P2P 网络中基于权重的动态信任模型 *

王涛春, 罗永龙, 左开中, 接　标
(安徽师范大学 数学计算机科学学院, 安徽 芜湖 241003)

摘　要: 针对现有模型存在的不足,借鉴人类对信任的评判习惯并参考交易涉及的主要因素,提出了 P2P 环境下一种基于权重的信任评价模型,在进行节点信任值评定时,着重考虑了交易权重对信任值变化的影响,并给出了信任值计算的方法和仿真实验。实验结果表明该信任评价模型能够准确地反映节点当前的信任度,特别对策略性欺骗和不诚实推荐具有很好的抑制作用。

关键词: 对等网络; 信任模型; 权重; 恶意行为
中图分类号: TP309　　**文献标志码**: A　　**文章编号**: 1001-3695(2011)01-0300-04
doi:10.3969/j.issn.1001-3695.2011.01.085

Dynamic trust model based on trade weight for P2P network

WANG Tao-chun, LUO Yong-long, ZUO Kai-zhong, JIE Biao
(*College of Mathematics & Computer Science*, *Anhui Normal University*, *Wuhu Anhui* 241003, *China*)

Abstract: Directing at the shortcomings of the existing model and drawing on the human habit of trust assessment and the main factors involved in transactions, this paper proposed a dynamic trust model based on trade weight for P2P network. While assessing the node trust value, the model put emphasis on the effect of trade weight on trust value, and specifically provided the method for trust value computing and the simulation. Results of the simulation show that the trust model can accurately reflect the current node trust value, and effectively resist the strategic deception and dishonest feedback.

Key words: peer-to-peer; trust model; trade weight; malicious behavior

Peer-to-peer(P2P)技术应用广泛,特别是 P2P 电子商务的快速发展,使得其在商业经济中发挥越来越重要的作用。但由于 P2P 系统中各个节点之间是平等的,它们既是消费者也是服务者,具有开放、动态、匿名和无中心等特点,使得在交易中出现大量的欺骗行为和低质量的服务[1],直接制约着电子商务的进一步发展。通过建立有效的信任评价模型,是降低交易风险和提高 P2P 系统整体可用性的有效解决方案。节点在每次交易前,都要对目标节点进行信任评价,评价结果低于某个阈值时拒绝交易,否则进行交易,并根据交易结果动态地修改目标节点的信任评价。

对目标节点的信任评价主要取决于直接信任评价和间接信任评价。也就是说,既可以依据与目标节点的交易记录来得出对目标节点的直接信任评价,又可以通过其他节点的推荐获得目标节点的间接信任评价。通过信任评价完成对目标节点信任量化和分级,已广泛应用于 P2P 系统中[2,3]。但现有的很多信任模型存在漏洞,受到节点的恶意攻击:a)恶意节点先进行多次的成功交易,提高其信任评价,然后利用其高信任评价进行欺骗交易,而当信任评价下降到一定程度时,再通过成功交易提高其信任评价,如此反复摇摆,不仅使其利益最大化,还能保持一定的信任评价[4]。b)不诚实的推荐。恶意节点通过协同作弊使其自身获得相当高的全局信任,欺骗其他节点来与其交易。因此,一个有效的 P2P 系统信任模型必须考虑这两方面的漏洞。本文根据 P2P 电子商务中利益这个最重要的因素,给出了 P2P 环境下一种基于权重的信任评价模型。该模型对上述两种恶意节点的攻击具有很好的抑制作用,使得信任评定是一个动态的过程,而不是简单的平均值处理。

1　相关工作

将目前存在的信任模型归纳起来可以分为依赖第三方和不依赖第三方两大类信任模型。依赖第三方的典型信任模型是基于 PKI 的信任模型[5],这类模型中存在一个或多个中心节点,这些中心节点负责整个网络的监督管理,同时中心节点可以颁发证书给可信的新节点作为其身份的凭证,并定期通告违规的节点。这些系统往往是中心依赖,存在扩展性差、容易产生单点失效等问题,也与 P2P 的分布式属性不相符合。

