文章编号:1001 - 9081(2009)10 - 2606 - 05

P2P 环境下去中心化的多方公平交换协议

何 频,陈 明,吴开贵
(重庆大学 计算机学院,重庆 400030)
(hepin@ cqu. edu. cn)

摘 要:针对 P2P 环境下有价数字资源的多方交换存在资源认证和交换对象协商等问题,提出一种去中心化的多方公平交换协议。协议采用交叉验证理论进行资源的认证和验证,采用交换意向的单向发布机制和新型单向网状交换结构,较好地解决了多方交换对象协商问题,实现了交易拓扑的保密性。最后证明了在交叉验证理论可证明正确的前提下,协议具有公平性。

关键词:对等网络;多方公平交换;离线半可信第三方;交叉验证
中图分类号: TP393 **文献标志码**:A

Decentralized fair multi-party exchange protocol under P2P environment

HE Pin, CHEN Ming, WU Kai-gui
(*College of Computer, Chongqing University, Chongqing* 400030, *China*)

Abstract: The multi-party exchange of valuable digital resources in P2P environment has some problem on resources certification and objects exchange. A decentralized fair multi-party exchange protocol was proposed. The protocol adopted cross-validation theory to identify recourses and solved the problem of the negotiation among multi-party exchanges in term of one-way release mechanism and the new one-way exchange mesh structure. Meanwhile, the protocol certificated its own fairness on the basis of right cross validation.

Key words: Peer-to-Peer (P2P); multi-party fair exchange; off-line semi-trusted third party; cross validation

0 引言

多方公平交换协议的研究起源于 N. Asokan 等人的工作[1],他们将先前的两方公平交换协议[2]扩展到了多方情形,并在此工作[2]中提出了离线第三方的概念,使用离线第三方的公平交换协议被称为乐观公平交换协议(Optimistic Protocols for Fair Exchanges,OPFE)。随后,国内外学者对多方公平交换进行了大量研究,主要集中在两个方面:一方面是单对多交换协议[3-6],即一个主体同时与多个主体进行公平交易;另一方面是多对多交换协议[1,7-11],即多个主体间以一种公平的方式进行交易。多对多交换协议主要有环型和网型两种实现方式:环型协议往往存在效率和公平性方面的缺陷[12-13],网型交易要求每个参与实体至少发出和收到一个电子商品。

在 P2P 环境下,实现有价资源的公平交换渐渐成为该领域的研究热点之一[6,14-17]。文献[14-15]作者提出了在 P2P 网络中支持电子商务的解决方案,该方案引入银行节点层和银行服务协议来解决有价资源的支付问题,实现了两方情形下数字资源的买卖。文献[6]作者提出了一种适用于 P2P 环境的一对多组合乐观公平交换协议,此种协议的特点在于多方行为的相互关联,其中一方的行为失误将会造成整个交换的失败,因此,当网络不稳定或者网络中存在恶意实体时,该协议实施较困难。文献[16-17]作者提出由交换双方随机选择 n 个 peer 节点合成分布式可信第三方来代替专用可信第三方的思想,并利用门限秘密共享来防止第三方节点的合谋。该方法提供了一种在 P2P 环境下难于实施专用可信第三方问题的解决方案,可是文献[17]作者要求分布式 TTP 中至少存在 m 个有效节点(通常 $m > 2n/3$),即假设 m 个诚实节点的消息能可靠传输,这个假设在恶意节点的主动攻击下显得较为脆弱,且实施较为复杂,难以扩展到多方交换情形。另外,这些工作都较少涉及有价资源的认证、交换对象和交换条件的协商等问题。

本文提出一种在 P2P 环境下去中心化的多对多型乐观公平交换协议,很好地解决了在 P2P 网络中节点间有价数字资源交换的问题。协议采用交叉验证理论[18]进行有价资源的认证和验证,采用离线半可信第三方[8]进行争端解决,交易拓扑则借鉴了环型协议的思想采用新型单向网状结构,使得交易结构清晰且易于实施。协议分为四个阶段,较好地解决了资源验证、交换对象协商和自动争端解决等问题,具有公平性、STTP 行为可验证性和交易拓扑保密性等性质。另外,我们还讨论了多方交换协议应满足的多方公平性概念。

1 交叉验证理论

文献[18]作者提出的交叉验证理论主要用于在交换双方互不信任的环境下,防止交换中的一方提供虚假的数字资源,即提供数字资源的交叉验证。其原理描述如下。

定义 1 m 是小于一个大整数 N 的非负整数,M 是 m 的集合,即有 $M = \{m \mid 0 \leqslant m < N\}$。

定义 2 给定一个整数 a 和一个正整数 N,式(1)成立:

$$a = qN + r \tag{1}$$

这里,$0 \leqslant r < N$,且 $q = \lfloor a/N \rfloor$。$\lfloor x \rfloor$ 表示取小于 x 的最大整数。

