基于数字签名和数字水印的 P2P 协同工作认证技术

The authentication technology of P2P collaboration environment based on the digital signature and digital water marking

何建新 刘国兴 (湖南城市学院计算机科学系 湖南益阳 413000)

摘 要: 为了适用 P2P 协同工作的安全需求,针对 P2P 协作系统中数据传输的特殊性,分析了 P2P 协同工作所存在的安全问题,探讨了 P2P 环境下建立可信协作关系的信息认证技术,提出了一种结合数字签名和数字水印的信息认证技术方案,该方法能够实现对等用户间的身份真实性认证和传输内容的完整性认证,使得用户伪装、非法篡改、伪造信息更加困难。分析表明该方法具有安全性高,可信度高等特点,适合于 P2P 环境下信息的安全传输。

关键词: P2P 协同工作 数字签名 数字水印

1 引言

P2P(Peer – to – Peer,即对等网络)是一种分布式网络。它改变了互联网上以服务器为中心的模式,此网络参与者既是资源提供者(Server),又是资源获取者(Client)。目前 P2P 的主要应用包括:协同工作、对等计算、文件共享和搜索引擎等,其中协同工作是指对等点为完成某一特定任务形成的一个群组,他们相互共享资源、即时交互信息,而且协作系统中的一个用户可以在同一时刻将一个信息多点传送到若干个用户。随着 Internet 网络技术飞速发展,P2P 协作系统用户间诸如视频、音频、图像等数字化信息的传输和共享成为最常见的信息交互形式,数字化信息迅速高效共享的同时,也存在着潜在风险,恶意的个人与团体可能很容易冒充其它协作者窃取、篡改信息。因此 P2P 环境下数字化信息的认证已成为目前信息安全领域的一个研究热点。本文主要分析了 P2P 协同工作的安全特性,以传输数字图像信息为例,结合数字水印认证原理,提出了一种结合数字签名和数字水印的 P2P 信息认证技术方案,其它诸如音频、视频等信息认证具有类比性。

2 P2P 协同工作的安全需求

随着项目规模不断扩大,项目实施中"协同工作"日益受到重视。目前软件一般是基于 C/S 或 B/S 模型开发,P2P 技术实现的协同工作无需 Server 支持,而且同样可以组合成工作组,在之上共享信息,提供更好的"协同工作"能力。

协同工作系统中主要成员有制作者、消费者和管理者,各个成员根据职责的不同,对安全的要求也不同,主要包括[1]:

(1) 系统成员信任关系管理。能够根据节点交易的历史记录,得到成员信任度。

(2) 灵活多样的认证机制。同时支持多种认证方式,支持节点间的双向认证。

(3) 系统用户间的安全通信。保证交互、共享信息的机密性、完整性和不可否认性。

(4) 可信协作关系的建立。解决系统用户间身份认证和信息认证问题。

本文主要解决 P2P 环境下可信协作关系的建立。

提出了一种结合数字签名和数字水印的信息认证技术方案，实现对等用户间的身份真实性认证和传输内容的完整性认证。采用数字水印认证算法，直接将认证信息嵌入到原始信息中，不需要提供另外的存储空间；还可以防止第三方伪装成通信的任何一方进行欺骗行为，同时也能保证信息的完整性，从而建立起可信协作关系。

3 P2P 环境下信息认证技术

数字签名和数字水印信息认证技术构成了 P2P 环境下节点间建立可信协作关系信息认证技术的基础。

3.1 传统数字签名认证

传统数字签名算法，保证发送与接收的文件内容完全一致，但数字媒体信息经过各种压缩格式转换和常规信号处理（如图像有损压缩、去噪、滤波），会产生很多无意失真，但基本不影响视听觉感知。因此，传统数字签名方法不适合验证多媒体信息的真实性。我们需要能够容忍一定误差的宽松数字签名认证机制。

3.2 宽松数字签名认证[2]