不依赖第三方的信任模型主要研究的是模拟人类社会信任建立方式的分布式信任模型,特别是 P2P 领域建立了很多分布式的基于信誉的信任模型。Aberer 等人[6]提出基于抱怨的信任评价机制,该模型中任一个节点可以随时抱怨其他节点,系统通过收集一个节点所有的抱怨信息来确定该节点的信誉,即一个节点收到的抱怨越多,越不值得信任。这种模型只是将节点评价进行简单综合,无法抑制恶意节点的诋毁行为。Li Xiong 等人[7]提出的一种基于信誉的 P2P 电子社区的信任

收稿日期: 2010-07-21; **修回日期**: 2010-09-19　**基金项目**: 国家自然科学基金资助项目(60703071);安徽省自然科学基金资助项目(070412043);安徽师范大学青年科学基金资助项目(2007xqn58)

作者简介:王涛春(1979-),男,安徽无为人,讲师,硕士,主要研究方向为安全多方计算、移动计算(taochunwang@gmail.com);罗永龙(1972-),男,安徽太湖人,教授,博士,主要研究方向为信息安全、可信计算、安全计算;左开中(1974-),男,安徽宿州人,副教授,博士,主要研究方向为可信计算、信息安全、三值光计算机;接标(1977-),男,安徽宿州人,讲师,硕士,主要研究方向为机器视觉与模式识别.

模型 PeerTrust。PeerTrust 的信任计算单纯地依赖其他节点的反馈,需要维护较大的社群,计算复杂度高,惩罚和激励效果不够理想。Beth 等人[8]提出的基于经验和概率统计的信任评价模型,对信任度的计算仅采用简单的平均值处理,不能有效抑制恶意节点的各种欺诈和攻击行为。Yao Wang 等人[9]提出的基于 Bayesian 的信任模型,主要是依据一定的参数,利用 Bayesian 概率的方法来计算可信度,具有片面性,没有考虑恶意节点。还有一些基于时间因子的信任模型[10,11],强调随着时间的推移以前的交易经验的权值也随着衰减,没有充分考虑交互满意度的趋势以及交互的上下文因素对信任值计算的影响,信任评价的合理性有待加强。

2　基于权重的动态信任模型

节点之间进行交易之前需要进行信任评价,信任评价可以通过直接信任 DT 和间接信任 RT 获得。直接信任是两个节点之间直接交易历史的经验获得,间接信任是通过其他节点的反馈信息获得。本文针对已有的信任评价模型的漏洞,同时,为了抑制恶意节点通过各种欺骗行为和狡猾策略以获得最大利益。提出了基于权重的动态信任模型。模型定义了影响信任值计算的主要因素,如交易的满意程度、交易的上下文因素、交易次数等,并从交易的反馈趋势和交易的上下文因素(如价格)两个最重要的因素着手,动态地调整权重集合实现信任计算,使信任计算更好地适应动态信任关系、简化了信任计算的过程、提高计算效率和信任评价的准确性。

2.1　直接信任计算

直接信任是节点 A 依据自身与节点 B 之间的交易记录,对目标节点 B 未来行为的主观期望,本文主要从交易的满意程度、交易的上下文、信任衰减、惩罚和激励等角度出发,探讨直接信任计算的方法,具体如下:

a)交易的满意程度。节点 A 与节点 B 进行交易后,根据 B 提供的服务质量或行为给出不同的评价,-1 表示负面评价,0 表示为中性评价,1 表示为正面评价。

定义 1　用 $FE_A^i(B)$ 表示节点 A 对节点 B 第 i 次交易的满意程度,即 $FE_A^i(B)=\{1,0,-1\}$,$DT_A^i(B)$ 表示节点 A 和节点 B 进行 i 次交易后的直接信任值,则第 N 次交易后其信任值为

$$DT_A^N(B)=\frac{\sum_{i=1}^{N}FE_A^i(B)}{N} \tag{1}$$

b)交易的上下文。信任评价仅仅靠交易的满意程度来决定是有很大缺陷的,如在电子商务中,一些狡猾的节点通过多次的小金额的成功交易来提高自己的信任度,然后进行一次大金额的欺骗交易,这样一直重复操作,信任度仍然很高,这显然是非常不合理的。

