高效的动态组播群通信认证签字方案*

李先贤, 怀进鹏

(北京航空航天大学 计算机科学与工程系,北京 100083)

E-mail: lixx@cscw.buaa.edu.cn

http://www.buaa.edu.cn

摘要: 由于组播群组的动态性和数据传送的不可靠性,相对于点到点通信,组播通信的安全认证更为复杂.在组播数据发送源认证问题中,签字的速度和长度是实现认证的主要障碍.为了解决这个问题,通过引入新的认证技术——认证矩阵,提出了一个有效的适用于大数量动态的群组和不可靠数据传送的组播认证签字方案.相对于目前的组播包认证方案,该方案可显著地降低签字长度,提高签字速度,并可提供不可抵赖服务,可应用于如多媒体数据传输、多方会议以及远程教育等广泛的应用领域.

关键词: 组播通信;数字签字;安全认证

中图法分类号: TP393 **文献标识码**: A

近年来,基于IP组播技术的多方协作研究与应用迅速成为一类重要的分布式应用方向,例如,在网络多媒体数据传输、股票报价、多方会议以及远程教育等应用领域,组播通信为其提供了非常有效的传输方式.IP组播包通过组播分布树传送到多个接收者,组播分布树则是由一个组播路由协议[1]形成的,任何主机都可以通过群组管理协议(Internet group management protocol,简称IGMP)[1]动态地加入或退出一个群组,IP组播群组很容易通过分布树扩展为具有大量成员的群组,所以,分布树的易扩展性使IP组播模型成为当前一种非常有效的通信模型.然而,它同时给IP组播带来了许多安全问题,其中的一个瓶颈问题是组播通信中数据发送的可认证性.在点到点的通信中,可用公钥签字技术来实现认证性,然而,由于公钥签字算法的效率是相当低的,例如在200MHZ的PC机上,模为1024 bits RSA算法每秒只能产生约40个包的签字,而在组通信中需发送极大数量的数据包,对每个包用公钥签字显然是行不通的.因此,必须设计有效的签字算法.

本文首先简要介绍和分析了该领域已有的研究工作;然后,导入一种新的认证技术,提出了一个可以显著减少签字长度的优化签字方案,并深入研究了算法的安全性和复杂性;最后,分析和证明了本文提出的签字方案的效率及其特点.本文未特别说明的概念和术语与文献[2]一致.

1 国内外相关研究工作

在网络数据传输的可靠性可以得到保证的前提下,R.Gennaro等人[3]提出流签字(stream signature)的技术签署多数量消息,在这个方案中,每一条链只需对开始的包用公钥算法签字,链内的每个包含有下一个包的密码杂凑值,用于验证下一个包.这对可靠网络传输协议(如TCP/IP)是一个很好的方案.然而,由于这个方案不能容许一个包丢失,而组播通信难以保证可靠性,所以这个方

* 收稿日期: 2000-07-26; 修改日期: 2001-03-05

基金项目: 国家自然科学基金资助项目(60073006);国防预研基金资助项目(00J16.5.4.HK0135);国防基础科研基金资助项目(JI300B004);北京市科技新星计划资助项目(952874000)

作者简介: 李先贤(1969-),男,广西桂林人,博士生,讲师,主要研究领域为网络安全;怀进鹏(1962-),男,山东济南人,博士,教授,博士生导师,主要研究领域为人工智能,协同工作,网络安全.

案不适用于不可靠的组通信应用环境.文献[4]改进了流签字技术,可部分地解决包丢失问题,然而还需要在每个包上附加过多消息以用于认证,因而效率不高.

Canetti 等人[5]引入了另一种认证技术——非对称 MAC(message authentication code)认证,用于解决组播源认证问题.它的基本思想是发送者拥有一定数量的密钥,将这些密钥分成一些子集,发送者与每个接收者分别共享这些密钥的子集,发送者用所有的密钥计算消息的 MAC 值,附加在消息上传送,而每个接收者用他所拥有的密钥验证相对应的 MAC 部分.如果一个接收者不知道其他接收者的密钥,则无法伪造 MAC 进行欺骗.然而,这个方案还存在如下几个问题:首先,当有足够数量的接收者勾结起来,可以欺骗其他接收者时,要求发送者计算的 MAC 密钥数是可互相勾结的最大数的线性函数,所以这个方案只适用于较小的群组;其次,发送者将这些密钥子集分配给每个接收者本身是需要解决的问题,特别是在动态群组中增加了不安全因素;第 3,这个签字方案没有提供非抵赖服务,注意到每一个接收者由于能产生自己所能认证的合法 MAC,从而没有证据向第三方证明发送者发送过的消息.