宽松数字签名认证由两部分组成：产生原始图像的数字签名和验证待测图像的真伪。在发送方，首先根据图像内容提取特征得到 Co，然后作 Hash 操作以减少数据量，得到 Ho，最后根据私钥 Kpv 对 Ho 加密，得到签名 S。在接收方，对于待测图像提取特征 Ct，然后求 Hash 值，得到 Ht，根据公钥解密收到的签名 S，得到 Ho，然后比较 Ht 和 Ho 来判断真实性，如果两者的差小于阈值说明图像真实。算法设计者可事先测出图像经过压缩、亮度/对比度增强等一般性处理后引入图像的误差，作为判定真实性的阈值参数提供给图像使用者。

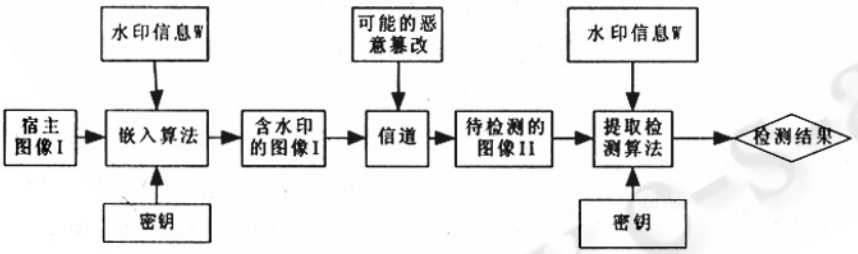

图 1　认证水印系统的一般结构

3.3 数字水印认证

数字水印是利用人类知觉系统的冗余，在不影响数字媒体感官质量的前提下将与媒体内容相关或不相关的标志信息作为水印直接嵌入媒体内容中，当媒体内容需要认证时，可根据提取的水印信息来判断其是否真实完整。

数字水印一般可分为：用于版权保护的鲁棒水印和用于防篡改的认证水印。水印认证算法，主要包括易损水印和半易损水印两大类[3]。基于数字水印的认证系统通常包括三部分：水印产生，水印嵌入和水印提取检测。认证水印系统的一般结构可用图 1 表示。

认证水印在图像发生改变时自身也会相应发生改变，可以根据水印的变化判断图像是否发生改变，甚至找出被篡改的区域。认证过程中所使用的密钥是用来对水印信息加密或生成水印的关键部分。

4 基于数字签名和数字水印的 P2P 协同工作认证方案

在图像真实性方面，易损水印由于其安全的嵌入策略以及对篡改的高敏感性，可以用来判断图像有无被篡改或替换；在图像的完整性方面，根据水印嵌入机制，水印直接嵌入宿主内部，不需要另外的存储空间，且嵌入导致的信息轻微改动主观上不可感知，这使得嵌入信息的删除非常困难，而且保证了嵌入信息与原信息脱离，从而保证了完整性认证能力，而数字签名用以完成完整性验证的信息摘要却必须与原信息结合，而且需要额外的数据存储空间，因此在嵌入水印的设计上，用户可以采用另外一些有意义或者直观的信息，使得认证过程更加具体化[4]。综上所述，作为数字签名的互补技术，易损水印完全满足了图像信息认证系统的新要求。通过结合两种认证技术，构建高安全性和高效性的认证系统是完全可行的。

由于目前数字水印的载体以图像居多，因此我们假设 P2P 协同工作的合法用户都具有能表明身份的图像，如徽章、印章等，而且考虑到 P2P 的动态性，为了加快水印处理速度，提高工作效率，本方案中采用直接在图像的空域嵌入水印的算法。其算法原理如图 2 所示。

本认证方案采用非对称密钥体制，设协作发送方P(制作者)，其公钥为 K_{pu}，私钥为 K_{pv}；协作的接受方C(消费者)，其公钥为 K_{cu}，私钥为 K_{cv}。算法描述如下：