定义 2　节点 A 与 B 进行第 i 次交易,其交易权重(额)用 $WT_A^i(B)$ 表示,则第 N 次交易后其信任值变为

$$DT_A^N(B)=\frac{\sum_{i=1}^{N}FE_A^i(B)\times WT_A^i(B)}{\sum_{i=1}^{N}WT_A^i(B)} \tag{2}$$

从定义 2 可知,节点即使进行多次交易金额很小的交易,节点的信任度也不会有很大的提高。算法提高了信任度评价的合理性。

c)信任衰减。节点 B 的近期行为更能反映节点 B 的信任度,随着交易的进行,越早完成的交易在计算信任值时对其经验值和权重应该进行更多的折扣,同时,这样也给交易者机会纠正过去的欺骗行为或低质量的服务,鼓励其未来的诚实行为和提供高质量的服务。因此需要对先前的经验加入衰减因子。很多文献以时间作为衰减因子,但这种方式存在很大的漏洞,节点在进行大金额的欺骗行为之后可以长时间的停止交易,这样随着时间的推移以前的经验所占信任度的比重变得很低,因此笔者认为交易间隔次数作为衰减因子更能真实反映节点的信任度,杜绝上面所提的欺骗方式。

定义 3　节点 A 与 B 进行第 i 次交易,在计算之前第 $j(j<i)$ 次交易所产生的信任值和权重需进行一定的折扣,折扣率用 δ 表示,则第 N 次交易后其信任值变为

$$DT_A^N(B)=\frac{\sum_{i=1}^{N}FE_A^i(B)\times WT_A^i(B)\times\delta^{N-i}}{\sum_{i=1}^{N}WT_A^i(B)\times\delta^{N-i}} \tag{3}$$

其中:δ^{N-i} 表示第 $i(i<N)$ 次交易的折扣率。

从上面的计算式得出,在计算第 i 交易后的信任度时可以利用第 $i-1$ 次交易后信任值和权重总和值,而不必重复计算,用 $SWT_A^i(B)$ 表示节点 A 和 B 进行 i 次交易的权重总和,因此上面的计算式可优化为

$$DT_A^N(B)=\frac{DT_A^{N-1}(B)\times SWT_A^{N-1}(B)\times\delta+FE_A^N(B)\times WT_A^N(B)}{SWT_A^N(B)} \tag{4}$$

其中:$SWT_A^N(B)=SWT_A^{N-1}(B)\times\delta+WT_A^N(B)$。

证明 1　对式(4)进行如下推导。

其分子为

$$\begin{aligned}&DT_A^{N-1}(B)\times SWT_A^{N-1}(B)\times\delta+FE_A^N(B)\times WT_A^N(B)=\\&\frac{DT_A^{N-2}(B)\times SWT_A^{N-2}(B)\times\delta+FE_A^{N-1}(B)\times WT_A^{N-1}(B)}{SWT_A^{N-1}(B)}\times\\&SWT_A^{N-1}(B)\times\delta+FE_A^N(B)\times WT_A^N(B)=\\&(DT_A^{N-2}(B)\times SWT_A^{N-2}(B)\times\delta+FE_A^{N-1}(B)\times WT_A^{N-1}(B))\times\\&\delta+FE_A^N(B)\times WT_A^N(B)=DT_A^{N-2}(B)\times SWT_A^{N-2}(B)\times\delta^2+\\&FE_A^{N-1}(B)\times WT_A^{N-1}(B)\times\delta+FE_A^N(B)\times WT_A^N(B)\cdots=\\&FE_A^1(B)\times WT_A^1(B)\times\delta^{N-1}+FE_A^2(B)\times WT_A^2(B)\times\delta^{N-2}+\\&\cdots+FE_A^N(B)\times WT_A^N(B)=\sum_{i=1}^{N}FE_A^i(B)\times WT_A^i(B)\times\delta^{N-i}\end{aligned}$$

分母为

$$\begin{aligned}&SWT_A^N(B)=SWT_A^{N-1}(B)\times\delta+WT_A^N(B)=\\&(SWT_A^{N-2}(B)\times\delta+WT_A^{N-1}(B))\times\delta+WT_A^N(B)=\\&SWT_A^{N-2}(B)\times\delta^2+WT_A^{N-1}(B)\times\delta+WT_A^N(B)\cdots=\\&WT_A^1(B)\times\delta^{N-1}+WT_A^2(B)\times\delta^{N-2}+\cdots+WT_A^N(B)=\\&\sum_{i=1}^{N}WT_A^i(B)\times\delta^{N-i}\end{aligned}$$