Pankaj 等人[6]采用在线、离线计算相结合的办法,利用一次性公钥数字签字技术,提出了一个快速、简洁的组播通信包认证签字方案.文献[6]中所提方案的基本思想是:发送者首先离线计算产生大量一次性公钥签字密钥对,并用发送者的长期公钥(如 RSA 公钥)对每对一次性密钥的公钥部分签字,将其缓存备用,在发送消息时,用一次性私钥消息进行签字,而将所存储的一次性公钥以及对它的签字附加在发送的消息上用于验证.这个方案将公钥签字较高的费用离线计算,解决了在线签字的速度问题,并适用于大数量动态的群组,应用 TCR(target collision resistance)函数可压缩签字的长度,具有一定的实用价值.但这个方案最主要的问题在于:没有解决验证签字的速度问题,由于接收者必须用发送者的长期公钥去验证每个包的一次公钥的合法性(这个费用是相当高的),而且计算只能在线并行计算,耗费接收主机大量的计算资源,以致极易受到拒绝服务这一类型的攻击;这个方案另一潜在的安全问题是:发送者用长期公钥对大量的一次密钥对签字,当接收者可以掌握这些一次密钥对的私钥时,则可以冒充发送者的身份发送消息.

2 高效的组播认证方案

流签字是一个非常有效的方案,它的问题在于不能用于有包丢失的通信.这里,我们将引入一种新的认证算法以代替通常的 Hash 函数,从而得到一个高效的组播认证方案(efficient multicast authentication scheme,简称 EMAS),以用于不可靠的网络通信认证,并且可提供抗抵赖服务.下面首先介绍一种认证算法.

2.1 认证矩阵

我们首先介绍几个常用的概念:

抗碰撞函数(target collision resistance functions)[6]:称一个可有效计算函数 $H:M\to\{0,1\}^l$ 是抗碰撞的,如果对选取的 $m_0\in M(M\subseteq\{0,1\}^*$,任何攻击者都可以找到 $m\neq m_0$,使得 $H(m)=H(m_0)$的概率可忽略.例如,通常的 Hash 函数和 MAC 函数都属于这一类函数.

伪随机函数(pseudo-random functions)[7]:伪随机函数是由 Goldreich,Goldwasser 和 Micali 引入到密码学中来,是现代密码学的基础,在密码学中起着重要的作用.然而,这里先讨论一类只有一个比特输出的伪随机函数——称为单比特伪随机函数(具有比 Hash 函数更快的运算速度[7]).

假设 $F=\{f_i\}_{i\in A}$是伪随机函数族,其中,每个 $f_i:M\to\{0,1\}$是单比特伪随机函数,那么具有以

下性质:

(1) 对 $\sigma\in M$,设 $\Pr(f(\sigma)=f(\sigma'))$表示多项式能力攻击者可选取 $\sigma'\in M$ 使得 $\sigma\neq\sigma'$并且 $f_i(\sigma)=f_i(\sigma')$的概率,则有 $\Pr(f(\sigma)=f(\sigma'))<\frac{1}{2}+\varepsilon$,这里,$\varepsilon$可忽略.

(2) 对任何 $i\neq j$,函数 f_i 与 f_j 不相关.

记号. 令 f 是由 M 到$\{0,1\}$的伪随机函数,记 $f(x,y)=f(x|y)$,$x,y\in M$,这里,"|"表示并接.

定义 2.1. 设 $x_1,x_2,\ldots,x_n,y_1,y_2,\ldots,y_m\in M$,$F=\{f_{ij}\}$是上述的单比特伪随机函数簇,我们如下规定"矩阵乘法运算"函数 F:

$$F\left(\begin{Bmatrix}x_1\\x_2\\\vdots\\x_n\end{Bmatrix}(y_1\quad y_2\quad\ldots\quad y_m)\right)=\begin{Bmatrix}f_{11}(x_1,y_1) & f_{12}(x_1,y_2) & \ldots & f_{1m}(x_1,y_m)\\ f_{21}(x_2,y_1) & f_{22}(x_2,y_2) & \ldots & f_{2m}(x_2,y_m)\\ \vdots & \vdots & \vdots & \vdots\\ f_{n1}(x_n,y_1) & f_{n2}(x_n,y_2) & \ldots & f_{nm}(x_n,y_m)\end{Bmatrix}$$

简记作 $F(X,Y)$. 这里,$X=(x_1,x_2,\ldots,x_n)$,$Y=(y_1,y_2,\ldots,y_m)$.

定理 2.1. $F=\{f_{ij}\}$是如定义 2.1 中所描述的单比特伪随机函数簇,并如定义 2.1 中规定相应的函数. 令$C=(c_{ij})_{n\times m}$是布尔矩阵,$c_{ij}\in\{0,1\}$,那么对任何多项式计算能力攻击者,可求出 $\alpha=(a_1,a_2,\ldots,a_n)$和 $\beta=(b_1,b_2,\ldots,b_m)$,$a_i,b_j\in M$,使得 $F(\alpha,\beta)=C$ 的概率可以忽略.