收稿日期:2009 - 04 - 16;**修回日期**:2009 - 06 - 18。 **基金项目**:国家自然科学基金资助项目(90818028)。

作者简介:何频(1962 -),男,重庆人,副教授,主要研究方向:计算机软件; 陈明(1978 -),男,重庆人,博士研究生,主要研究方向:形式化分析技术; 吴开贵(1966 -),男,重庆人,副教授,博士,主要研究方向:信息安全。

定义 3　对于正整数 a、b 和 N,如果 $a \bmod N = b \bmod N$,那么记为 $a \equiv b \bmod N$。

定义 4　如果正整数 a 和 b 仅有一个公因数 1,即 $\gcd(a, b) = 1$,那么 a 和 b 互素。

定义 5　对于正整数 a、x 和 n,且 $n > 1$,如果 $\gcd(a, n) = 1$ 且 $a \cdot x = 1 \bmod n$,那么 x 被看作 $a \bmod n$ 的乘法逆元。

定义 6　对于整数集 $\{n_1, n_2, \cdots, n_k\}$,如果有 $\gcd(n_i, n_j) = 1$ 且 $(i \neq j)$,那么 $\{n_1, n_2, \cdots, n_k\}$ 被称为两两互素。

定义 7　欧拉函数 $\varphi(N)$ 定义为少于或等于 N 的数中与 N 互素的数的数目。

欧拉函数具有如下性质:

1) 如果 N 是素数,那么 $\varphi(N) = N - 1$;

2) 如果 $N = N_1 N_2 \cdots N_k$,且 $n_1, n_2, \cdots, n_k$ 两两互素,那么 $\varphi(N) = \varphi(N_1)\varphi(N_2)\cdots\varphi(N_k)$。

定理 1　欧拉定理表明对于每一对互素的数 a 和 N,式(2)成立:

$$a^{\varphi(N)} \equiv 1 \bmod N \tag{2}$$

推论 1　如果 $0 < m < N$,$N = N_1 N_2 \cdots N_k$ 且 $n_1, n_2, \cdots, n_k$ 是素数,那么 $m^{x\varphi(N)+1} \equiv m \bmod N$。

定义 8　加密密钥 K 是一个有序对 $\langle e, N\rangle$,其中 N 是不同素数的乘积,且 $N > M$,e 与 $\varphi(N)$ 互素,密钥 K 形如 $K = N^e$。

定义 9　用加密密钥 $K = \langle e, N\rangle$ 对消息 m 的加密记为 $[m, K]$,计算表达式如下:

$$[m, \langle e, N\rangle] = m^e \bmod N \tag{3}$$

定义 10　K 对应的解密密钥 K^{-1} 记为 $\langle d, N\rangle$,K^{-1} 满足 $ed \equiv 1 \bmod \varphi(N)$。

定理 2　对于任何消息 m,有:

$$[[m, K], K^{-1}] = [[m, K^{-1}], K] = m \tag{4}$$

这里,$K = \langle e, N\rangle$,$K^{-1} = \langle d, N\rangle$。

推论 2　对于加密算法 $[m, K]$,如果满足下列关系:$[[m, K], K^{-1}] = [[m, K^{-1}], K] = m$,那么 $[m, K]$ 被认为是一一对应的。

定义 11　两个密钥 $K_1 = \langle e_1, N_1\rangle$ 和 $K_2 = \langle e_2, N_2\rangle$,如果 $e_1 = e_2$,且 N_1 和 N_2 互素,那么 K_1 和 K_2 被认为是相容的。

定义 12　如果 K_1 和 K_2 是两个相容密钥,那么积密钥 $K_1 \times K_2$ 记为 $\langle e, N_1N_2\rangle$。

引理 1　对于正整数 a、N_1 和 N_2,有:

$$(a \bmod N_1N_2) \equiv a \bmod N_1 \tag{5}$$

定理 3　对于任意两个消息 m 和 m',有:

1) $[m, K_1 \times K_2] \equiv [m', K_1] \bmod N_1$ 当且仅当 $m = m'$;

2) $[m, K_1 \times K_2] \equiv [m', K_2] \bmod N_2$ 当且仅当 $m = m'$;

这里,$K_1 = \langle e, N_1\rangle$,$K_2 = \langle e, N_2\rangle$,$K_1 \times K_2 = \langle e, N_1N_2\rangle$。

上面定理证明请参考文献[18]。交叉验证理论主要适用于电子商务协议。当互不信任的交换双方在交换之前,可使用交叉验证理论检验被交换的数字资源的真伪。

假设 m 是待交换的数字资源,权威机构 CA 产生加密密钥 $K_1 = \langle e, N_1\rangle$ 和对应的解密密钥 $K_1^{-1} = \langle d, N_1\rangle$,然后将 K_1 发送给拥有 m 的实体 P_i。P_i 产生相容密钥 K_2,用积密钥加密消息得 $M = [m, K_1 \times K_2]$,并将 M 发送给 CA。CA 发布 M 到公共目录。某个期望交易的实体 $P_j (i \neq j)$ 从公共目录下载 M,并向 P_i 请求 $M' = [m, K_2]$,P_j 可验证 $M \equiv M' \bmod N_2$(根据定理 3)。当交易完成,P_i 向 P_j 发送 K_2^{-1},P_j 可计算 $[M', K_2^{-1}]$,或者向 CA 提起仲裁,请求 K_1^{-1},然后计算 $[M, K_1^{-1}]$。