因此可得,式(3)与(4)等价。

这种用固定的折扣率系数 δ 也存在明显的漏洞,即节点在进行大金额的欺骗行为之后,快速进行多笔金额较小的正面交易,可以达到相同的目的。因此不能使用固定的折扣率,而是把折扣率与当前交易的权重(交易额)联系起来,用 δ_i 表示计算第 i 次交易的折扣率。其中 $\delta_i=\frac{SWT_A^{i-1}(B)}{SWT_A^{i-1}(B)+WT_A^i(B)}$,当 $i=1$ 时折扣率为 1。

定义 4　节点 A 与节点 B 进行第 i 次交易,在计算之前第 $j(j<i)$ 次交易所产生的信任值和权重需进行一定的折扣,折扣率用 δ 表示,则第 N 次交易后其信任值变为

$$DT_A^N(B)=\frac{DT_A^{N-1}(B)\times SWT_A^{N-1}(B)\times\delta_N+FE_A^N(B)\times WT_A^N(B)}{SWT_A^N(B)} \tag{5}$$

其中：$\delta_N = \frac{SWT_A^{N-1}(B)}{SWT_A^{N-1}(B) + WT_A^N(B)}$，$SWT_A^N(B) = SWT_A^{N-1}(B) \times \delta + WT_A^N(B)$。

d)惩罚和激励。人类社会的信任总是缓慢增加、快速减少的，也就是说需要通过许多次成功的交互才能建立的信任在几个失败的交互发生之后就会丧失。所以在计算信任值时引入自适应的信任因子，使得信任值的计算具有缓慢上升快速下降的特点，这更符合人类社会的信任行为。

定义 5　更新信任值时，不仅需要考虑当前第 N 次交易的结果和权重，还需要考虑当前的惩罚激励函数 $PI_A^N(B)$，则节点 A 与 B 进行第 N 次交易后其信任值变为

$$DT_A^N(B) = \frac{DT_A^{N-1}(B) \times SWT_A^{N-1}(B) \times \delta_N + FE_A^N(B) \times WT_A^N(B) \times PI_A^N(B)}{SWT_A^N(B)} \tag{6}$$

其中：$PI_A^N(B) = \begin{cases} PIF_A^N(B), FE_A^N(B) = 1 \text{ 或 } 0 \\ 1, FE_A^N(B) = -1 \end{cases}$　$PIF_A^N(B) \in [0,1]$

$$PIF_A^N(B) = \begin{cases} 1, PIF_A^{N-1}(B) \geqslant 1 - \Delta\phi \text{ 且 } FE_A^{N-1}(B) = 1 \\ PIF_A^{N-1}(B) + \Delta\phi, PIF_A^{N-1}(B) < 1 - \Delta\phi \text{ 且 } FE_A^{N-1}(B) = 1 \\ PIF_A^{N-1}(B), FE_A^{N-1}(B) = 0 \\ PIF_A^{N-1}(B) - \Delta\varphi, PIF_A^{N-1}(B) \geqslant \Delta\varphi \text{ 且 } FE_A^{N-1}(B) = -1 \\ 0, PIF_A^{N-1}(B) < \Delta\varphi \text{ 且 } FE_A^{N-1}(B) = -1 \end{cases}$$

$PIF_A^N(B)$ 为惩罚激励因子，$\Delta\phi$ 为交易成功事务激励参数，$\Delta\varphi$ 为失败事务惩罚参数，为了满足信任慢增快少，笔者取值 $\Delta\phi < \Delta\varphi$，达到了惩罚的效果，更符合人类社会的信任习惯。

2.2　间接信任值的计算

当一个节点与另一个节点没有直接信任时，必须依赖一个或多个第三方节点推荐形成的间接信任来评定目标节点的信任度。节点 A 要与 B 进行交易之前，需要计算与节点 B 的间接信任，节点 A 会向与自己有信任关系的节点广播信任查询消息，再对反馈的信息进行合成得到节点 A 对 B 的间接信任。人类的习惯是对不同的人推荐的可信度是不一样的，即越信任的节点推荐的信息越可靠。