证明:伪随机函数 F 的性质,意味着对多项式计算能力主体只能通过试验求出 $X=(x_1,x_2,\ldots,x_n)$和 $Y=(y_1,y_2,\ldots,y_m)$使得 $F(X,Y)=C$. 为便于表示,令 $w=1/2+\varepsilon$,不失一般性,假设 $n\leqslant m$,那么只需证明当攻击者试验次数为 l,则成功概率 $q\leqslant lw^n$,即证明了本定理. 显然,攻击者试验 1 次,可以看做是选取 X_0,Y_0,验证 $F(X_0,Y_0)-C$ 是否成立. 假设事件 A_s 表示攻击者第 s 次试验成功,即选取 $X^s=(x_1^s,x_2^s,\ldots,x_n^s)$,$Y^s=(y_1^s,y_2^s,\ldots,y_m^s)$使得 $F(X^s,Y^s)=C$ 成立. 那么,当试验次数为 l 时,至少有 1 次成功的概率为 $q=\sum_{s=2}^{l}Pr(A_s|\neg A_{s-1},\ldots,\neg A_1)+Pr(A_1)$. 由函数 f_{ij}的随机性,显然有 $Pr(A_1)=w^{mn}$. 下面,我们只需证明:$Pr(A_s|\neg A_{s-1},\ldots,\neg A_1)\leqslant w^n$,则有 $q<(l-1)w^n+w^{mn}\leqslant lw^n$.

注意到第 s 次试验与前面的试验事件不是互相独立的,必须考虑事件 A_s 与$\neg A_{s-1},\ldots,\neg A_1$ 的关系. 由伪随机函数 f_{ij}的性质可知,在第 s 次试验中,如果攻击者选取的(x_i^s,y_j^s)在前面的试验中没有出现,即$(x_i^s,y_j^s)\neq(x_i^t,y_j^t)(t<s)$,那么使得 $f_{ij}(x_i^s,y_j^s)=c_{ij}$成立的概率为 w,记作 $Pr(f_{ij}(x_i^s,y_j^s)-c_{ij})=w$. 现在我们分两种情形进行讨论:

(1) 若在 $x_1^s,\ldots,x_n^s,y_1^s,\ldots,y_m^s$ 中至少有一个变量 x_i^s(或 y_j^s)在以前试验中没有出现,这时 $f_{i1}(x_i^s,y_1^s),\ldots,f_{im}(x_i^s,y_m^s)$在前面的试验中没有被计算,故 $Pr(f_{i1}(x_i^s,y_1^s)=c_{i1})=w,\ldots,Pr(f_{im}(x_i^s,y_m^s)-c_{im})=w$,从而得到

$$Pr(A_s,\neg A_{s-1},\ldots,\neg A_1)\leqslant Pr(f_{i1}(x_i^s,y_1^s)=c_{i1})\ldots Pr(f_{im}(x_i^s,y_m^s)=c_{im})=w^m\leqslant w^n.$$

对于 y_j^s 有完全类似的结果.

(2) 否则假设 $x_1^s=x_1^{t_1},\ldots,x_n^s=x_1^{t_n},y_1^s=y_1^{k_1},\ldots,y_m^s=y_m^{k_m}$,其中 $t_i,k_j<s$. 首先,这些正整数 $t_1,\ldots,t_n,k_1,\ldots,k_m$ 不能全部相等,否则,假设都等于 $t(<s)$,则 $X^s=X^t,Y^s=Y^t$,即重复了第 t 次试验,从而有 $Pr(A_s|\neg A_{s-1},\ldots,\neg A_1)=0$.

① 若 $k_1=k_2=\ldots=k_m$,那么至少有一个 t_i,使得 $t_i\neq k_1,\ldots,t_i\neq k_m$,故在前 $s-1$ 次试验中没有

出现过$(x_i^s,y_1^s)=(x_1^{t_1},y_1^{k_1}),\ldots,(x_i^s,y_m^s)=(x_1^{t_1},y_1^{k_m})$,由$F=\{f_{ij}\}$的性质有:$Pr(f_{i1}(x_i^s,y_1^s)=c_{i1})=w,\ldots,Pr(f_{im}(x_i^s,y_m^s)=c_{im})=w$,故

$$Pr(A_s|\neg A_{s-1},\ldots,\neg A_1)\leqslant Pr(f_{i1}(x_i^s,y_1^s)=c_{i1})\ldots Pr(f_{im}(x_1^s,y_m^s)=c_{im})=w^m\leqslant w^n;$$

