(Trust Module)

信任模块用于度量实体间的信任关系。这里，将信任关系量化到一个信任值域：[−1,1]，其中−1 表示完全不信任(complete distrust)；0 表示没有信任关系(no trust)；1 表示完全信任(complete trust)。

实体间信任关系的度量需要考虑两个重要相关因素：时间和历史交互经验(Historical Interaction Experience)。

(1) 时间。一般来说，实体之间的信任关系随着时间的增长逐步衰减。

若以往的信任值为 DT_i，则有：

$$DT_{i+1}=\lambda^{\Delta t}\cdot DT_i \tag{1}$$

其中 $\lambda^{\Delta t}$ 表示时间因素。λ 是一个时间因素调整因子，$0<\lambda<1$，反映了信任值随时间变化的衰减程度，Δt 是两次交互的时间间隔。

(2) 历史交互经验。也就是实体间以前有过交互记录，具有直接信任值。历史交互经验因素(用 HI 表示)以下面公式[12]进行衡量：

$$HI=\frac{n_a-n_r}{n} \tag{2}$$

其中 n_r 是请求被访问实体拒绝的次数，n_a 是请求被接受的次数，n 是提出访问请求的实体提出的请求的总次数($n=n_a+n_r$)，$-1\leqslant HI\leqslant 1$。

每次实体间通信完毕，被访问的实体对提出访问请求的实体的信任值 DT_i 更新如式(3)。

其中 μ 是历史交互经验调节因子，$\mu\in[1,2]$，它决定了历史交互经验在信任值更新时的影响度。

$$DT_i=\begin{cases}DT_i\mu^{HI}, & DT_i>0 \text{ 且 } HI\geqslant 0\\ |DT_i|\mu^{HI}, & DT_i<0 \text{ 且 } HI\geqslant 0\\ -DT_i\mu^{|HI|}, & DT_i>0 \text{ 且 } HI<0\\ DT_i\mu^{|HI|}, & DT_i<0 \text{ 且 } HI<0\\ \mu^{HI}, & DT_i=0 \text{ 且 } HI\geqslant 0\\ -\mu^{|HI|}, & DT_i=0 \text{ 且 } HI<0\end{cases} \tag{3}$$

这里应该注意，如果 $DT_i>1$，则需要调整 DT_i 为 1，如果 $DT_i<-1$，调整 DT_i 为 −1，以保证 $DT_i\in[-1,1]$。此外，如果实体间是第一次交互，若被访问实体接受服务访问请求，则置提出访问请求的实体的信任值 $DT_i=1$；若拒绝访问请求，则置 $DT_i=-1$(在交互活动中，总认为第一印象是非常重要的)。

图 1 给出了集成以上两个因素的一条信任值变化曲线。

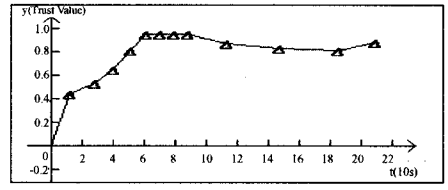


图 1 集成时间和历史经验因素的信任值变化曲线

3.2 信誉模块(Reputation Module)

如果实体间没有直接信任关系可以参考，或者直接信任关系达不到最低的信任阈值的要求，就需要借助于信誉模块，请求其它可信实体给出对提出访问请求的实体的信誉信息。这里的可信实体是指那些被访问实体信任的实体，也就是被访问实体对这些实体的信任值高于最低的信任阈值。

一个实体的信誉主要是来自其它实体对该实体的推荐(recommendations)。在信任模块中已经对实体的直接信任(直接信誉)有所考虑，所以在信誉模块中，只考虑来自其它实体的推荐，其中推荐者必须是可信的。

