有扰信道下基于门限密码的链式组播源认证技术

黎剑兵*[①] 李 庆[②] 董庆宽[②] 李小平[①]
[①](西安电子科技大学空间科学与技术学院 西安 710126)
[②](西安电子科技大学综合业务网国家重点实验室 西安 710071)

摘 要：组播是一种被广泛应用的通信技术。组播源认证是组播安全中的重要问题，特别是在有扰信道中实现组播源认证具有很大的挑战性。该文提出一种基于门限密码的链式组播源认证技术，以解决有扰信道上的组播源认证问题。基于组播源认证的安全需求和 Dolev-Yao 模型，该文首先给出链式组播源认证的安全假设和安全模型；然后结合 Shamir 的门限秘密共享技术，设计一种适合于有扰信道的组播源认证协议并进行了安全性分析。对协议的仿真结果表明，该文设计的组播源认证在保证较好的通信性能前提下具有良好的抗丢包能力。

关键词：网络安全；组播；组播源认证；门限密码；安全模型
中图分类号： TP393.08 **文献标识码**： A **文章编号**：1009-5896(2015)05-1227-07
DOI: 10.11999/JEIT140884

A Chained Multicast Source Authentication Technology Based on the Threshold Cryptography in A Noisy Channel

Li Jian-bing[①] Li Qing[②] Dong Qing-kuang[②] Li Xiao-ping[①]
[①](*School of Aerospace Science and Technology*, *Xidian University*, *Xi'an* 710126, *China*)
[②](*State Key Laboratory of Integrated Services Networks*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: Multicast is a widely applied communication technology. Multicast source authentication is an important problem in multicast security. Especially, it is a big challenge to implement the multicast source authentication in a noisy channel. In order to solve the problem of multicast source authentication in the noisy channel, a chained multicast source authentication technology based on the threshold cryptography is proposed. Firstly, the security assumption and security model of the chained multicast source authentication is provided based on the security requirement of the multicast source authentication and Dolev-Yao model. Then, a new multicast source authentication protocol adapted to the noisy channel is designed by using the threshold secret sharing technology. Finally, the security of the proposed protocol is analyzed. The simulation results show that the multicast source authentication protocol has a good ability to resist packet loss and ensure good communication performance.

Key words: Internet security; Multicast; Multicast source authentication; Threshold cryptography; Security model

1 引言

随着通信和网络技术的迅猛发展，单发多收型信息传输应用越来越广泛。采用传统单播方式来传播此类信息时，发送源的负担与客户数目成正比，对传输效率影响极大[1]。组播技术可避免单播中服务器为每一个接收方提供相同内容的拷贝，可节省发送数据主机的系统资源、带宽以及骨干网的传输带宽。但是，组播技术也面临着诸多问题需要解决，如组播路由的建立[2,3]、组播的稳定性[4]和组播的安全等。其中，组播安全问题中，组播数据流的消息源认证问题(简称组播源认证)是实现组播通信安全的一个关键问题，受到了广泛关注。它主要解决发送方的身份认证和消息源认证。

考虑到数字签名的计算开销问题，目前的研究都是以数字签名为基础结合对称密码技术来设计组播源认证的，根据采用的密码技术不同可分为基于非对称密钥的组播源认证算法和基于对称密钥的组播源认证算法。基于对称密钥的组播源认证算法主要有定时的高效损耗容忍流认证技术(TESLA)[5]和非对称的消息认证码(MAC)技术[6]两种。TESLA 通过密钥延迟技术解决因所有人都使用同一密钥而导致的不具有辨别性问题。此算法的优点在于计算开销和通信开销小，只要公布密钥的包不丢失，丢包

2014-07-07 收到，2014-09-28 改回
国家自然科学基金(61373172)和中央高校基本科研业务费(7214390604)资助课题
*通信作者：黎剑兵 jbli@mail.xidian.edu.cn

对其就没有任何影响；缺点是需要松散的时间同步。该算法的实时性与每组数据包的数目有关：每个密钥签名的包数目越多，需要等待的时间越长、延迟越大；反之，通信用于发布密钥的带宽增加，不利于通信。非对称的 MAC 技术通过发送方和接收方拥有不对等的密钥集来区别发送方。这种算法的优点在于对称密钥加密速度快、计算开销小；缺点在于接收方会接收到无用的信息，当组成员很多时，无用的通信开销及收发双方过多的计算导致延迟过大，且组内部的共谋攻击容易产生。