② 若$k_1,k_2,\ldots,k_m$不都相等,那么对任何$t_i,i=1,\ldots,n$,必存在$k_{r_i}\in\{k_1,\ldots,k_m\}$使得$t_i\neq k_{r_i}$,$r_i\in\{1,\ldots,m\}$,因此,$(x_1^s,y_{r_1}^s)=(x_1^{t_1},y_{r_1}^{k_{r_1}}),\ldots,(x_n^s,y_{r_n}^s=(x_n^{t_n},y_{r_n}^{k_{r_n}})$在前$s-1$次试验中没有出现,那么有$Pr(f_{1r_1}(x_1^s,y_{r_1}^s)=c_{1r_1})=w,\ldots,Pr(f_{nr_n}(x_n^s,y_{r_n}^s)=c_{nr_n})=w$,故有

$$Pr(A_s\ \neg A_{s-1},\ldots,\neg A_1)\leqslant Pr(f_{1r_1}(x_1^s,y_{r_1}^s)=c_{1r_1})\ldots Pr(f_{nr_n}(x_n^s,y_{r_n}^s)=c_{nr_n})=w^n.$$

综上所述,无论哪一种情形,都有$Pr(A_s\ \neg A_{s-1},\ldots,\neg A_1)\leqslant w^n$,证明完成.

推论 2.1. 在定理 2.1 的假设下,设$\alpha=(a_1,a_2,\ldots,a_n)$,$\beta=(b_1,b_1,\ldots,b_m)$,其中$a_i,b_j\in M$,$C=F(\alpha,\beta)$,那么对任何多项式攻击者求$X=(x_1,x_2,\ldots,x_n)$和$Y=(y_1,y_2,\ldots,y_m)$,并且$X\neq\alpha$或$Y\neq\beta$使得$F(X,Y)=C$的概率可忽略,因此,$F$是抗碰撞函数.

证明:由对定理 2.1 的证明过程得出推论 2.1 是很容易的,这里不再详细证明.

定义 2.2. 在上述推论中,称矩阵$C=(c_{ij})_{n\times m}$是消息$a_1,a_2,\ldots,a_n,b_1,b_2,\ldots,b_m$的认证矩阵.

为了保证认证矩阵的安全性,必须保证自然数$N_0(=\min\{n,m\})$足够大,N_0的选取根据应用中假设攻击者具有的计算能力而定,称N_0为认证矩阵的安全基数.安全基数为N_0的认证矩阵相当于N_0比特输出的 Hash 函数的安全性.通常认为 80 是相当安全的,在要求较强安全性的应用中,N_0选取 128 或更多.

认证矩阵有以下性质:

设C是消息$a_1,a_2,\ldots,a_n,b_1,b_2,\ldots,b_m$的认证矩阵,若剩余消息集为$\{a_{i_1},\ldots,a_{i_s},b_{j_1},\ldots,b_{j_t}\}$,其中$\{i_1,\ldots,i_s\}\subseteq\{1,2,\ldots,n\}$,$\{j_1,\ldots,j_t\}\subseteq\{1,2,\ldots,m\}$,那么只需$i_s\geqslant N_0$且$j_t\geqslant N_0$,同样可以安全地进行认证.我们将利用这个性质解决传输中包丢失的问题.

注记.可用单比特输出的 MAC 函数$f_{e_{ij}}$(e_{ij}是一个 MAC 密钥)代替单比特伪随机函数f_{ij},显然,单比特 MAC 函数簇$F=\{f_{e_{ij}}\}$(e_{ij}互不相同)也具有上述性质.

2.2 EMAS 的描述

利用第 2.1 节中的认证矩阵,构造一个高效的组播源认证方案 EMAS.我们先来规定一些符号:

- H表示抗碰撞 Hash 函数,输出值为 80 bits(或 128 bits).
- 消息发送者A有一个公开密钥证书,$SK_A(PK_A)$分别是相应的私钥(公钥),如 RSA.
- $F=\{f_{ij}\}_{1\leqslant i\leqslant n,1\leqslant j\leqslant m}$是一个函数簇,其中每个$f_{ij}:M\to\{0,1\}$是单比特输出的 MAC 函数.$F$对所有接收者公开.
- N_0是如前所述的安全基数,例如取$N_0=80$(或 128),这根据具体应用而定.

基本思想是:消息发送者将要发送的消息包划分为一些链,而每条链由消息块组成.一条链可记为$M=\bigcup_{i=1}^{l}P_i$,其中每个$P_i=\{p_{ij}|j=1,\ldots,n\}$是发送包的集.适当地选取$n,l$的大小,可具有很高的概率,使得每一个消息块乘余的包不少于N_0,在下一节中我们将具体讨论相关内容,这里只讨论签字和验证的算法,而不给出具体的实现细节.

对任意一条链$M=\bigcup_{i=1}^{l}P_i,P_i=\{p_{ij}|j=1,\ldots,n\}$,给每一个包$p_{ij}$编号为$(i,j)$.