这样，一个实体对提出访问请求的实体的总的信任值的计算，就包括直接信任和推荐信任两个部分，如下式[9]所示：

$$T=\begin{cases}\rho DT+(1-\rho)RT, & DT\text{存在},RT\text{存在}\\ DT, & DT\text{存在},RT\text{不存在}\\ RT, & DT\text{不存在},RT\text{存在}\\ 0, & DT\text{和}RT\text{均不存在}\end{cases} \tag{4}$$

其中 T 表示总的信任值，DT 表示对提出访问请求的节点的直接信任值，RT 表示对提出访问请求的节点的推荐信任值，ρ 和 $(1-\rho)$ 分别表示直接信任和推荐信任所占的权重，$0.5\leqslant\rho<1$(总是认为直接信任占较大的权重)。推荐信任值 RT 的计算方法如下：

$$RT=\frac{\sum_{i=1}^{n}rec_i}{n} \tag{5}$$

其中，n 为可信推荐者的个数，rec_i 是第 i 个推荐信任值，其计算方法如下：

$$rec_i=\begin{cases}\rho\cdot DT(P,N)+(1-\rho)\cdot RT(N,Q), & RT(N,Q)\text{存在}\\ \text{null}, & RT(N,Q)\text{不存在}\end{cases} \tag{6}$$

其中 $RT(N,Q)$ 表示可信节点 N 对节点 Q(提出访问请求的实体)的推荐信任值。如果需要多跳计算才能获得推荐信任值，则 $RT(N,Q)$ 的计算方法同式(4)；$DT(P,N)$ 表示节点 P

(被访问实体)对可信节点 N(非节点 Q)的直接信任值,ρ 的含义与式(4)中的相同;*null* 表示没有任何推荐信息。

图 2 给出了一个普适计算环境中各个节点间的信任关系。节点 P 代表被访问实体,节点 Q 代表提出访问请求的实体,其中的推荐信任值可能是多跳(hops)计算才能获得的。有向线段上的数字表示一个实体对另外一个实体的信任值,这里使用有向线段是因为实体间的信任关系不是对称的。

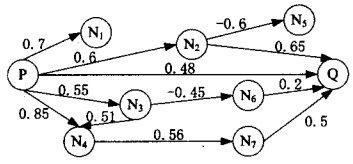


图 2 一个普适计算场景中各节点信任关系示意图

这里给出被访问实体(P)对提出访问请求的实体(Q)的信任值获取算法:

(1) 被访问实体查找历史访问记录;

(2) 获取所有可信实体;

(3) 如果可信实体 N 是目标节点 Q,则获取直接信任值;

(4) 如果可信实体 N 不是目标节点 Q 且跳数没有超过阈值,则向可信实体发出推荐请求并接收推荐信任值;

(5) 判断是否有推荐信息,利用式(5)和式(6)计算推荐信任值;

(6) 利用式(4)计算总体信任值。

推荐者接到推荐请求后给出的多跳推荐的处理算法与上面的算法基本相同,如下:

(1) 推荐者查找历史访问记录;

(2) 获取所有可信实体;

(3) 如果可信实体 N 是目标节点 Q,获取直接推荐信任值;

(4) 如果可信实体 N 不是目标节点 Q 且跳数没有超过阈值,则向可信实体发出推荐请求并接收间接推荐信任值;

(5) 判断是否有间接推荐信息,利用式(5)和式(6)计算间接推荐信息;

(6) 判断是否有直接或间接推荐信息。如果有,则利用式(4)计算总体推荐信任值,向请求方发送推荐信任值;否则,向请求方发送信息告知没有任何推荐信息。

3.3 风险分析模块

在某些情况下,实体之间没有信任关系或者信任值达不到预定的信任阈值要求,因此需要借助风险分析模块来决定是否允许实体的访问。在风险分析模块中,主要考虑两个因素:

(1) 提出访问请求的实体的风险度量。在该模块中,被访问实体对提出访问请求的实体的风险度量包括两个方面:直接风险度量和间接风险度量。

直接风险度量如下:

$$\omega_D=\frac{n_r}{n} \tag{7}$$

其中 n 是提出访问请求的实体的请求的总次数,n_r 是被访问实体拒绝的请求次数。当 $n=0$ 时,设定 $w_D=0.5$。

间接风险度量如下:

$$\omega_R=\frac{m_r}{m} \tag{8}$$

其中 m 是来自可信实体的推荐个数,m_r 是这些推荐中不好的推荐个数(不好的推荐是指来自可信实体的推荐信任值低于信任阈值)。当 $m=0$ 时,设定 $w_R=0.5$。

很明显可以看出,当 $0.5<w_D\leqslant 1$ 且 $0.5<w_D\leqslant 1$ 时,提出访问请求的实体的风险是非常高的。

(2) 被访问实体自身对于安全的考虑。在该模块中,用被访问实体的历史交互行为记录来度量,度量方法如下:

$$\theta=\frac{t_r}{t} \tag{9}$$

其中 t 是历史记录中所有实体对被访问实体提供的该服务的访问请求的个数,t_r 是其中被拒绝的请求的个数。当 $t=0$ 时,设定 $\theta=0.5$。

综合考虑以上两个因素,在决策模块中,如果 $\theta<\frac{1}{2}(\omega_D+\omega_R)$,则认为风险因素较高,拒绝实体的访问请求,否则接受该请求。

3.4 模型处理流程描述

该模型处理流程如图 3 所示,其中决策模块嵌入到各个模块之中。被访问实体首先计算对提出访问请求的实体的直接信任值。如果直接信任值大于预先设定的信任阈值 α,则接受该实体的访问请求;否则需要请求其它可信实体给出对该实体的推荐信任值,然后利用式(4)计算对该实体的总的信任值,再判断是否大于阈值 α。如果总的信任值大于阈值 α,则接受该实体的访问请求;否则需要利用式(7),式(8)和式(9)进行风险分析,以决定是否接受该实体的访问请求。

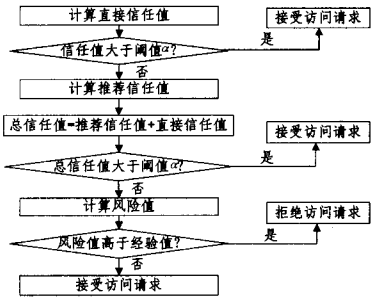


图 3 信任管理模型处理流程图

对该信任管理模型的分析如下。

优点:模型中集成了多跳信任推荐模块和风险分析模块,考虑了信任关系度量的多种相关因素,能够较好地满足普适计算环境下大规模陌生实体间的访问要求。

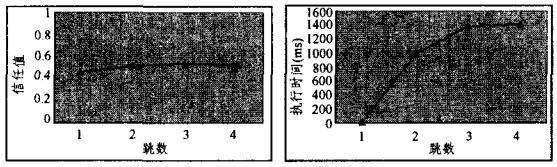
缺点:环境中的实体对每个提出访问请求的实体都要记录下其历史交互信息,如信任值、总的访问次数、拒绝访问次数等,因此可能会提高实体的存储开销。但是,考虑到实体间的信任关系随着时间衰减这一特点,如果实体间的交互历史超过某一时间阈值,则该记录可以不再保留。所以,总的来看,该模型不会对实体造成过高的存储开销。

4 模型实现及仿真结果

为了验证该信任管理模型的有效性,利用 Java 语言实现了该模型。仿真实验是在一个局域网中进行的,表 1 和图 4 分别给出了图 2 这种情况下不同跳数时的性能比较,其中参数值如下:$\alpha=0.5$,$\lambda=0.9$,$\mu=1.3$,$\rho=0.6$。

表 1　不同跳数情况下的性能比较

跳数	1	2	3	4
信任值	0.453	0.5153	0.532	0.523
执行时间	15ms	984ms	1391ms	1406ms
推荐个数	0	1	2	3
处理结果	Reject	Accept	Accept	Accept