定义 6　节点 A 接收到这些反馈信息后，对这些信息进行合成，得到对节点 B 的间接信任，具体为

$$RT_A(B) = \frac{\sum_{C \in Dset(A)} T_A(C) \times DT_C(B) \times SWT_C(B)}{\sum_{C \in Dset(A)} T_A(C) \times SWT_C(B)} \tag{7}$$

其中：$C \in Dset(A)$ 为所有与节点 A 有信任关系的集合，$T_A(C)$ 为节点 A 对推荐节点的信任值，在间接信任计算中，与节点 A 信任值越大的节点推荐的权重也越大，可以有效减少合伙欺骗节点提供的虚假反馈信息。同时，考虑推荐节点与目标节点的交易总额，保证其推荐的信息更可靠。

2.3　全局信任值的计算

信任是关于某一节点的信任，包括一个节点对另一个节点的直接信任和从其他节点获得的推荐信任。通过信任计算，节点 A 得到对节点 B 的直接信任值和间接信任值后，再对这两个信任值进行合成，得到全局信任值。不失一般性直接信任和间接信任的权重分别为 α 和 β，则 $\alpha + \beta = 1$。

定义 7　节点 A 通过计算和反馈信息，获得对节点 B 的直接信任值和间接信任值，通过合成计算出对节点 B 的全局信任值，具体为

$$T_A(B) = \alpha \times DT_A(B) + (1 - \alpha) \times RT_A(B) \tag{8}$$

$$\alpha = 1 - \frac{DW}{SWT_A(B)}$$

其中：α 为直接信任的权值，α 的取值与交易的次数和总额有关，交易的次数越多、总额越大则 α 的取值越大，如果 $SWT_A(B) = 0$，则 $\alpha = 0$，$0 \leqslant \alpha \leqslant 1$，$DW$ 为设定的交易额的门槛值。

从上面公式可以看出，当节点的交易额很小时主要为信息推荐交易，随着交易额的增加，直接信任的权值也在增加，即节点越来越相信自己的判断，更符合人类社会交互的事实。

3　仿真实验

笔者通过模拟实验考察信任评价模型对摇摆节点和协同作弊节点的抑制能力。模拟恶意节点通过一段时间的合作交互获得一定的信任评价后，采用一次大额度的欺骗交易，再进行多次小额度的成功交易并作周期性的摇摆。本文设置成功交互激励为 0.008，失败交易惩罚为 0.02，在交易额的基础上其衰减率为 0.95，实验仿真是基于 VC ++ 实现，模拟结果如图 1 所示。从图 1 可以看出：与现有模型比较，本文的模型对摇摆节点的行为更加敏感，惩罚力度更大，更加看重摇摆行为过程中否定的交互经验以及交易额，使得当节点进行额度较大的欺骗交易时，其信任值迅速下降，并通过惩罚机制，使其恢复到原来水平的速度比下降的速度慢得多，而且随着节点行为的不断摇摆，信任值呈下降趋势，更符合人的交互习惯。

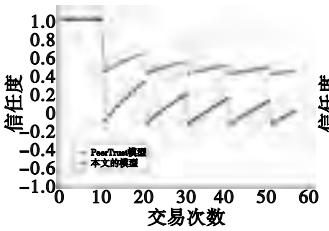

图1　策略性欺骗行为节点信任值变化

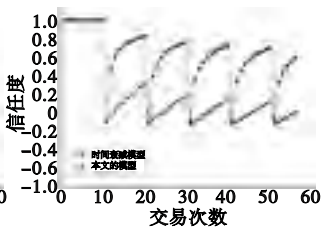

图2　衰减因子策略性欺骗行为节点信任值变化

衰减因子是反映过往交易经验在计算信任值时的所占权值的变化，很多信任评价模型的衰减因子是以时间为单位的，狡猾的恶意节点可以针对这个特点进行另类的摇摆行为，即欺骗交易后先间隔较长时间再进行多次间隔时间短的成功交易，弱化欺骗行为所带来的影响，快速提高信任值，不符合实际交易特点，同时，以时间作为衰减因子，则在每次计算信任值时都要重新计算以前每次交易的经验值，随着交易的进行，计算量会迅速膨胀，影响计算效率。从图 2 可以看出，基于时间衰减的信任模型虽然在进行欺骗行为后其信任值快速下降，但通过时间策略信任值也可以快速得到提高，而基于权重的信任模型比基于时间衰减的信任模型对这类狡猾节点有更好的抑制作用。