签字产生

(1) 首先,对每个 $p_{ij}\in P_i$ 计算 $k_{ij}=H(p_{ij})$, $j=1,\ldots,n$,则 k_{ij} 是 p_{ij} 的认证信息,附加在包 p_{ij} 上传送;

(2) 对所有 $1\leqslant i\leqslant l-1$ 和 $1\leqslant j\leqslant n$,计算 $c_{rj}^i=f_{ri}(k_{i+1,r},p_{ij})$, $p_{ij}\in P_i$, $r=1,2,\ldots,n$;令 $k_{ij}=(c_{1j}^i|c_{2j}^i|\ldots|c_{nj}^i)\in\{0,1\}^n$, k_{ij} 是 p_{ij} 的认证信息,附加在 p_{ij} 上;

(3) 用 A 的私钥计算签字 $S_{1j}=Sig_A(k_{1j})$, $j=1,\ldots,n$,附加在 p_{1j} 上传送.

签字验证

假设接收到的消息为 $M'=\bigcup_{i=1}^{l}P'_i$, $P'_1=\{p'_{1j}=(p_{1j},k_{1j},s_{1j})\}$, $P'_i=\{p'_{ij}=(p_{ij},k_{ij})\}(i=2,\ldots,l)$, i,j 是包的编号, k_{ij} 是包 p_{ij} 的认证信息, s_{1j} 是 k_{1j} 的签字.首先,若检查存在 P'_i 的包少于 N_0,则认证失败.否则,执行下面的步骤:

(1) 对每个 j,用 A 的公钥验证 $Ver_{PK_A}(k_{1j},s_{1j})=T$ 是否合法;

(2) 令 $J_i=\{j|$存在 $p_{ij}\in P'_i\}$, $1\leqslant i<l$.验证等式 $(k_{ij})_r=f_{ri}(k_{i+1,r},p_{ij})$ 对所有 $j\in J_i$, $r\in J_{i+1}$ 是否成立,这里, $(k_{ij})_r$ 表示 k_{ij} 的第 r 比特;

(3) 对所有 $j\in J_l$ 验证 $k_{lj}=H(p_{lj})$.

如果上面所有验证都通过,则认为所有消息为真.

正确性

只需进行简单检验,方案的正确性是显然的,这里不再详细讨论.

2.3 安全性分析

设 $A=(a_{ij})_{n\times m}$ 是 $n\times m$ 矩阵,集合 $I=\{i_1,i_2,\ldots,i_s\}\subseteq\{1,2,\ldots,n\}$, $J=\{j_1,j_2,\ldots,j_t\}\subseteq\{1,2,\ldots,m\}$,用 $A_{I,J}$ 记第 r 行、第 v 列元素为 a_{i_r,j_v} 的矩阵,即 $A_{I,J}=(a_{ij})_{i\in I,j\in J}$.

定理 2.2. 在EMAS中,任何一个不知道 A 的私钥的主体可伪造消息 m,使得接收者作为真实消息接受的概率可忽略,即EMAS是一个安全认证方案.

证明:在EMAS中,只需证明对任何 $m\notin M$,这里, $M=\{p_{ij}\ j=1,\ldots,n,i=1,\ldots,l\}$,任何多项式的计算能力主体可以使 m 通过EMAS中的验证的概率可忽略.

使用第2.2节中的符号,令 $J_i=\{j_1^{(i)},j_2^{(i)},\ldots,j_{N_i}^{(i)}\}$, $i=1,\ldots,l$, $|J_i|=N_i\geqslant N_0$; α_i 和 $(p_{i,j_1^{(i)}},p_{i,j_2^{(i)}},\ldots,p_{i,j_{N_i}^{(i)}})$ 和 $\kappa_i=(k_{i,j_1^{(i)}},k_{i,j_2^{(i)}},\ldots,k_{i,j_{N_i}^{(i)}})$,这里,每个 $k_{i,j_r^{(i)}}$ 是附加在 $p_{i,j_r^{(i)}}$ 上的认证信息.令

$$\beta_i=\begin{pmatrix}(k_{i,j_1^{(i)}})_{j_1^{(i+1)}} & (k_{i,j_2^{(i)}})_{j_1^{(i+1)}} & \ldots & (k_{i,j_{N_i}^{(i)}})_{j_1^{(i+1)}}\\ (k_{i,j_1^{(i)}})_{j_2^{(i+1)}} & (k_{i,j_2^{(i)}})_{j_2^{(i+1)}} & \ldots & (k_{i,j_{N_i}^{(i)}})_{j_2^{(i+1)}}\\ \vdots & \vdots & \vdots & \vdots\\ (k_{i,j_1^{(i)}})_{j_{N_{i+1}}^{(i+1)}} & (k_{i,j_2^{(i)}})_{j_{N_{i+1}}^{(i+1)}} & \ldots & (k_{i,j_{N_i}^{(i)}})_{j_{N_{i+1}}^{(i+1)}}\end{pmatrix}$$

