第33卷 第15期 计 算 机 工 程 2007年8月
Vol.33 No.15 Computer Engineering August 2007
·博士论文· 文章编号：1000—3428(2007)15—0001—02 文献标识码：A 中图分类号：TP309

一个安全的P2P网络数字内容保护方案

王晓明
(暨南大学计算机系，广州 510632)

摘 要：分析了Gu等人提出的P2P网络数字内容保护方案，指出其中存在合谋攻击，即当P2P网络中大于门限值的LAA合谋，就可以重新构造网络的秘密多项式函数，得到网络的秘密参数，从而破坏P2P网络的数字内容保护机制。基于该方案，提出了一种新的P2P网络数字内容保护方案，不仅具有Gu等人方案的特点，而且能抵抗合谋攻击。

关键词：P2P网络；数字内容保护；合谋攻击

Protection Scheme of Digital Content in P2P Network

WANG Xiao-ming
(Department of Computer Science, Jinan University, Guangzhou 510632)

【Abstract】 This paper analyzes Gu's scheme and proposes a conspiracy attack on it. Using the conspiracy attack, any t (t is threshold value) or more LAs (license authorities) may woke together to reconstruct the secret polynomial of the license and derive the secure share keys of other LAs in P2P networks. They can also impersonate some other LAs to generate a valid partial license and break the protected mechanism of digital content in P2P network. A digital content protected scheme is presented for P2P networks based on Gu's scheme. The new scheme can achieve all the properties in Gu's scheme, and withstand the conspiracy attack in Gu's scheme.

【Key words】 peer-to-peer(P2P) network; digital content protection; conspiracy attack

近几年，对传统网络的数字内容保护的研究非常活跃，已出现了很多数字内容保护系统[1~5]。但针对对等网络的数字内容的保护系统或方案还不多。最近，Gu等人提出了一个P2P（peer-to-peer）网络的数字内容保护方案[6]，该方案将传统的集中认证中心对数字内容保护的服务分散到整个P2P网络中，由网络中的若干LA(license authority)分担。如申请节点要使用保护的数字内容，就必须获得网络中一定阈值的LA批准。这种数字内容保护方案非常适合分布式的P2P网络，但是Gu等人的方案存在合谋攻击。

1 Gu等人的方案和它的缺陷

1.1 Gu等人的方案

假设P2P网络中存在很多可信节点，记为LA。SK为发行者私钥，PK为发行者公钥。

(1)发布者对数字内容进行加密。加密算法采用AES。

(2)生成含有加密密钥和访问规则的数字证书$license$，并用PK加密此数字证书，加密算法采用RSA[7]，即$prel=(license)^{PK}$。

(3)发布者选择n个LA=$\{LA_1,LA_2,\ldots,LA_n\}$，并把$SK$分成$n$份子密钥分发给每个LA，即

1)发布者选择一个随机多项式

$$f(x)=SK+a_1x+\ldots+a_{t-1}x^{t-1} \quad (1)$$

计算$S_i=f(id_i)\bmod\phi(N)$，秘密送S_i给每一个LA。其中，id_i为LA的标志；N为RSA算法中的大和数（2个大素数的乘机）；$\phi(N)$为N的欧拉数；

2)公布$\{g^{SK},\ldots,g^{a_{t-1}}\}$，其中，元素$g\in Z_N^*$；

3)每个LA验证$g^{S_i}=g^{SK}(g^{a_1})^{id_1}\ldots(g^{a_{t-1}})^{id_i^{t-1}} \bmod N$，如等式成立，$S_i$有效。

(4)当使用保护的数字内容时，使用者必须获得t(门限值)个LA签发的子数字证书，合成t个子数字证书得到数字证书，从而得到加密密钥。

1)使用者向LA发出获得子数字证书的请求。

2)每个LA选择随机数u，计算$prel_i=(prel)^{S_i} \bmod N$，$A_1=g^u$，$A_2=(prel)^u$，$r=u-cS_i$，$c=hash(g^{S_i},prel_i,A_1,A_2)$，送$prel_i,A_1,A_2,r$给使用者。

3)收到所有$prel_i,A_1,A_2,r$后，使用者计算

$$g^{S_i}=g^{SK}(g^{a_1})^{id_1}\ldots(g^{a_{t-1}})^{id_i^{t-1}} \bmod N$$

分别验证$g^r(g^{S_i})^c=A_1$，$prel^r(prel_i)^c=A_2$，如等式成立，$prel_i$是有效的。

4)使用者计算

$$l_{id_i}(0)=\prod_{j=1,j\neq i}^{t}{}^{-id_j}\!\!\diagup\!\!_{id_i-id_j}，\quad license=\prod_{i=1}^{t}(prel_i)^{l_{id_i}(0)}=(prel)^{\sum_{i=1}^{t}S_il_{id_i}(0)}$$
$$=(prel)^{SK}=((license)^{PK})^{SK} \bmod N$$