(a) 信任值比较　(b) 执行时间比较

图 4　不同跳数情况下的性能比较曲线图

图 5 和图 6 分别给出了跳数为 1 和 2 时被访问实体对提出访问请求的实体的信任值变化曲线。图 6 中，黑色节点代表该请求被接受。需要指出的是，第五个请求的信任值(0.495)小于阈值 α(0.5)，而该请求仍被接受，这是因为决策模块判断风险值小于安全经验值($(\omega_D+\omega_R)/2=0.1$ 而 $\theta=0.11$)；随着时间的增长，信任值越来越小，这是因为来自推荐的信任值随着时间的增长而衰减(将来可以设置一个时间阈值规避这一失真的情况)。

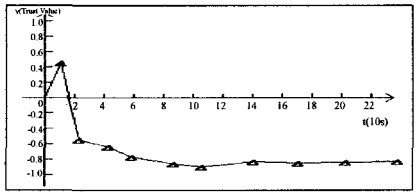


图 5　跳数为 1 时实体上的信任值变化曲线

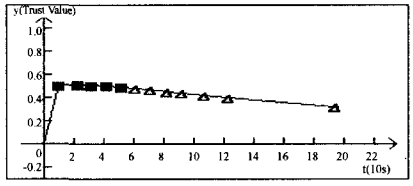


图 6　跳数为 2 时实体上的信任值变化曲线

从以上仿真结果可以看出，不同跳数的推荐信息可以使得实体间的信任关系得到不同程度的改善，但同时模型的执行时间会有所增长，因此在实际应用中应该根据不同的需要设置合理的跳数阈值。此外，模型中集成了风险分析机制，决策模块可以根据风险分析值决定是否接受实体的访问请求，这对于普适计算环境下的大量陌生实体间的交互是尤其适用的。为了更好地满足实际需要，还可以根据具体的要求调整不同的参数值的大小。比如，可以动态调整信任阈值 α 的大小以满足不同层次的安全需求。

结束语　本文提出了一个新的普适计算信任管理模型，该模型综合集成了信任、信誉和风险分析机制，考虑了影响信任值的多种相关因素。仿真试验结果证明该模型是有效的，可以很好地应用于动态变化的普适计算环境中。

此外，还应该注意到，在普适计算环境下，实体间的信任关系同上下文环境是紧密相关的，不同的上下文环境，实体间的信任值可能是不同的。因此，必须基于上下文考虑实体间的信任关系。本文提出的信任管理模型可以比较容易地扩展到不同的上下文环境的情况，只是实体间需要进一步区分不同的上下文环境下的信任关系，这是今后研究中需要进一步完成的工作。

参 考 文 献

[1] Sharmin M, Ahmed S, Ahamed S I. An adaptive lightweight trust reliant secure resource discovery for pervasive computing environments // Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06). Pisa, Italy, March 2006: 258-263

[2] Sharmin M, Ahmed S, Ahamed S I. SAFE-RD (Secure, Adaptive, Fault Tolerant, and Efficient Resource Discovery) in pervasive computing environments // Proceedings of the IEEE International Conference on Information Technology (ITCC 2005). Las Vegas, NV, USA, April 2005: 271-276

[3] Sharmin M, Ahmed S, Ahamed S I. MARKS (Middleware Adaptability for Resource Discovery, Knowledge Usability and Self-healing) for Mobile Devices of Pervasive Computing Environments // Proceedings of the 3rd International Conference on Information Technology: New Generations (ITNG 2006). Las Vegas, Nevada, USA, April 2006: 306-313

[4] Rehak M, Foltyn L, Pěchou çek M, et al. Trust model for open ubiquitous agent systems // Proceedings of the IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT). Washington, DC, USA, September 2005: 536-542

[5] He R, Niu J, Zhang G. CBTM: A trust model with uncertainty quantification and reasoning for pervasive computing // Pan Y, Chen D, Guo M, et al., eds. Proceedings of the Third International Symposium on Parallel and Distributed Processing and Applications (ISPA 2005). Nanjing, China, November 2005: 541-552