协同作弊行为是恶意节点典型的攻击手段，本文模型不仅考虑推荐值还考虑推荐节点本身的可信度和交易总额，这样可以有效地抑制不诚实推荐。而且随着节点本身与目标节点交易次数的增加，直接信任在全局信任合成时的比重会越来越大，降低因为协同作弊而影响信任计算的准确性。为了模拟本文模型的实验结果，不失一般性把所有节点分为四类，分别为：a)诚实节点(HE)；b)正常节点(NR)；c)恶意节点(CH)；d)狡猾的恶意节点(SC)。根据交易结果给出评价级别，分别为：−1 表示负面评价，0 表示为中性评价，1 表示为正面评价。同时给出每种节点交易结果的概率，进行欺骗交易时的交易额(用 Tvalue 表示，成功交易时的交易额默认为 1)和诚实反馈(Hback 表示)的概率。具体值如表 1 所示。

表 1　四类节点的参数分布

	HE	*NR*	*CH*	*SC*
−1	5%	10%	70%	10%
0	10%	60%	20%	10%
+1	85%	30%	10%	80%
*T*value	1	1	1	8
*H*back	100%	90%	10%	0%

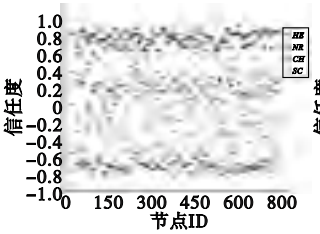

图3　50 000轮交易后四类节点信任值分布

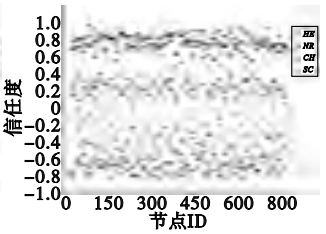

图4　200 000轮交易后四类节点信任值分布

设置每类节点的个数为 200,随机对这 800 个节点进行交易,其交易的参数如表 1 所示,图 3 和 4 分别为进行 50 000 轮和 200 000 轮交易后各节点的信任值。通过图 3 和 4 可知该信任评价模型对诚实节点、一般节点和恶意节点都有良好准确的评价结果,由于信任模型会随着直接交易次数和额度的增加,信任评价会越来越依靠直接交易的结果,对比图 3 和 4 第四类狡猾恶意节点的信任评价结果可得出,随着交易的不断进行,狡猾的恶意节点即使互相提供虚假推荐,其信任值也在不断地降低。由此通过上面的实验可以看出,基于权重的动态信任模型对摇摆节点和提供虚假推荐的狡猾恶意节点具有很好的抑制作用。

4　结束语

本文提出了 P2P 环境下一种基于权重的信任评价模型,着重考虑了交易额对信任值的影响,通过分析简化运算式,降低了计算的复杂性。仿真实验表明该模型对策略性欺骗和不诚实推荐具有很好的抑制作用。下一步的研究工作是进一步完善本文的 P2P 信任评价模型,包括:引入更有效的惩罚和激励机制;更符合人类社会习惯的信任衰减规律;更有效、准确地合成直接信任和间接信任等。

参考文献:

[1] ADARAND E, HUBERMAN B. Free riding on Gnutella, CSL-00-3 [R]. Palo Alto: Xerox PARC, 2000.

[2] RESNICK P, ZECKHAUSER R. Trust among strangers in Internet transactions : Empirical analysis of eBay's reputation system[C]// Proc of Electronics of Internet and e-Commerce. 2002:127-157.

[3] RINDOVA V P, KOTHA S. Building reputation on the Internet: Lessons from amazon. com and its competitors[R]. [S. l.]:University of Was-hington Business School,2001.

[4] MANCHALA D W. E-commerce trust metrics and models[J]. Internet Computing,2000,4(2):36-44.