是一个 $N_{i+1}\times N_i$ 的矩阵, $(k_{i,j_r^{(i)}})_{j_r^{(i+1)}}$ 表示 $k_{i,j_r^{(i)}}$ 的第 $j_r^{(i+1)}$ 比特,在EMAS中验证其合法性意味着:

$$\beta_1=F_{J_2,J_1}(\kappa_2,\alpha_1),\beta_2=F_{J_3,J_2}(\kappa_3,\alpha_2),\ldots,\beta_{l-1}=F_{J_l,J_{l-1}}(\kappa_l,\alpha_{l-1}),$$

其中 β_i 是消息组 (κ_{i-1},α_i) 的认证矩阵,注意到 β_i 是 κ_i 的一个子矩阵,因而由 κ_i 可惟一确定. $Ver_{PK_A}(k_{1,j},s_{1j})=T$ 意味着每个 $k_{1,j_r^{(1)}}$ 被伪造的概率可忽略,从而有 κ_1 被伪造概率可忽略, β_1 是同样的.因为 $|J_2|,|J_1|\geqslant N_0$,由推论2.1可知, F_{J_2,J_1} 是抗碰撞函数,故 α_1,κ_2 被伪造的概率可忽略,而 β_2 由 κ_2 惟一确定,如此继续下去, $\alpha_2,\ldots,\alpha_{l-1}$ 和 κ_2 被伪造概率可忽略,又由于 $\kappa_l=(H(p_{l,j_1^{(l)}}),\ldots,$

$H(p_{t,j_{N_j}^{(t)}})$),由 Hash 函数 H 的安全性可知,每个 $p_{t,j_t^{(t)}}$ 只有可忽略的概率被伪造.这样就证明了EMAS的安全性. □

不可抵赖性

在EMAS方案中,对消息的签字由发送者的公钥签字和认证矩阵抗碰撞性保证其真实性,前面讨论过它们都能阻止伪造和抵赖,且任何第三方均可验证它的真实性,同时由安全性分析我们看到,除了发送者以外,任何人(包括合法接收者)都不能伪造或篡改消息,因此接收者可以通过出示消息的签字来证明发送者确实发送过这些消息,即是不可抵赖的.

3 EMAS方案的实现与效率分析

EMAS方案的效率由块的大小以及链的长度来确定,而块的大小由网络失包率和安全基数决定,我们首先给出分块大小、链的长度以及失包率之间的一些关系.为了方便叙述,首先假设每个包的丢失率是独立的,则有以下定理:

定理 3.1. 设一个有 n 个消息的块通过包丢失率为 $p(0\leqslant p<1)$的网络传送,则接收者收到这个块消息的个数小于 $N_0(n)$的概率为 $\sum_{k=n-N_0+1}^{n} C_n^k p^k (1-p)^{n-k}$,从而 l 个这样的分块经由丢失率为 p 的网络传送,至少有一个块的剩余消息数少于 N_0 的概率为 $q=1-(1-u)^l$,这里,$u=\sum_{k=n-N_0+1}^{n} C_n^k p^k (1-p)^{n-k}$,从而有 $l\leqslant \ln(1-q)/\ln(1-u)$.

证明:每个包的丢失概率互相独立,故符合二项式概率分布,定理 3.1 的结论是显然的.

注意到,在网络传输中,包的丢失概率不是互相独立的,因此对一个消息链 $M=\bigcup_{i=1}^{l} P_i$,$P_i=\{p_{ij}\mid j=1,\ldots,n\}$不必按顺序 $p_{11},p_{12},\ldots,p_{1n},p_{21},\ldots,p_{2n},\ldots,p_{ln}$发送包,可以按 $p_{11},p_{21},\ldots,p_{l1},p_{12},p_{22},\ldots p_{l2},p_{1n},\ldots,p_{ln}$的顺序发送.这样,对于每个块 P_i 中的包的丢失率可视为相等的.

例如,设 $M=\bigcup_{i=1}^{l} P_i(P_i=\{p_{ij}\mid j=1,\ldots,n\})$是消息链.表 1 的数据部分说明了包丢失率、链的长度和块大小之间的关系.表中数据根据定理 3.1 估算,其中 N_0 是安全基数,p 是包丢失率,q 是认证失败概率.

Table 1 The failing verification probability with different loss probability

表 1 对不同失包率认证失败概率比较

N_0	p	n	l	q
100	0.4	256	1 000	4.85×10^{-9}
128	0.3	232	1 000	6.86×10^{-4}
128	0.3	200	1 000	4.72×10^{-5}

我们看到,当 $n\leqslant256$,$l\leqslant2^{10}=1024$,这在失包率不大于 40% 的网络通信中已经可以保证足够的安全性($N_0\geqslant100$),且会有极高验证概率(即 q 非常小).这样,用 18 bits 可以给所有数据包编号,故每条链的包(消息)数不应超过 2^{18},下面我们分析方案 EMAS 的实现效率.