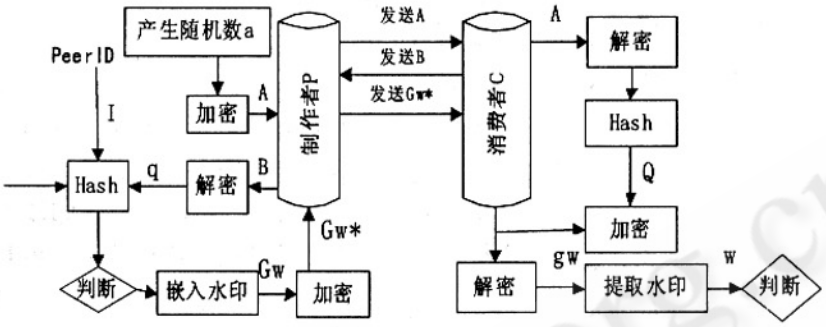

图 2　水印嵌入与提取算法原理

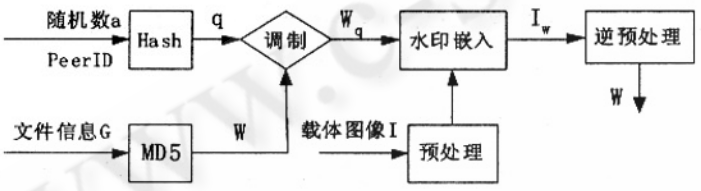

图 3　水印嵌入算法原理图

(1) 发送方P对信息签名加密。P生成随机数a，利用自己的私钥对其签名(加密)，即 $E_{Kpv}(a)$，然后用C的公钥进行加密得到A，即 $A = E_{Kcu}(E_{Kpv}(a))$，将A发送给接受方，同时记录时间 t_{p0} 和a。

(2) 接收方C对A的验证签名及数字证书颁发。C收到A，利用自己的私钥进行解密，即 $D_{Kcv}(A)$，然后用P的公钥进行验证签名(解密)得到s，即 $s = D_{Kpu}(D_{Kcv}(A))$；将s和自己的PeerID进行Hash运算得到Q，即 $Q = h(s, PeerID)$；再对Q用C的私钥签名(加密)，用P的公钥加密得到B，即 $B = E_{Kpu}(E_{Kcv}(Q))$；把B发送给P，并记录发送时间 t_{c0}。

(3) 发送方获得数字证书。发送方记录接收到B的时间 t_{p1}，对B进行解密和验证签名，得到q，即 $q = D_{Kcu}(D_{Kpv}(B))$，为了不占用过多时间，必须设定一个时间阈值 t_p，为发送方允许的最大时间间隔，判断如下：

if ($t_{p1} - t_{p0} < t_p$ and $h(a, PeerID) = q$)

then (下一步操作)

else 中断此次通信

(4) 水印嵌入机制。上述步骤确保了通信双方身份的真实性认证，但对于信息内容的可信度却没有提供保障，下面采用易损水印技术来实现所传输信息内容的完整性认证。

① 计算G(文件信息摘要)的MD5值，作为水印信息W；

② 用q作为水印密钥，对水印信息w加密得到 W_q；

③ 对载体图像I(本算法中假设是表明用户身份的数字公章图像)作预处理(经某种变换域变换)，将 W_q 嵌入得到 I_w；

④ 将 I_w 插入到要传输的G中，得到 G_w，对 G_w 进行加密得到 G_w*，即 $G_w* = E_{Kcu}(E_{Kpv}(G_w))$；

⑤ 将 G_w* 发送给消费者。

嵌入水印算法基本原理如图3所示。

以用户私钥作为水印嵌入密钥，以公钥作为水印证实密钥，满足了信息认证系统对于用户发送不可抵赖性和不可否认性的内在要求，而且易损水印保证了会话过程中信息的完整性和真实性，从而满足了内容认证的要求。

(5) 水印提取检测并确立协作关系。C收到Gw*并解密，得到gw，即 $gw = D_{Kpu}(D_{Kcv}(Gw*))$，并记录收到Gw*的时间 t_{c1}。通过水印提取，得到Wq′，利用Q从Wq′中提出W，而W′则由计算所收到的文件内容信息摘要得到。水印的检测一般依赖提取水印W与原始水印W′的差图来判断。差图的实际意义是比较两幅二值图像之间的差异，如果相应像素点的像素值相等，则在差值图像上像素值为0，即表现为白色点；反之则为1，表现为黑色点。文献[5]给出了稀疏点的定义，按照这个定义分别计算水印差图中稀疏点与稠密点个数，若定义：m = 差图中稀疏点的像素总数；n = 差图中稠密点的像素总数；s = 水印差图中像素点总数；$\lambda = (m+n)/s$，若 $\lambda = 0$，则说明图像没有被篡改，即 $W = = W'$；若 $\lambda > 0$，则计算 $\delta = m/n$，若 $\delta > T$(T为检测方设定的一个非负门限值)，则认为存在偶然攻