2　去中心化的多方交换协议

我们提出一种在 P2P 环境下真正去中心化的多对多公平交换协议。本协议主要面向 P2P 环境下节点彼此间的有价资源交换,并非真正的电子商务,因此不需要银行的参与,这就去除了银行等相对中心节点。

2.1　标识符说明

协议主要包含三类实体:1) P_i,即普通 P2P 节点,$i \in \{0, 1, \cdots, n\}$;2) CA,即权威认证中心节点,主要负责数字资源的认证和发布,为了防止该节点成为性能瓶颈或拒绝服务攻击对象,CA 节点可离线运行;3) STTP,半可信第三方的思想特别适合 P2P 应用环境,我们可以引入信任模型,将部分信任度高的 P2P 节点作为 STTP,我们假设 STTP 可以执行部分违反协议的欺骗行为,但是 STTP 不会与任何交换实体合谋欺骗其他交换实体。

$[m, K]$:表示用密钥 K 对消息 m 加密;

$H(\cdot)$:表示安全的单向散列函数;

$Sig_X(m)$:表示实体 X 对消息 m 的签名,本协议采用 ELGamal 签名算法;

$X \rightarrow Y$: m:表示实体 X 向实体 Y 发送消息 m;

$X \Leftarrow \mathrm{CA} \mid Y$: m:表示实体 X 从 CA 公告栏下载属于实体 Y 的消息 m;

$\mathrm{CA} \dashv$: m: 表示 CA 发布消息 m 到公告栏;

$m \parallel n$:表示消息 m 与 n 连接;

$\forall$:表示每一个实体。

2.2　协议描述

假设所有实体都拥有两对公私密钥对,一对用于加解密,一对用于签名及签名验证,并假设 STTP 与 P2P 节点之间的通信信道是可恢复信道[19]。

本协议分为四个阶段。第一个阶段是有价消息的认证、注册和发布,在这一阶段,有需要交换有价资源的实体 P_i 向 CA 中心提交它的数字资源和描述信息,CA 对数字资源进行离线认证,并为该资源分配一个全局唯一的编号 Mid_i,$Mid_i \in \{0, 1, \cdots, k\}$ 然后发布到公告栏。第二个阶段是交换准备阶段,各实体 P_i 查看 CA 公告栏,初步选定待交换的实体对象集 $Q_i (P_i \notin Q_i)$ 以及对应的数字资源,然后 P_i 向 Q_i 中的每个实体发送一个交易请求消息,一段时间以后,P_i 从接收到的交易请求实体列表里面筛选以确定最后的待交易对象实体集 Q_i',显然 $Q_i' \subseteq Q_i$,接着,从 CA 公告栏下载 Q_i' 中每个实体对应的有价资源验证信息。第三个阶段是交换阶段,P_i 向 Q_i' 中编号大于 i 的实体 $P_j (i < j)$ 发起交易,并进行数字资源的交易。这里,规定 P_i 只能向编号大于它的实体 P_j 发起交易的目的是为了避免因双向发起交易而引起的交易混乱。第四个阶段为争端解决阶段,如果交易出现不公平现象,那么某个实体 P_i 向 STTP 发起争端裁决请求,STTP 进行相应裁决。下面详细地描述每个阶段的运行机制。

2.2.1　资源认证与发布

在这一阶段,首先由实体 P_i 向 CA 提交数字资源认证请求,执行过程如下:

$$P_i \rightarrow \mathrm{CA}: [P_i \parallel Desc_{mi} \parallel m_i \parallel DT_i \parallel Sig_{Pi}(H(\Sigma_1)), K_{\mathrm{CA}}]$$

$$\Sigma_1 = P_i \parallel Desc_{mi} \parallel m_i \parallel DT_i$$

$CA \rightarrow P_i$: $[K_{i1} \parallel Sig_{CA}(K_{i1}), K_{Pi}]$

$P_i \rightarrow CA$: $[m_i, K_{i1} \times K_{i2}] \parallel K_{i2} \parallel Sig_{Pi}(H([m_i, K_{i1} \times K_{i2}] \parallel K_{i2}))$

$CA \dashv$: $P_i \parallel Mid_i \parallel Desc_{mi} \parallel [m_i, K_{i1} \times K_{i2}] \parallel K_{i1} \parallel K_{i2} \parallel DT_i \parallel Sig_{CA}(H(\Sigma_2))$