用 C 记每个附加消息量(包括认证信息和编号),a 是单比特输出伪随机函数 f_{ij} 完成 1 次运算所需要的时间,而 b 是公钥产生 1 个签字的时间,d 是公钥验证 1 个签字所需时间,则

签字长度为

$$C=n+18\text{ bits};$$

签字平均速度为

$$R_S=\frac{nl}{n^2(l-1)a+na+nb}=\frac{l}{n(l-1)a+a+b}(\text{packets/s});$$

验证平均速度为

$$R_S=\frac{nl}{n^2(l-1)a+na+nd}=\frac{l}{n(l-1)a+a+d}(\text{packets/s}).$$

例:在200MHZ的PC上,对64 bytes的包,单比特伪随机函数产生一个比特认证信息的时间约为$a=1/500000$秒,RSA公钥产生一个签字的时间约为$b=1/40$秒,RSA验证一个签字的时间约为$d=1/30000$秒.表2中给出了EMAS实现费用的相关数据,其中p表示网络失包率,块大小为n,N_0是安全基数,l为链长,q表示可成功认证的概率,C表示附加信息长度,T_S和T_V分别表示签字产生和验证的速度.

Table 2 Performance parameters of EMAS

表2 EMAS的实现效率

p	N	l	N_0	q	C (bits)	T_S(bytes/s)	T_V(bytes/s)
0.3	160	500	80	$1-1.97\times10^{-5}$	178	≈2700×64	≈3100×64
0.3	200	500	100	$1-5.45\times10^{-7}$	218	≈2380×64	≈2500×64
0.2	128	500	80	$1-7.2\times10^{-4}$	146	≈3270×64	≈3910×64
0.1	112	500	80	$1-4.1\times10^{-6}$	130	≈3655×64	≈4470×64

4 实用的组播认证方案

从上述结果可以看出,使用单比特输出的伪随机函数只需每个包附加很少的认证信息,几乎没有剩余信息.但另一方面,每条链的包数量较多,这使得实现中需进行较多的缓存.用多比特输出的MAC函数(例如10bits的MAC函数)替代EMAS中的单比特伪随机函数,可以得到一个较为实用的组播认证方案,我们称之为PMAS(practical multicast authentication scheme).PMAS的安全性分析完全类似于对EMAS的相应分析,限于篇幅,这里不再赘述.

PMAS的签字产生和验证算法完成类似于EMAS的相应算法.设$F=\{f_{ij}\}$是由k比特输出的MAC函数组成的簇,类似地,$M=\bigcup_{i=1}^{l}P_i(|P_i|=n)$是消息链,$N_0$是安全基数,那么每个块$P_i$只需剩余消息数不少于$N_0/k$,即可进行验证,因此可降低每个块的包数量,提高签字速度,但也因此增加了签字长度.适当地选取MAC函数的输出长度k,可使方案具有较高的效率,k的选取应根据具体应用环境而定.

例:当选取10bits输出的伪随机函数时,表3给出PMAS的实现数据,相应的实现参数以及符号的含义与表2相同(注:由于减少了链的消息数,只需12bits用于编号,故附加在每个包的消息总量为$C=10n+12$).

Table 3 Performance parameters of PMAS

表3 PMAS的实现效率

p	N	l	N_0	q	C (bits)	T_S(bytes/s)	T_V(bytes/s)
0.3	24	100	80	$1-4.39\times10^{-3}$	252	≈3360×64	≈2280×64
0.2	20	100	80	$1-1.52\times10^{-3}$	212	≈3450×64	≈25000×64
0.1	16	100	80	$1-5.92\times10^{-4}$	172	≈3550×64	≈31200×64

相关结果效率

文献[6]所提出的在线/离线方案需附加每个包的认证信息总长度至少为280bytes=2240 bits;而在400MHZ的处理器上,签字(验证)运算的平均速度(包括离线/在线时间)仅为410包/秒,并且这个方案必须花费存储空间用于保存一次性密钥,这也增加了系统的不安全性,因此本

文提出的方案可以显著地提高效率.

文献[5]中提出的"不对称MAC"方案,在较好的情况下,秘密泄露接收者不超过10个,在损失一些安全性的条件下,用总数为760个MAC密钥签字,签字长度为760bits,签字速度为660包/秒,验证速度可达6 600包/秒,而当需要较强的安全性时,签字长度则需1 900bits,并且这个方案的签字长度是接收者数的线性函数,因此不能用于大群组通信.