基于非对称密钥的组播源认证算法主要有哈希树(Hash Tree)和哈希链(Hash chain)两种结构。哈希树算法的优点是安全性较高，能够较好地抵抗篡改攻击；签名针对一组数据包，减少了签名的次数；缺点是通信开销和计算开销较大，有一定的延迟。这类算法主要有层次组播源认证算法算法(HMSA)[7]、自适应组播源认证(AMSA)[8]、自适应组播数据源认证(AMDOA)[9]和组播源认证与拥塞控制综合方法(IAMSAC) [10]。哈希链算法的优点是通信开销小；缺点是抗丢包能力、安全性一般较差[11]。典型哈希链算法有简单哈希链(SHC)[12,13]、高效多链流签名(EMSS)[14]、接收方驱动的层次哈希链组播源认证(RHL)[15]、有损信道组播认证(MALC)[16]和基于多哈希链的组播源认证(MHC)[17]。相对哈希树算法而言，哈希链算法在实时性、灵活性和总体开销上都具有一定优势，能够适应开放的网络环境中的组播。现有的改进算法主要通过增加存储负载和通信负载来增强链式组播的抗丢包能力和安全性，缺点较明显。

本文在链式组播源认证方法的基础上引入门限密码技术，以解决有扰信道上的组播源认证问题，在信道丢包率门限范围内时，丢包对认证将没有任何影响，而且门限值可以根据信道情况进行调整。本文所提算法在继承了链式组播源认证算法通信开销小、实时性好等特点的基础上解决了抗丢包性差的问题，提高了安全性。为了便于统一分析链式组播源认证算法的安全性问题，本文针对组播源认证的安全需求提出基于 Dolev-Yao[18]模型的安全假设和安全模型。

本文内容安排为：第 1 节为引言；第 2 节提出链式组播源认证算法的安全假设并对其建立安全模型；第 3 节详细叙述基于门限密码的链式组播源认证协议并证明协议的安全性；第 4 节对本文提出的协议进行仿真、安全性分析和性能分析；最后在第 5 节中给出本文结论。

2 组播源认证技术的安全模型

2.1 链式组播源认证算法的安全假设

组播源认证算法是密码协议的一种。本文在 Delov-Yao 模型中的安全假设基础上对链式组播源认证协议做出如下安全假设：

(1)多个接收方获得完全相同的消息，因此参与方为发送方 A 和接收方 R。

(2)发送方 A 发送消息时，使用数字签名算法对消息的首个数据包签名，用于接收方的身份验证。其余数据包使用哈希链结构。在链式组播源认证中签名算法 $\mathrm{S_s}(\bullet)$ 通常包括两个部分：

(a)基本数字签名算法 $\mathrm{Sig}(\bullet)$：文中使用现有成熟数字签名算法并假定是安全的。

(b)源认证算法 $\mathrm{S}(\bullet)$：用以增强安全性并降低通信开销，是证明安全性时主要关注的部分。

(3)接收方 R 的认证过程与相关数据包中的内容相关；

(4)针对链式组播源认证协议，除了组播源认证协议中的攻击外，还存在一种特殊的攻击——替换攻击[19]。对于替换攻击，攻击者必须至少控制连续的两组数据包才能进行，因此在传输延迟门限上进行恰当的限制也可以对这类攻击进行很好的避免或减弱。一般的只要传输延迟门限设置在相邻两组数据包的发送时间间隔以内即可抗击此类攻击。假设传输延迟门限已经根据算法复杂度、相邻两组数据包的最小发送时间间隔和信道环境给予确定，那么接收方验证时，除了按照验证算法进行验证以外，还要逐组检验数据包的延迟，如果延迟超过门限值，则丢弃数据包。

2.2 链式组播源认证算法模型

2.2.1 符号描述 令 γ 表示满足协议的数据包中有限长比特串，γ^* 表示字符串 γ 中的元素，$i \le t, j \le t$。$\gamma = \alpha \parallel \beta$ 表示有限长字符串 γ 由有限长字符串 α 和有限长字符串 β 组成。字符串 γ 具有两种约减集。一是字符串 $\gamma|_{\mathrm{Sig}}$，表示从字符串 γ 中去除掉数字签名的内容。字符串 $\overline{\gamma}$ 表示在 $\gamma|_{\mathrm{Sig}}$ 的基础上去除消息明文，明文在证明中可以忽略。