$\Sigma_2 = P_i \parallel Mid_i \parallel Desc_{mi} \parallel [m_i, K_{i1} \times K_{i2}] \parallel K_{i1} \parallel K_{i2} \parallel DT_i$

$CA \rightarrow$ STTP: $[Mid_i \parallel K_{i1}^{-1} \parallel TS_i \parallel Sig_{CA}(H(\Sigma_3)), K_{STTP}]$

$\Sigma_3 = Mid_i \parallel K_{i1}^{-1} \parallel TS_i$

资源认证请求消息包含五个部分：身份标识 P_i、数字资源 m_i 及其描述 $Desc_{mi}$、资源有效期 DT_i 以及 P_i 对前面四项消息摘要的签名 $Sig_{Pi}(H(\Sigma_1))$。CA 验证资源后产生密钥对 $\langle K_{i1}, K_{i1}^{-1} \rangle$，然后向 P_i 发送加密密钥 K_{i1} 并签名。P_i 接收到 K_{i1} 后，产生与 K_{i1} 相容的密钥对 $\langle K_{i2}, K_{i2}^{-1} \rangle$，用积密钥 $K_{i1} \times K_{i2}$ 加密数字资源并签名，将加密后的数字资源、K_{i2} 及其签名发送给 CA。CA 利用交叉验证理论[18] 验证加密资源和 K_{i2} 的有效性，为该资源分配一个全局唯一的标识符 Mid_i，然后发布资源信息以及 CA 对该资源信息摘要的签名到公告栏，将 K_{i1} 对应的解密密钥 K_{i1}^{-1} 以及相应资源编号伴随签名发送给 STTP，并用时间戳 TS_i 防止重放攻击。到此，资源 m_i 的认证和发布阶段结束。

2.2.2 交换准备阶段

交换准备阶段主要完成交易对象协商和交易相关信息下载，过程如下：

$\forall P_i \rightarrow (\forall P_j \in Q_i)$: $[P_j \parallel Mid_i \parallel Mid_j \parallel T_i \parallel Sig_{Pi}(H(\Sigma_4)), K_{Pj}]$

$\Sigma_4 = P_j \parallel Mid_i \parallel Mid_j \parallel T_i$

$\forall P_i \Leftarrow$ CA $\mid \forall (P_j \in Q_i')$: $P_j \parallel Mid_j \parallel Desc_{mj} \parallel [m_j, K_{j1} \times K_{j2}] \parallel K_{j1} \parallel K_{j2} \parallel DT_j \parallel Sig_{CA}(H(\Sigma_5))$

$\Sigma_5 = P_j \parallel Mid_j \parallel Desc_{mj} \parallel [m_j, K_{j1} \times K_{j2}] \parallel K_{j1} \parallel K_{j2} \parallel DT_j$

首先，每一个期望交易的实体 P_i 查询 CA 公告栏，初步选定待交易的对象实体集 Q_i。然后，P_i 向 Q_i 中的每个实体 $P_j (i \neq j)$ 发送交易请求消息 $(P_j \parallel Mid_i \parallel Mid_j \parallel T_i)$ 并签名，其中，Mid_i 和 Mid_j 为待交易的数字资源编号，P_j 为本次交易的对象实体，T_i 为本次交易协商的时限，即交易请求在 T_i 时间结束以前有效。在一段时间以后（可定义为 T_i），P_i 检测接收到的来自其他实体的交易请求，挑选出来自 Q_i 中且待交易数字资源与自己发送的交易请求相同的那部分请求消息，并检验其数字签名，以此确定最终的待交易对象实体集 Q_i'，显然 $Q_i' \subseteq Q_i$。如图 1 所示。

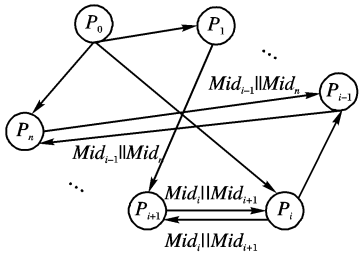

图 1 交易对象协商机制

图 1 中，箭头表示交易请求发送方向。可见，这个过程是一个隐蔽的协商机制，即每个实体单向发布自己的交易意向，然后选择与自己交易意向重叠的所有实体作为最终的交易对象，如图中 $\langle P_{i-1}, P_n \rangle$ 和 $\langle P_i, P_{i+1} \rangle$ 两对实体成功达成交易意向，其余交易请求作废，并且这个协商结果对外保密，只有交易双方知道。交易对象确定以后，每个 P_i 从 CA 公告栏下载所需的相关消息，并检验 CA 签名的有效性。

2.2.3 交换阶段

首先，P_i 向 Q_i' 中编号大于 i 的实体 $P_j (i < j)$ 发起交易，这样做的目的是为了避免因双向发起交易而引起的交易混乱，原理如图 2 所示。