[6] He R, Niu J, Yuan M, et al. A novel cloud-based trust model for pervasive computing // Proceedings of the Fourth International Conference on Computer and Information Technology (CIT'04). Wuhan, China, September 2004: 693-700

[7] He R, Niu J, Hu K. A novel approach to evaluate trustworthiness and uncertainty of trust relationships in peer-to-peer computing // Proceedings of the Fifth International Conference on Computer and Information Technology (CIT'05). Shanghai, China, September 2005: 382-388

[8] Almenarez F, Marin A, Dyaz D, et al. Developing a model for trust management in pervasive devices // Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06). Pisa, Italy, March 2006: 267-271

[9] Haque M M, Ahamed S I. An omnipresent formal trust model (FTM) for pervasive computing environment // Proceedings of the 31st Annual International Computer Software and Applications Conference (COMPSAC 2007). Beijing, China, July 2007: 49-56

[10] 郭亚军，洪帆. 普适计算的信任计算模型. 计算机科学，2005，32(10)：59-62

[11] Xiu D, Liu Z. A dynamic trust model for pervasive computing environments // Proceedings of the Fourth Annual Security Conference. Las Vegas, NV, March 2005

(下转第 113 页)

(2)U_B 诚实，而 U_A 是不诚实的，没有遵守新协议。如果 U_A 想通过发送不正确的证明来欺骗 U_B，由于 VEDL[4] 的安全性，U_B 可以检测出这种欺骗。如果 U_A 在 Step3 发送了有效的消息，但在 Step5 拒绝把他的有效签名发送给 U_B，这时 U_B 可以要求所有的 STTP 去解决这次纠纷。若至少 t 个 STTP 返回了有效的 a_{1i}，根据 PVSS 的安全性，就可以恢复出真正的秘密 a_1，从而得到 U_A 的签名。这种情况也保证了协议的公平性。

(3)U_A 诚实，而 U_B 没有诚实的遵守协议。当在 Step4 中发送无效的签名 z_B' 给 U_A 时，U_A 可以检测出来并拒绝向 U_B 发送签名 z_A，以达到公平。另外，若 U_B 在 Step3 中收到 U_A 的消息后直接执行解决纠纷子协议，此时要求 U_B 向每个 $STTP_i$ 发送 b_{1i} 和 $E_{PK_{T_i}}(a_{1i})$，如果至少有 t 个 $STTP_i$ 诚实地验证了 b_{1i} 和 a_{1i}，并按照协议把它们分别发送给 U_A 和 U_B，则新协议仍能实现公平性。

分析表明：协议结束时，要么 U_A 和 U_B 都得到了对方对合同的签名，要么 U_A 和 U_B 都没有得到对方的签名，协议保证了双方的公平性。

4.2 保密性

在解决纠纷子协议中，由于每个 STTP 解密得到的只是部分签名的分享值，因此即使有 t 个以上的 STTP 是不诚实的，他们相互合作恢复出来的也只是对合同的部分签名，并不能由此而得出对合同的完整签名。因此在整个交易过程中，双方交换的签名对 STTP 始终是保密的。

4.3 抗合谋性

如果 U_B 想获得 U_A 的签名 z_A，但又不想向 U_A 泄露自己的签名，他可以通过与 STTP 合谋来实现这个目的。由 PVSS 可知，U_B 必须和至少 t 个 STTP 合谋才能得到 a_1 进而求出 z_A，但是 t 个以上的 STTP 与 U_B 同时合谋的概率是很小的。PVSS 增加了用户和 STTP 合谋的难度，因此该新协议从一定程度上来说是抗合谋的。为了保证新协议在可能发生合谋的情况下仍然具有公平性，要求 $\left\lfloor \frac{n}{2} \right\rfloor + 1 \leqslant t \leqslant$ 诚实 STTP 的个数。