5)从数字证书($license$)中得到加密密钥，解除数字内容的保护，使用数字内容。

1.2 Gu等人的方案的缺陷

Gu等人的方案存在合谋攻击，即当P2P网络中大于门限值t的LA合谋，就可以重新构造网络的秘密多项式函数$f(x)=SK+a_1x+\ldots+a_{t-1}x^{t-1}$（式(1)），得到网络的秘密参数，伪造其他LA签发数字证书，从而破坏了网络的数字内容保护机制。攻击方法如下：

t个LA互相泄漏各自的子密钥S_i，然后计算$f(x)=\sum_{i=1}^{t}S_i\prod_{j=1,j\neq i}^{t}-id_j/id_i-id_j$，从而重新构造了P2P网

基金项目：广东省自然科学基金资助项目(04300708)；暨南大学自然科学基金资助项目

作者简介：王晓明(1960－)，女，博士、教授，主研方向：密码学，计算机网络安全

收稿日期：2006-08-10 **E-mail：**wxmsq@eyou.com

络的秘密多项式函数 $f(x)=SK+a_1x+...+a_{t-1}x^{t-1}$（式(1)），这些恶意的LA就能计算发行者的密钥$SK$和任何其它LA的子密钥$S_l$，伪造其他LA签发数字证书，破坏P2P网络的数字内容保护机制。

2 本文的方案

假设P2P网络中存在很多可信节点，记为LA。设 p_1,p_2,p_1',p_2',q 为安全的大素数，且 $N=p_1p_2=(2qp_1'+1)(2qp_2'+1)$，阶为$q$的元素$g$ (即 $g^q=1 \bmod N$)，h是一个安全的Hash函数。设d和e分别为数字内容发布者的私钥和公钥，且满足 $gcd(e,\varphi(N))=1$，$ed=1 \bmod \phi(N)$，$\varphi(N)=(p_1-1)(p_2-1)$。每个节点$n_i$都有一对密钥 $(k_i,P_i=g^{k_i} \bmod N)$，其中，$k_i$为$n_i$的私钥；$P_i$为$n_i$公钥。 $D_{P_i}(E_{k_i}(x))\equiv x,\forall x$，其中，$E_{P_i}\{\cdot\}$和$D_{k_i}\{\cdot\}$分别代表加密和解密运算；$id_i$为$n_i$的身份标志。

2.1 数字证书的生成过程

(1)发布者对数字内容进行加密并将其散发至 P2P 网络，任何节点都可以复制此加密的数字内容。加密密钥为 x，加密算法采用 AES。

(2)生成含有加密密钥x和访问规则的数字证书$license$，并用 e 加密此数字证书，加密算法为 RSA[7]，即 $prel=(license)^e \bmod N$。

2.2 子密钥分发过程

将发布者的私钥 d 分成 n 个子密钥后，分发到 P2P 网络中 n 个可信任的 LA，即

(1)发布者选择n个LA、随机数w_l(l=1,2,…,m+1-t)和一个随机多项式

$$f(x)=a_0+a_1x+...+a_mx^m \tag{2}$$

计算

$$S_i=f(id_i) \bmod q(i=1,2,...,n)$$

$$z_j=prel^{[f(w_j)\prod_{l=1,l\neq j}^{m+1-t}-w_l/w_j-w_l]} \bmod N\ (j=1,2,...,m+1-t)$$

其中，$d=f(0)=\sum_{i=1}^{m}a_0$ 为网络的私钥；$y=g^d \bmod N$为网络的公钥。秘密送 S_i 每一个 LA$_i$(i=1,2,…,n)，公布 y, z_j(j=1,2,…,m+1-t)和 $\vartheta_\eta=g^{a_\eta} \bmod N\ (\eta=1,...,m)$。

(2)每个LA$_i$验证 $g^{S_i}=y\prod_{\eta=1}^{m}(\vartheta_\eta)^{ID_i^\eta} \bmod N$，如等式成立，子密钥$S_i$有效。

2.3 保护的数字内容使用过程

当使用保护的数字内容时，使用者必须获得 t（门限值）个 LA 签发的子数字证书，合成 t 个子数字证书得到数字证书，从而得到加密密钥 x。

(1)使用者向 LA 发出获得数字证书的请求。

(2)n 个 LA 中有 t 个同意签发子数字证书，即每个 $LA_i\in LA_t$ 选择随机数 α，计算 $prel_i=(prel)^{S_i} \bmod N$，$A_1=g^\alpha \bmod N$，$A_2=(prel)^\alpha \bmod N$，$c=h(g^{S_i},prel_i,A_1,A_2)$，$r=\alpha-cS_i \bmod q$，送 $prel_i,A_1,A_2,r$ 给使用者。

(3)收到所有 $prel_i,A_1,A_2,r$ 后，使用者首先计算

$$g^{S_i}=y\prod_{\eta=1}^{m}(\vartheta_\eta)^{ID_i^\eta} \bmod N$$

然后分别验证 $g^r(g^{S_i})^c \bmod N=A_1$，$prel^r(prel_i)^c \bmod N=A_2$，如等式成立，$prel_i$有效。

(4)使用者计算数字证书

$$license=\prod_{i=1}^{t}(prel_i)^{L_i(0)}[\prod_{j=1}^{m+1-t}(z_j)^{\prod_{l=1}^{t}-id_l/w_j-id_l}] \\ =((licese)^e)^d \bmod N \tag{3}$$