击,否则认为存在恶意篡改。

然后根据网络情况设定一个时间阈值,设阈值 t_c 为接受方允许的最大时间间隔,判断如下:

if($t_{cl} - t_{c0} < t_c$ and W = =W')

then(建立可信协作关系)

else 中断此次通信

P2P 环境下双方身份通过上述真实性认证和传输内容完整性认证后,就可以进行协同工作了。

5 协同工作认证方案安全性能分析

本算法采用水印信息嵌入到数字图像中,它可以有效防止篡改,文件内容稍加改动,其 MD5 值就会与水印信息中的原值不同。协作的双方通过对提取出的水印进行检测,就可以判断出内容是否被篡改了,同时确认对方身份。

比如多个节点之间要建立协作关系,协作发起方 P 向合法协作者 C 传送文件。若有非法用户 E(攻击者)想窃取该机密文件,他用不法手段窃取了合法协作者的私钥 K_{cv},伪装成合法协作者C,然后他截取了 P 发送过来的 A,用合法协作者的私钥 K_{cv}和发起方的公钥 K_{pu}可以解密得到 b,但是他不知道该用户的 PeerID,因此无法获得正确的 Q,设其生成 Q',当 P 收到 Q',解密得到 q',然后他再用正确的 ID 和 a 进行 Hash 运算,显然这个值不等于 q'。此时 P 就知道对方不是他想要通信的对象,攻击者 E 伪装为合法协作者失败。

若攻击者 E 想伪装成制作者 P,向合法协作者提供虚假资料进行欺骗,同样,攻击者先截获合法协作者所生成的 Q,直接将 Q 作为水印信息,但他不具备 P 的私钥 K_{pv},合法协作者 C 对接收到的 Gw 解密后,计算得到的 W 不可能和 W'相同,即合法协作者会认为信息无效,攻击者伪装成协作发起者失败。

该算法还可防止不可否认性,即协作发起者 P 否认信息是由他发出的,以及否认资料是由他所提供的。因为 C 可以向公证机构出示 P 的随即数 a 和其 ID,计算 q,通过水印检测算法利用 q 可以把水印提取出来,从而验证传输的信息中存在与 P 对应的水印,这就说明随机数 a 确实由 P 生成,这样 P 就不能否认其之前的行为。因此协作的发起者必须对自己的行为负责,从而维护协作双方的利益。

6 小结

本文提出了一种将数字签名和数字水印相结合应用到 P2P 协同工作中的认证技术方案,该方案主要针对 P2P 无中心,不可能提供存储空间来存储认证码的缺陷,利用数字水印可以将认证信息嵌入到原始信息中,不需要存储空间的特点,从而使身份认证过程更为严密。由于针对数字信息的基于水印技术的安全认证技术尚处于探索阶段,因此系统的一些安全漏洞及一些未知的攻击还有待分析和加强,下一步我们将更深入研究如何利用易损水印及双密钥机制对 P2P 环境下的信息提供更完善的认证保护。

参考文献

1 张铁军、张玉清、战守义、张德华, Peer - to - Peer 典型应用安全需求分析[J], 计算机工程,2004,31(20):56 - 58.

2 SCHNEIDER M, CHANGS - F. A robust content based digital signature for image authentication[A]. Proceedings of IEEE Int. Conference on Image Processing [C]. Lausanne, Switzerland, 1996,3:227 - 230.

3 邹潇湘, 多媒体数字水印技术研究[D], 北京:中国科学院计算技术研究所,2003.7.

4 夏旭、朱从旭、陈志刚, P2P 协同工作环境下的一种多媒体认证系统[J], 计算机应用,2007.4,27(4):846 - 850.

5 HU JQ, HUANG JW, HUANG DR, etal. Image fragile water marking based on fusion of multi - resolution tamper detection [J]. ElectronicsLetters, 2002, 38(24):1512 - 1513.