令 Σ 表示有限个序列集合，Σ^+ 表示满足协议 T 的消息的全集。

2.2.2 链式组播源认证算法的模型描述

定义 1 令 T 是一个组播源认证协议，定义发送方 A 发送的第 i 个消息中包括对第 j 个消息认证：$\alpha_i = m_i \parallel S(m_j) \parallel \mathrm{Sig}$，其中源认证消息可以是一个或多个。其中 $i \le t, j \le t$，t 表示数据包数目。

定义 2 令 T 是一个组播源认证协议，定义接收方针对发送方的消息具有操作 β_j。接收方实现操作 β_j 即计算 $\beta_j \alpha_i = V(S(m_j))$ 为 1 时，认为第 j 个消息 m_j 真实可信并接收消息。其中 $i \le t, j \le t$，t 表示数据包数目。

定义 3　T 是一个组播源认证协议，协议 T 可以由发送方 A 的消息 α_i 和接收方的操作 β_j 表示。令 $\Sigma_1(Z)=\Sigma(\alpha_i)\cup\Sigma(\beta_j)$ 表示攻击者 Z 已知的发送消息的集合和验证的集合，即攻击者 Z 得知所有信道中的消息；$\Sigma_2(A)=\Sigma(\alpha_j)$ 表示发送消息的集合；$\Sigma_3(B)=\Sigma(\beta_j)$ 表示接收操作即验证的集合。其中 $i\le t, j\le t$，t 表示数据包数目。

当存在字符串 $\gamma,\gamma\in\Sigma^+$，若存在 $\overline{\beta_i\gamma}=1$，协议 T 不安全，否则协议 T 安全，其中 $\beta_i\gamma=V(\gamma)$。攻击者的目的是在任意一步中找出比特串 γ 并通过接收方 R 的验证，使得 $\beta_i\gamma=V(\gamma)$。

2.2.3 链式组播源认证算法的安全性质描述及证明

定理 1　对于链式组播源认证算法 T，在规定的传输延迟门限内，如果对于每一个 i, j，都有 $\beta_j\alpha_i=1$，则认为算法是安全的。

证明　必要性：考虑算法的安全假设，安全的算法可确保消息真实性和可验证性，即对于每一个 i，都有 $\beta_j\alpha_i=1$。因此定理 1 的必要性成立，即安全的组播源认证算法必然可以得到对于每一个 i，都有 $\beta_j\alpha_i=1$。

充分性：假设算法是不安全的，则依据定义 3，存在字符串 $\gamma,\gamma\in\Sigma^+$，使得 $\overline{\beta_i\gamma}=1$。即在忽略替换攻击的情况下，如果对于每一个 i，都有 $\beta_j\alpha_i=1$，且 $\beta_j(\gamma)=V(\gamma)=1$ 成立。这种情况下，γ 具有两种形式：(1) $\gamma=S(m_i)$，这种情况在忽略替换攻击的情况下，对攻击者而言，没有任何意义。(2) $\gamma\ne S(m_i)$，即攻击者找到一个不同于 $S(m_i)$ 的字符串，使得 $V(\gamma)=1$。设计者通常在设计算法的时候，使用完善的单向函数得到 $S(m_i)$。这样攻击者要得到 $\gamma\ne S(m_i)$ 的情况下，使得 $\beta_j(\gamma)=V(\gamma)=1$，只有找到单向函数的碰撞，这是计算上不可行的。因此，与假设矛盾，攻击者无法找出这样的字符串 γ，使得 $\beta_j(\gamma)=V(\gamma)=1$。所以，对于链式组播源认证算法，在忽略替换攻击的情况下，如果对于每一个 i，都有 $\beta_j\alpha_i=1$，可以认为算法是安全的，其中 $i\le t, j\le t$，t 表示数据包数目，即充分性可证明。

证毕

3　基于门限密码的链式组播源认证方案设计

3.1 协议设计

3.1.1 参数及参数选择

(1) 参数说明：z 为组成员共享的一个组密钥；(p_U,S_U) 为成员 U 的公私钥对；$p\ge 2^{160}$ 为大素数；n 是每组发送数据包的个数；s_{ij} 消息中第 i 组第 j+1 个数据；$\mathrm{H}(\bullet)$ 表示安全的哈希函数；$\mathrm{E}_{\mathrm{Zs}}(\bullet)$ 为加密算法，密钥为组密钥 $\mathrm{Z_s}$；$\mathrm{Sig_{Sk}}(\bullet)$ 为签名算法，s_U 为签名者的私钥；k 为门限密码中的门限值，也限制每组中最多丢包数。