其中，$L_i(0)=[\prod_{l=1,l\neq i}^{t}-id_l/id_i-id_l][\prod_{l=1}^{m+1-t}-w_l/id_i-w_l]$。

(5)从数字证书中得到加密密钥 x，从而可以解除数字内容的保护，使用数字内容。

2.4 子密钥的更新过程

经过一定时间后，一些签发数字证书的子密钥S_i就有可能被攻击者获得，如果攻击者获得t（门限值）个子密钥，那么整个P2P网络的数字内容的保护机制就被破坏。因此，为了防止攻击者的攻击，应周期地更新签发数字证书的子密钥。

在一个新的周期开始前，每个LA$_i$应该完成以下步骤：

(1)选择随机多项式 $f_i'(x)=a_{i1}'x+...+a_{im}'x^m \bmod q$，其中，$0<a_{ij}'<q\ (j=1,...,m)$。计算 $f_i'(id_j)\ (j=1,2,...,n)$，并秘密发送 $f_i'(id_j)$ 给每个LA$_i$。公布

$$\vartheta_i'=g^{a_i\eta} \bmod N(\eta=1,...,m)$$

$$z'^i_j=prel^{[f_i'(w_j)\prod_{l=1}^{m+1-t}-w_l/w_j-w_l]} \bmod N\ (j=1,2,...,m+1-t)$$

(2)收到所有的 $f_i'(id_j)$ 后，LA$_i$ 分别验证 $g^{f_i'(id_j)}=\prod_{l=1}^{m}(\vartheta_i')^{id_j^l} \bmod N$，如等式成立，则计算签发数字证书的更新子密钥为 $\bar{S}_j=S_j+\sum_{i=1}^{n}f_i'(id_j) \bmod q$，计算

$$\bar{z}_j=z_j\prod_{i=1}^{n}z_j'^i=g^{f(w_j)\prod_{l=1,l\neq j}^{m+1-t}-w_l/w_j-w_l}g^{\sum_{i=1}^{n}f_i'(w_j)\prod_{l=1,l\neq j}^{m+1-t}-w_l/w_j-w_l} \\ =g^{\bar{f}(w_j)\prod_{l=1,l\neq j}^{m+1-t}-w_l/w_j-w_l} \bmod N\ (j=1,2,...,m+1-t)$$

其中，$\bar{f}(w_j)=f(w_j)+\sum_{i=1}^{n}f_i'(w_j)$。公布 $\bar{z}_j$，更新后的子密钥为 $\bar{S}_j=S_j+\sum_{i=1}^{n}f_i'(id_j) \bmod q$。

2.5 拥有子密钥 LA 的更改

当拥有子密钥的某个LA准备离开P2P网络时，该LA首先广播自己要离开的消息，推荐另一个LA'承担自己的审核权力，并告知其他n-1 个LA。如有t个LA同意，那么他们将联合授予子密钥给LA'，从而节点LA'就获得部分审核权利。而准备离去的LA$_i$只在这一周期内起作用，因为在下一周期，签发数字证书的子密钥已经更新，节点LA$_i$拥有的子密钥已经被废除。t个LA按以下方式授予子密钥给节点LA'：

(1)每个LA计算 $\tau_i=S_iL_i(id')+\lambda_i \bmod q$，并送 τ_i 给LA'。其中，λ_i是随机数，且 $\sum_{i=1}^{t}\lambda_i=0$，$L_i(id')=\prod_{l=1,l\neq i}^{t}\frac{id'-id_l}{id_i-id_l}$；$L_i(id')$ 是公共参数，为了防止从 $S_iL_i(id')$得到S_i，本文采用了文献[8]的方法，即加随机数 λ_i，每个LA'有一个秘密的随机数 λ_i，且 $\sum_{i=1}^{t}\lambda_i=0$。

(2)LA'收到所有 τ_i，计算

$$S'=\sum_{i=1}^{t}\tau_i=\sum_{i=1}^{t}(S_iL_i(id')+\lambda_i) \bmod q$$

验证

$$g^{S'}=\prod_{i=1}^{t}[y\prod_{\eta=1}^{m}(\vartheta_\eta)^{ID_i^\eta}]^{L_i(id')} \bmod N$$

如等式成立，LA'获得了签发数字证书的子密钥 S'，于是 LA' 就获得部分审核权力。

2.6 安全性的分析

(1)通过式(3)可以得到数字证书

证明

$$license=\prod_{i=1}^{t}(prel_i)^{L_i(0)}[\prod_{j=1}^{m+1-t}(z_j)^{\prod_{l=1}^{t}-id_l/w_j-id_l}] \\ =(prel^{\sum_{i=1}^{t}S_iL_i(0)})[prel^{\sum_{j=1}^{m+1-t}f(w_j)\prod_{l=1,l\neq j}^{m+1-t}-w_l/w_j-w_l\prod_{l=1}^{t}-id_l/w_j-id_l} \\ =(pewl)^d=((licese)^e)^d \bmod N$$

(2)更新子密钥后，P2P 网络的公钥不变

证明

因为

（下转第 32 页）