[5] ALTMAN J. PKI Security for JXTA overlay networks, TR-I2-03-06 [R]. Palo Alto: Sun Microsystem, 2003.

[6] ABERER K, DESPOTOVIC Z. Managing trust in a peer-to-peer information system[C]//Proc of the 10th International Conference on Information and Knowledge Management. New York: ACM Press, 2001:310-317.

[7] LI Xiong, LIU L. PeerTrust: Supporting reputation-based trust in peer-to-peer communities[J]. IEEE Trans on Data and Knowledge Engineering: Special Issue on Peer-to-Peer Based Data Management, 2004,16(7):843-857.

[8] BETH T, BORCHERDING M, KLEIN B. Valuation of trust in open network[C]//Proc of European Symposium on Research in Security. 1994.

[9] WANG Y, VASSILEVA J. Bayesian network trust model in peer-to-peer networks[C]//Proc of the 2nd Int'l Workshop on Agents and Peer-to-Peer Computing. Berlin: Springer-Verlag, 2004:23-34.

[10] 常俊胜,王怀民,尹刚. DyTrust:一种 P2P 系统中基于时间帧的动态信任模型[J]. 计算机学报,2006,8(29):1301-1307.

[11] HUANG C L, HU H P, WANG Z Y. Modeling time-related trust [C]//Proc of the 3rd International Conference on Grid and Cooperative Computing. Wuhan:[s. n.],2004:382-389.

(上接第 299 页)

4.3　指定验证性

具有指定验证者的签名方案的安全性还应包括指定验证性,即只有签名者指定的验证者可以验证签名的有效性,除签名者之外的任何其他第三方在无法获得验证者私钥的情况下都不能验证签名的有效性。

在上述方案的验证阶段,当指定验证者 Bob 收到消息 M 的签名(S,h,M)后,首先需要计算

$$R' = e(S,P)e(H_1(x_B P_A \| M)$$

然后才能够验证消息 M 的签名(S,h,M)的有效性,而计算 R' 的过程中用到了指定验证者 Bob 的私钥 x_B。也就是说在没有指定验证者 Bob 的私钥 x_B 的前提下,任何人都不能够验证消息 M 的签名(S,h,M)的有效性。因此方案满足指定验证者的性质。

4.4　随机性

通过引入随机数,使得对同一消息产生相同签名的概率为 $1/q$(q 为大素数,且 $q \geq 2^k$),从而避免了消息的重放。

5　结束语

鉴于具有指定验证者的数字签名具有广泛的实际应用价值,自从其概念被提出以来就一直为众多研究学者们所青睐。本文在研究了司光东等人的方案后,发现他们的方案存在一个共同的缺陷——易于遭受重放攻击。本文在文献[4]的基础上新构造了一个高效的具有指定验证者的签名方案。虽然不具备原方案签名长度短的优势,但消息的签名长度与 ECDSA 签名长度相当,仍然具有高效的特点。相比于原方案,新构造的方案避免了消息的重放而且适用于更广泛的网络环境。同时,在随机预言机模型下和 CDH 问题困难假设下证明了本文的方案是安全的。

参考文献:

[1] JAKOBSSON M, SAKO R. IMPAGLIAZZO R, Designatured verifier proofs and their applications[C]//Proc of Advances in Eurocrypt. LNCS, 1070. [S. l.] Springer-Verlag,1996:143-154.

[2] SAEEDNIA M, KRAMER S, MARKOVITCH O. An efficient strong designated verifier scheme[C]//Proc of ICISC. [S. l.]: Springer-Verlag,2003:40-54.

[3] BONEH D, LYNN B, SHACHAM H. Short signatures from the weil pairings[C]//Proc of Advances in Cryptology-Asiacrypt'01, LNCS, 2248. [S. l.]:Springer-Verlag. 2001:514-532.

[4] HUANG X, SUSILO W, MU Y, *et al*. Short designated verifier signature scheme and its identity-based variant[J]. International Journal of Network Security,2008,6(1):82-93.

[5] 司光东, 辛向军, 陈原,等. 具有指定验证者的短签名方案[J]. 电子学报,2008,36(1):24-27.

[6] 贺雯, 张建中. 高效的具有指定验证者的代理签名方案[J]. 计算机应用研究,2009,26(10):3901-3902.