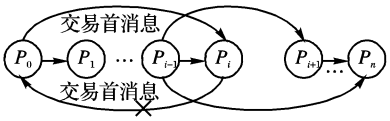

图 2 交换发起方案

由图 2 可以看出，始终由编号较低的一方主动发起交换避免了因双向发起交换引起的混乱，例如，图 2 中 P_i 向 P_0 发起的交换。交换过程如下。

$\forall P_i \rightarrow \forall ((P_j \in Q_i') \wedge (i < j))$: $[tid_{ij} \parallel Mid_i \parallel Mid_j \parallel [m_i, K_{i1}] \parallel [m_i, K_{i2}] \parallel Sig_{Pi}(H(\Sigma_6)), K_{Pj}]$

$\Sigma_6 = tid_{ij} \parallel Mid_i \parallel Mid_j$

$\forall P_j \rightarrow \forall P_i$: $[tid_{ij} \parallel [m_j, K_{j1}] \parallel [m_j, K_{j2}] \parallel TS_{ij} \parallel Sig_{Pj}(H(\Sigma_7)), K_{Pi}]$

$\Sigma_7 = tid_{ij} \parallel Mid_i \parallel Mid_j \parallel TS_{ij} \parallel Sig_{Pi}(H(\Sigma_6))$

$\forall P_i \rightarrow \forall P_j$: $[tid_{ij} \parallel K_{i2}^{-1}, K_{Pj}]$

$\forall P_j \rightarrow \forall P_i$: $[tid_{ij} \parallel R \parallel K_{j2}^{-1}, K_{Pi}]$

这里，$\forall P_i \rightarrow \forall ((P_j \in Q_i') \wedge (i < j))$ 表示每个需交换实体（$\forall P_i$）向 Q_i' 中编号大于 i 的实体（$\forall ((P_j \in Q_i') \wedge (i < j))$）发送消息 Σ。Σ 由 P_i 随机生成的交易标识符 tid_{ij}、待交换数字资源标识符 $Mid_i \parallel Mid_j$、分别用 K_{i1} 和 K_{i2} 对数字资源加密的消息 $[m_i, K_{i1}] \parallel [m_i, K_{i2}]$ 以及 P_i 的签名消息 $Sig_{Pi}(H(\Sigma_6))$ 连接而成，并用接收实体公钥加密 Σ。P_j 收到消息 Σ 后查看待交易队列 Q_j'，检查待交换数字资源是否符合自己的要求，当前时钟是否超过了资源 Mid_i 的有效时间 DT_i，通过交叉验证理论检验加密资源的有效性，检验 P_i 签名的有效性。如果通过检验，每个 P_j 向对应的 P_i 发送交易确认消息，确认消息由交易标识符 tid_{ij}、用 K_{j1} 和 K_{j2} 对数字资源加密的消息 $[m_j, K_{j1}] \parallel [m_j, K_{j2}]$、时间戳 TS_{ij} 以及 P_j 的签名消息 $Sig_{Pj}(H(\Sigma_7))$ 连接而成，其中，$Sig_{Pj}(H(\Sigma_7))$ 作为 P_j 向 P_i 提供的非否认证据。收到确认消息后，P_i 检测时间戳，利用交叉验证理论检验加密资源的有效性，检验 P_j 签名的正确性。通过检验后，双方交换数字资源的解密密钥。值得注意的是，最后一条消息中的 R 表示 P_j 生成的一个随机值，用于区分前一条消息，以防止选择密文攻击。

2.2.4 争端解决阶段

如果交换阶段正常结束，那么毋须进行争端解决，只有当出现网络故障（数据包丢失）或某个交易实体有意欺骗时，进入争端解决阶段。根据交换阶段的执行过程，只有当 P_j 收到正确的解密密钥后才会向 P_i 发送相应的解密密钥，因此，争端不可能发生在 P_j 方。由此定义争端解决只能由交换发起方 P_i 提交，过程如下。

$P_i \rightarrow$ STTP: $[tid_{ij} \parallel Mid_i \parallel Mid_j \parallel Sig_{Pi}(H(\Sigma_6)) \parallel TS_{ij} \parallel Sig_{Pj}(H(\Sigma_7)), K_{STTP}]$

STTP $\rightarrow P_j$: $[tid_{ij} \parallel K_{i1}^{-1} \parallel TS_i \parallel Sig_{CA}(H(\Sigma_{i3})), K_{Pj}]$

STTP $\rightarrow P_i$: $[tid_{ij} \parallel K_{j1}^{-1} \parallel TS_j \parallel Sig_{CA}(H(\Sigma_{j3})), K_{Pi}]$