(2)门限密码主要根据 Shamir 的基于差值多项式的门限密码技术，本文中使用的差值多项式可以描述为 $f(x)=a_4x^4+a_3x^3+a_2x^2+a_1x+a_0 \bmod p$，在本文的方案论述中以 $n=5, k=3$ 为例进行描述。

(3)确定 n 个两两不等的预设值，这里以 $n=5$ 为例，本文中选择 $x_0,\ x_1,\cdots,\ x_4$，5 个 8 bit 值，组内成员预计算范德蒙行列式 $\boldsymbol{D}$ 如式(1)所示，并同时计算 $\boldsymbol{D}$ 的伴随阵存储下来。

$$\boldsymbol{D}=\begin{vmatrix} x_0^4 & x_0^3 & x_0^2 & x_0 & 1\\ x_1^4 & x_1^3 & x_1^2 & x_1 & 1\\ x_2^4 & x_2^3 & x_2^2 & x_2 & 1\\ x_3^4 & x_3^3 & x_3^2 & x_3 & 1\\ x_4^4 & x_4^3 & x_4^2 & x_4 & 1 \end{vmatrix} \bmod(p) \tag{1}$$

3.1.2 协议设计

(1)第 1 组数据包及其签名的处理

步骤 1　发送方将要发送的数据包缓存 $n=5$ 个后作为第 1 组数据包，即 s_{1j}，并计算其哈希值 $H(s_{1j}), j=1,\ 2,\cdots,5$，令：$f(x_j)=H(s_{1j})=a_{14}x_j^4+a_{13}x_j^3+a_{12}x_j^2+a_{11}x_j^1+a_{10} \bmod(p), j=1,2,\cdots,5$。联立 5 个方程并利用 Cramer 法则，解出 $a_{1q}=\boldsymbol{D}_q/\boldsymbol{D} \bmod q$，其中，$a_{1q}$ 表示第 1 组数据包的第 q 个参数；$\boldsymbol{D}_q$ 是用向量 $[H(s_{10})\ H(s_{11})\ H(s_{12})\ H(s_{13})\ H(s_{14})]^{\mathrm{T}}$ 代替 $\boldsymbol{D}$ 中第 q 列所组成的行列式。这个过程可直接利用预存储的 $\boldsymbol{D}$ 的伴随阵完成。

步骤 2　将 a_{10}, a_{11}, $H(a_{14}\parallel a_{13}\parallel a_{12}\parallel a_{11}\parallel a_{10})$ 与本地时间 T_i，用私钥签名后发送，即发送 $a_{11}\parallel a_{10}\parallel T_0\parallel \mathrm{Sig_{Sk}}(a_{11}\parallel a_{10}\parallel H(a_{14}\parallel a_{13}\parallel a_{12}\parallel a_{11}\parallel a_{10})\parallel T_0)$ 作为首个签名包。

(2)发送方发送后续数据包

步骤 3　首先对数据包编号，每 5 个包为一组，s_{ij} 表示第 i 组的第 j 个数据包。按照步骤 1 求出各组的 a_{ij}。第 i 组数据包(第 1 组除外)发送内容为 $s_{ij}\parallel a_{i+1,1}\parallel a_{i+1,0}\parallel H_i(a_{i+1,4}\parallel a_{i+1,3}\parallel a_{i+1,2}\parallel a_{i+1,1}\parallel a_{i+1,0})\parallel T_i$。每一组消息用相同的时间戳 T_i，相当于组序列号，最后一组数据包不需计算下一组的认证信息。

认证算法如图 1 所示。

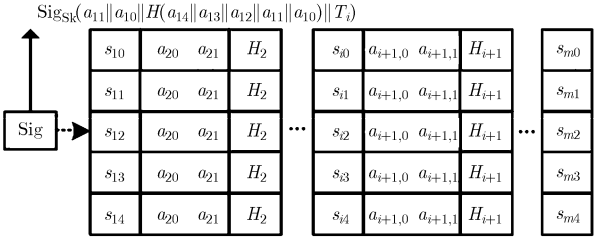

图 1 认证算法的图示

3.1.3 验证算法

步骤 1 接收方首先接收到签名包。验证签名以确认本次会话的新鲜性，同时保留 a_{10}，a_{11}，$H(a_{14}\|a_{13}\|a_{12}\|a_{11}\|a_{10})$，用于验证第 1 组数据。