5 结 论

本文提出了组播认证签字方案EMAS和PMAS.这些该方案可用于安全工作流签字以及其他需要处理大批量消息的组签字的应用.由前面的分析可以看出,这些方案具有如下特点:

(1) 高效率.这是EMAS(PMAS)方案最为显著的特点,由前面的分析可以看出,EMAS中附加到每个包的认证信息长度不到文献[6]中方案的1/10,而签字速度却提高了,这在组播通信中是极为重要的,因为在不可靠的网络中传送数据,IP包不能过大,较短的签字长度节约了宝贵的消息空间和带宽,因此这个方案在速度和签字带宽消耗方面都有显著的改善.PMAS用于签字的长度比EMAS稍大,但是却有更快的签字速度,且极大地减少了延缓验证时间,是更为实用的有效的方案.

(2) 安全性.EMAS和PMAS的安全性基于公钥签字算法的安全性和"认证矩阵"的安全性,由前面的安全性分析可以看到,"认证矩阵"基于伪随机函数,可通过加大每组消息数来加强安全性,因此,可根据实际应用确定很强的安全强度,代价是损失了一些效率,然而,在很强的安全性下仍可保证相对目前方案来说有较快的速度和较短的签字长度.EMAS和PMAS无须秘密共享与群密钥管理安全性无关.

(3) 不可抵赖性.在EMAS和PMAS方案中,即使所有接收者勾结也无法伪造签字,并验证算法可公开,故可提供不可抵赖安全需求.

(4) 广泛的适用性.EMAS和PMAS方案均可用于大数量的动态组播群组,可快速地对任意多数量的数据包进行批量签字,并可用于不可靠的网络环境,因此适用于目前大多数的分布式网络环境,具有很好的实用价值.

References:

[1] Deering, S. Host extensions for IP multicasting. Technical Report, RFC 1112, IETF, 1989.

[2] Bruce, Schneier, Translated by Wu, Shi-zhong, *et al.* Applied Cryptography: Protocols, Algorithms, and Source Code in C. Beijing: China Machine Press, 2000 (in Chinese).

[3] Gennaro, R., Rohatgi, P. How to sign digital streams. In: Burton, S., Kaliski, Jr. eds. Advances in Cryptology-CRYPTO'97. Berlin: Springer-Verlag, 1997. 180~197.

[4] Wong, C.K., Lam, S. Digital signatures for flows and multicasts. Technical Report, TR-98-15, Department of Computer Sciences, The University of Texas at Austin, 1998.

[5] Canetti, R., Garay, J., Itkis, G., *et al.* Multicast security: a taxonomy and some efficient constructions. In: IEEE Staff ed. Proceedings of the IEEE INFOCOM'99. New York: IEEE Communication Society, 1999. 708~716. http://www.research.ibm.com/security/publ.html.

[6] Pankaj, Rohatgi. A compact and fast hybrid signature scheme for multicast packet authentication. In: Proceedings of the 6th ACM Computer and Communications Security Conference. Singapore: ACM Press, 1999. 93~100. http://www.acm.org/pubs/articles/proceedings/commsec.

[7] Moni, Naor, Omer, Reingold. From unpredictability to indistinguishability: a simple construction of Pseudo-Random functions from MACs. In: Krawczyk, H., ed. Advances in Cryptology-Crypto'98. Berlin: Springer-Verlag, 1998. 267~282.

附中文参考文献：

[2] Bruce, Schneier, 吴世忠, 等译. 应用密码学：协议、算法与C源程序. 北京：机械工业出版社, 2000.

Efficient Authentication Signature Schemes for Dynamic Multicast Groups*

LI Xian-xian, HUAI Jin-peng

(*Department of Computer Science and Engineering, Beijing University of Aeronautics and Astronautics, Beijing* 100083, *China*)

E-mail: lixx@cscw.buaa.edu.cn

http://www.buaa.edu.cn

Abstract: Maintaining authenticity for multicast communication is inherently more complex than for unicast, which dues to the dynamic group and unreliable delivery. In the implementation of multicast authentication, the major obstacles lie on the lower signature rate and larger signature size overhead. To solve this problem, by using a new authentication technique called authentication matrix, a new signature scheme is proposed for large and dynamic multicast groups that can be used on the unreliable delivery network. Comparing with the existing schemes, in this scheme, the signature size overhead is much smaller and the signature rate is much higher, and it can provide the non-repudiation serve. It should have applications in many practical fields such as multimedia data transmission, live multi-party conferencing and long-distance education.

Key words: multicast communication; digital signature; secure authentication

* Received July 26, 2000; accepted March 5, 2001

Supported by the National Natural Science Foundation of China under Grant No. 60073006; the National Defence Advance Research Foundation of China under Grant No. 00J16.5.4.HK0135; the National Defence Fundamental Science Foundation of China under Grant No. JI300B004; the Science and Technology Nova Project of Beijing of China under Grant No. 952874000