首先，交换发起方 P_i 确认接收了正确的加密数字资源

$[m_j, K_{j1}]$,发送了正确的解密密钥 K_{i2}^{-1},但是没有收到正确的解密密钥 K_{j2}^{-1}。然后,P_i 向 STTP 发送争端解决请求消息,包括交易标识符 tid_{ij}、待交换资源标识符 Mid_i 和 Mid_j、P_i 的确认签名 $Sig_{Pi}(H(\Sigma_6))$、时间戳 TS_{ij} 和 P_j 的不可否认签名 $Sig_{Pj}(H(\Sigma_7))$。STTP 验证时间戳和各签名的有效性,通过 P_j 的签名 $Sig_{Pj}(H(\Sigma_7))$,STTP 可确认 P_j 已正确接收了相应的加密数字资源 $[m_i, K_{i1}]$。接着,STTP 向交换双方发送相应的解密密钥 K_{i1}^{-1} 和 K_{j1}^{-1},以及 CA 对密钥的签名。这里,STTP 仍然向 P_j 发送解密密钥是因为 P_i 发送的消息 $[tid_{ij} \parallel K_{i2}^{-1}, K_{Pj}]$ 可能由于网络故障而丢失,因此我们定义各实体与 STTP 的信道为可恢复信道,即发向和来自 STTP 的消息最终会到达规定的目标节点,但可能会存在一段时间延迟,这是由于如果各实体与 STTP 间的信道不可靠,那么将不可能满足公平性[19]。

3　协议分析

我们从协议有效性、交换公平性、STTP 行为可验证和交易拓扑的保密性几个方面来对本文协议进行分析。

3.1　协议有效性分析

定理 4　假设交叉验证理论是可证明正确的,并且各实体与 STTP 之间的信道是可恢复信道,那么本文提出的多方交换协议满足有效性。

证明

首先考察资源认证有效性。在此阶段,我们使用了公钥加密技术保持数据的机密性,采用了数字签名技术防止消息被篡改,签名实体对消息的真伪负责,另外,还使用了时间戳来防止重放攻击。这里,我们假定 CA 完全可信,认证请求者需向 CA 提供数字资源明文(m_i) 及其描述 $Desc_{mi}$,CA 需验证 m_i 和 $Desc_{mi}$ 符合要求才进入下一步,否则终止认证。接着,CA 利用交叉验证理论验证 P_i 上传的加密数字资源 $[m_i, K_{i1} \times K_{i2}]$ 和 K_{i2},如定理 3:

$$[m_i, K_{i1} \times K_{i2}] \equiv [m_i, K_{i1}] \bmod N_{i1} \tag{6}$$

$$[m_i, K_{i1} \times K_{i2}] \equiv [m_i, K_{i2}] \bmod N_{i2} \tag{7}$$

式(6) 中,K_{i1} 为 CA 产生的加密密钥。可见,资源认证的有效性依赖于交叉验证理论的正确性,即定理 3 的正确性[18]。

其次,考察交换对象协商机制的有效性。由 2.2.2 节的分析和图 1 表明,如果网络基本可靠(即不存在数据包大量丢失的情况),那么交换对象协商机制是有效的。另外,如果存在少量数据包丢失的情况,则可采取部分请求消息重发的方法增强协商成功的概率。

再次,我们考察交换过程的有效性。由图 2 可知交换的发起是有序的。假设交换双方是诚实的,同时假设信道是可靠的,交换过程的有效性同样依赖于交叉验证理论的正确性(即式(6)和(7)的正确性)、资源认证的有效性和交换对象协商机制的有效性。另外,如果交换双方是不诚实的或信道是不可靠的,则交换的有效性还依赖于争端解决的有效性。

最后,考察争端解决的有效性。由 2.2.4 节的分析可知,如果各实体与 STTP 间的信道是可恢复信道,那么正确的解密密钥最终会到达相应的接收实体,虽然可能存在一段时间延迟,因此,争端解决机制是有效的。

由上面的分析可见,本文协议的有效性依赖于交叉验证理论是可证明正确的,且各实体与 STTP 之间的信道是可恢复信道。　　证毕。

3.2　多方交换公平性分析

根据两方交换协议公平性定义[19]:交换双方要么获得彼此期望的数字资源,要么没有任何一方获得期望的数字资源。我们提出多方交换环境下的两两交换公平性概念,即多方交换中的每个两两交换满足两方交换公平性,那么该多方交换协议满足两两交换公平性。进而,具有两两交换公平性的多方交换协议满足多方交换公平性。另外,我们还假定所有参与实体都不会主动泄漏自己的秘密信息。

定理 5　假设交叉验证理论是可证明正确的,并且各实体与 STTP 之间的信道是可恢复信道,那么本文提出的多方交换协议满足两两交换公平性。

证明　由于本文多方交换协议中涉及的两两交换是相互独立的,因此,只需证明每个两两交换协议满足两方交换公平性。由交换过程可知,在 P_i 发送相应的数字资源解密密钥之前,P_i 和 P_j 都没有获得期望的数字资源,即此时是公平的。如果继续执行协议,由于交换实体可能是不诚实的以及信道不是完全可靠的,那么存在以下三种情况。