4.4 签名的完全性

在协议结束的时候，U_A 收到 U_B 对合同的签名 (c, z_B)，U_B 也收到 U_A 的签名 (c, z_A)。如果两个签名都是有效的签名，U_A 和 U_B 可以分别计算对合同的一个完全签名 $(c, z = z_A + z_B \pmod p)$。最终 U_A 和 U_B 都得到了包含双方签名的合同，使得新协议具有传统纸质合同的特点，因此具有一定的实用性。

4.5 安全性

该协议所具有的各种性质基于 VEDL 的安全性、PVSS 的安全性和离散对数难解问题。VEDL 和 PVSS 的安全性阻止了 U_A 的各种恶意行为，而离散对数难解问题也阻止了 U_B 想对该协议进行的各种攻击。另外，本文方案的安全性还取决于 Schnorr 签名的安全性和 Hash 函数的安全性。离线的 (t,n) 门限半可信第三方的引入使得该协议具有更好的安全性和可依赖性。

结束语 该协议通过引入 n 个半可信第三方，实现了签名者隐私的保密，大大降低了合谋的可能性，还具有传统纸质合同的特点，因此具有一定的实用性。但同时也增加了协议的复杂性和通信量，应该根据实际情况来确定协议中 t 和 n 的个数。多方公平合同签署协议是今后将要进一步研究的问题。

参 考 文 献

[1] Asokan N, Shoup V, Wander M. Optimistic Fair Exchange of Digital Signatures // Advances in Cryptology. Proceedings of EUROCRYPT 98. LNCS1403. Berlin: Springer-Verlag, 1998: 591-606

[2] Franklin M K, Reiter M K. Fair Exchange with a Semi-trusted Third Party[C] // Proc. of 4th ACM Conf. on Computer and Communication Security. Zurich, ACM Press, 1997: 1-5

[3] 蒋晓宁，叶澄清，潘雪增. 基于半可信离线第三方的公平交易协议[J]. 计算机研究与发展，2001，38(4)：502-508

[4] Stadler M. Publicly Verifiable Secret Sharing[C]// Advances in Cryptology, EUROCRYPT'96. Berlin: Springer-Verlag, 1996: 190-199

[5] Wang C H, Yin C H. Practical Implementations of a Non-disclosure Fair Contract Signing Protocol. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2006, E89-A(1): 297-309

[6] Schnorr C P. Efficient Signature Generation for Smart Cards [J]. Journal of Cryptology, 1991, 4(3): 161-174

[7] Chaum D. Zero-knowledge Undeniable Signatures // Advances in Cryptology. Proc of EUROCRYPT'90. Lecture Notes in Computer Science(LNCS), 473. Springer-Verlag, 1998: 458-464

(上接第 106 页)

[12] Yuan W, Guan D, Lee S, et al. A dynamic trust model based on naive bayes classifier for ubiquitous environments // Proceedings of the 2006 International Conference on High Performance Computing and Communications (HPCC-06). Munich, Germany, September 2006: 562-571

[13] Giang P D, Hung L X, Lee S, et al. A flexible trust-based access control mechanism for security and privacy enhancement in ubiquitous systems // Proceedings of the International Conference on Multimedia and Ubiquitous. Seoul, Korea, April 2007: 698-703

[14] Yuan W, Guan D, Lee S, et al. Using reputation system in ubiquitous healthcare // Proceedings of the 9th IEEE International Conference on e-Health Networking, Application & Services (Healthcom 2007). Taipei, China, June 2007: 182-186

[15] Jameel H, Hung L X, Kalim U, et al. A trust model for ubiquitous systems based on vectors of trust values // Proceedings of the Seventh IEEE International Symposium on Multimedia (ISM'05). Irvine, California, USA, December 2005: 674-679

[16] Sharmin M, Ahamed S I, Ahmed S, et al. SSRD+: A privacy-aware trust and security model for resource discovery in pervasive computing environment // Proceedings of the 30th Annual International Computer Software and Applications Conference (COMPSAC 2006). Chicago, USA, September 2006: 67-70