1)P_i 没有发送正确的解密密钥 K_{i2}^{-1},那么 P_j 不会发送解密密钥。P_i 可选择终止交换或发起争端解决,如果,P_i 选择终止交换,那么双方都没有获得有效的解密密钥,此时满足公平性。如果 P_i 发起争端解决,那么 STTP 通过双方的签名($Sig_{Pi}(H(\Sigma_6))$ 和 $Sig_{Pj}(H(\Sigma_7))$) 可知 P_i 和 P_j 都已收到正确的加密数字资源 $[m_i, K_{i1}]$ 和 $[m_j, K_{j1}]$,然后向交换双方同时发送正确的解密密钥 K_{i1}^{-1} 和 K_{j1}^{-1},密钥的有效性由 CA 的签名保证,由于各实体与 STTP 之间的信道为可恢复信道,所以解密密钥一定能到达指定的接收者,此时,P_i 和 P_j 都能获得有效的加密数字资源及有效的解密密钥,从而获得各自期望的数字资源。因此,协议满足公平性。

2)P_i 发送了正确的解密密钥 K_{i2}^{-1},而没有收到 P_j 发送的正确的解密密钥 K_{j2}^{-1}。这有两种可能,即 P_i 或 P_j 发送的解密密钥由于信道的原因丢失了,或者 P_j 没有发送相应的解密密钥。P_i 可发起争端解决,由定理 4,如果交叉验证理论是可证明正确的,且各实体与 STTP 之间的信道是可恢复信道,那么争端解决是有效的,P_i 和 P_j 都能获得各自期望的数字资源。此时,协议满足公平性。

3)P_i 收到了 P_j 发送的正确的解密密钥 K_{j2}^{-1}。由于 P_j 在没有获得有效的解密密钥 K_{i2}^{-1} 之前,不会发送相应的解密密钥 K_{j2}^{-1},由此可断定 P_j 已获得有效的数字资源。同时,P_i 也已收到有效的加密数字资源 $[m_j, K_{j2}]$($[m_j, K_{j2}]$ 有效性可由交叉验证理论检验) 和正确的解密密钥 K_{j2}^{-1},可判定 P_i 也可以解密获得有效的数字资源 m_j。因此,协议满足公平性。

可见,如果交叉验证理论是可证明正确的,并且各实体与 STTP 之间的信道是可恢复信道,那么本文提出的多方交换协议满足两两交换公平性。　　证毕。

3.3　对 STTP 行为的分析

由 STTP 的定义,STTP 可能会主动欺骗交换中的任何一方,且企图获得交换的数字资源,但不会与其中一方联合欺骗另外一方。

定理 6　如果交叉验证理论是可证明正确的,那么 STTP 不能获得任何交换的数字资源。

证明　STTP 虽然获得解密密钥 K_{i1}^{-1},但是如果没有交换其中一方的帮助,那么他将不能获得有效的加密数字资源 $[m_i, K_{i1}]$,因此,如果交叉验证理论是可证明正确的,那么

STTP 就不能获得有效的数字资源 m_i。 证毕。

另外,STTP 在争端解决中的行为是可验证的,所发送的解密密钥的有效性可由 CA 签名确保。

3.4 交易拓扑的保密性分析

交易拓扑的保密性是多方交换协议特有的一个性质,即最终发生的交易行为对外部是保密的。在本文协议中,每个消息都是被加密传输的,除了对应实体外都不能解密消息,因此不能从消息文本中获得交换实体信息。另外,由图 1 可知交换对象协商是单向发布信息,如果不能获得所有消息文本中的实体信息,那就不能通过交换对象协商过程获得成功配对的交换实体对。可见,本文协议的交易拓扑是保密的。

4 结语

本文提出一种适合 P2P 网络的去中心化多方公平交换协议,协议分为四个阶段,采用交叉验证理论进行有价资源的认证和验证,采用离线半可信第三方进行争端解决,较好地解决了资源验证、交换对象协商和自动争端解决等问题。协议的公平性依赖于交叉验证理论的可证明正确性以及交换实体与 STTP 之间信道的可恢复性。

对本文协议的形式化分析和仿真实验将是我们下一阶段的工作重点。另外,协议在交换对时间敏感的资源时较为脆弱,这是由于恶意实体可任意延迟解密密钥到达指定实体的时间,这也是基于离线第三方交换协议难以解决的一个重要问题[18],这个难题也是我们下一步需要研究的方向。

参考文献:

[1] ASOKAN N, SCHUTER M, WAIDNER M. Optimistic protocols for multi-party fair exchange, RZ 2892[R]. Zurich: IBM Research Division, 1996.

[2] ASOKAN N, SCHUNTER M, WAIDNER M. Optimistic protocols for fair exchanges[C]// Proceedings of the 4th ACM Conference on Computer and Communications Security. New York: ACM Press, 1997: 7 - 17.

[3] ONIEVA J A, ZHOU JIAN-YING, LOPEZ J. Non-repudiation protocols for multiple entities [J]. Computer Communications, 2004, 27(16): 1608 - 1616.

[4] KREMER S, MARKOWITCH O. A multi - party non - repudiation protocol [C]// Proceedings of the IFIP TC11 Fifteenth Annual Working Conference on Information Security for Global Information Infrastructures. Netherlands: Kluwer, 2000: 271 - 280.

[5] 韩志耕,罗军舟. 一个公平的多方不可否认协议[J]. 计算机学报, 2008, 31(10): 1705 - 1715.

[6] 刘义春. P2P 组合交易的公平支付协议[J]. 计算机工程, 2008, 34(18): 171 - 173.

[7] INSOO K, JISEON K, INGOO H, *et al*. Multi-party fair exchange protocol using ring architecture model [J]. Computers & Security, 2001, 20(5): 422 - 439.

[8] FRANKLIN M, TSUDIK G. Secure group barter: Multi-party fair exchange with semi-trusted neutral parties [J]. Heidelberg: Springer-Verlag, 1998: 90 - 102.

[9] BAO FENG, DENG R, NGUYEN K Q, *et al*. Multi-party fair exchange with an off-line trusted neutral party [C]// DEXA: Proceedings of the 10 th International Workshop on Database & Expert Systems Applications. Washington, DC: IEEE Computer Society Press, 1999: 858 - 862.

[10] 杜红珍,张建中. 一个新的带离线半可信第三方的多方公平交换协议[J]. 计算机应用研究, 2006, 23(7): 248 - 250.

[11] 李艳平,张建中. 带离线半可信第三方的多方交换协议[J]. 西安电子科技大学学报: 自然科学版, 2004, 31(5): 811 - 814.

[12] MUKHAMEDOV A, KREMER S, RITTER E. Analysis of a multi-party fair exchange protocol and formal proof of correctness in the strand space model[C/OL]. [2009 - 01 - 01]. http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/MKR-fcrypto05.pdf.

[13] GONZALEZ-DELEITO N, MARKOWITCH O. Exclusions and related trust relationships in multi-party fair exchange protocols [J]. Journal of Electronic Commerce Research and Application, 2007, 6(3): 343 - 357.

[14] ARORA G, HANNEGHAN M, MERABTI M. P2P overlay network to support E-commerce [C/OL]. [2009 - 01 - 01]. http://www.cms.livjm.ac.uk/pgnet2006/Programme/Papers/2006-101.pdf.

[15] ARORA G, HANNEGHAN M, MERABTI M. P2P commercial digital content exchange [J]. Journal on Electronic Commerce Research and Applications, 2005, 4(3): 250 - 263.

[16] 秦志光,罗绪成. P2P 共享系统中无需专用 TTP 的公平交换协议[J]. 电子科技大学学报, 2008, 35(4): 698 - 701.

[17] 赵洋,秦志光,蓝天,等. 一种适用于 P2P 环境的乐观公平交换协议[J]. 计算机应用, 2007, 27(8): 1881 - 1883.

[18] RAY I, RAY I, NATARAJAN N. An anonymous and failure resilient fair-exchange e-commerce protocol [J]. Decision Support Systems, 2005, 39(10): 267 - 292.

[19] KREMER S, MARKOWITCH O, ZHOU J. An intensive survey of non-repudiation protocols [J]. Computer Communications, 2002, 25(17): 1606 - 1621.

(上接第 2605 页)

式特点,而且具有较强的恶意行为检测能力,同时该模型考虑了移动 P2P 网络中移动终端的计算性能的差异和推荐信任的可扩展性。

参考文献:

[1] WALKERDINE J, LOCK S. Towards secure mobile P2P systems [C]// ICIW: Proceedings of the Second International Conference of Intern and Web Applications and Services. Washington, DC: IEEE Computer Society, 2007: 6.

[2] 欧中洪,宋美娜,战晓苏,等. 移动对等网络关键技术[J]. 软件学报, 2008, 19(2): 404 - 418.

[3] DUMA C, SHAHMEHRI N, CARONNI G. Dynamic trust metrics for peer-to-peer systems [C]// Proceedings of the 16th International Workshop on Database and Expert Systems Applications. Washington, DC: IEEE Computer Society, 2005: 776 - 781.

[4] 任艳,任平安,吴振强,等. 移动 P2P 网络中的多粒度信任模型[J]. 计算机工程与应用, 2009, 45(6): 137 - 140.

[5] 马新新,耿技. 对等网络信任和信誉机制研究综述[J]. 计算机应用, 2007, 27(8): 1935 - 1938.

[6] WANG LEI, ZHU YAN-QIN, JIN LAN-FANG, *et al*. Trust mechanism in distributed access control model of P2P networks [C]//Proceedings of the 7th IEEE/ACIS International Conference of Computer and Information Science. Portland: IEEE Press, 2008: 19 - 24.

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

[8] 李小勇,桂小林. 大规模分布式环境下动态信任模型研究[J]. 软件学报, 2007, 18(6): 1510 - 1521.