步骤 2 接收数据包，判断组，接收完一组时验证数据包内容。任取一组中的 k 个消息，结合收到的 $n-k$ 个系数可得出差值多项式的全部 5 个系数 $a_{i'4}$，$a_{i'3}$，$a_{i'2}$，$a_{i'1}$，$a_{i'0}$，计算 $H(a_{i'4}\|a_{i'3}\|a_{i'2}\|a_{i'1}\|a_{i'0})$ 并验证 $H(a_{i'4}\|a_{i'3}\|a_{i'2}\|a_{i'1}\|a_{i'0})=H(a_{14}\|a_{13}\|a_{12}\|a_{11}\|a_{10})$ 是否成立，若不成立则丢弃该分组。对于组内其它未参与上述计算的消息，可直接计算出哈希值并代入差值方程验证即可。

验证算法图如图 2 所示。

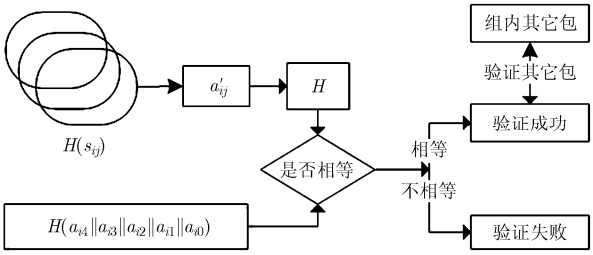

图 2 验证算法图示

算法的核心在于保证安全性的前提下，利用门限密码解决链式的抗丢包率问题。门限密码技术在算法中的体现为：当每个组中丢失包的个数少于 $n-k$ 时，都可以有效验证，门限值 $1-k/n\times100\%$，即当 n 个连续包内最大连续突发丢包率小于等于 $1-k/n\times100\%$ 时，即可以检验成功。

3.2 协议安全性证明

3.2.1 算法内部安全性证明

(1)认证算法和验证算法的数学抽象 发送方计算 3.1.3 节步骤 1 中所述的联立方程组，在已知 x_0, x_1, x_2, x_3, x_4 的基础上求得 a_4, a_3, a_2, a_1, a_0 并传输 $n-k=2$ 个参数，如 a_1, a_0。接收方根据接收到的数据包再次计算每组的参数并通过比较实现验证。在丢包情况下，假设只接收到前 3 个数据包，则

$$\left.\begin{aligned}&H(s_0)=f(x_0)=a_4x_0^4+a_3x_0^3+a_2x_0^2+a_1x_0+a_0\\&H(s_1)=f(x_1)=a_4x_1^4+a_3x_1^3+a_2x_1^2+a_1x_1+a_0\\&H(s_2)=f(x_2)=a_4x_2^4+a_3x_2^3+a_2x_2^2+a_1x_2+a_0\end{aligned}\right\}\ \mathrm{mod}(p)\quad(2)$$

已知 x_0, x_1, x_2, x_3, x_4 和 a_1, a_0，求得 a_4, a_3, a_2，即成功构造出与发送方相同的函数 $f_1(x)$。

(2)内部函数安全性的证明

(a)成功验证实现的证明(忽略攻击者攻击，只考虑传输错误时是否可以成功验证) 由协议的设计可知，发送方根据发送的一组数据包构造的多项式 $f(x)$ 是唯一确定的。设 $f'(x)$ 是接收方根据接收到信息唯一恢复的多项式。当丢包小于等于 $n-k$ 个时：因为 $f(x)$ 和 $f'(x)$ 都是唯一确定的，且 $\mathrm{H}(\bullet)$ 是完善的单项哈希函数，所以若存在传输错误，则 $f_i'(x)$ 与 $f_i(x)$ 的参数不相同，即：$H(a_{i'4}\|a_{i'3}\|a_{i'2}\|a_{i'1}\|a_{i'0})\neq H(a_{14}\|a_{13}\|a_{12}\|a_{11}\|a_{10})$，所以错误传输的数据包无法满足验证。当丢包大于 $n-k$ 个时，收方无法正确恢复多项式，因而无法验证。

(b)攻击者的伪造不可行证明 因为对于 $f(x)$，一个 x 有且只有一个对应的函数值 $f(x)$。所以若 x_1=x_2，则必有 $f(x_1)=f(x_2)$。因此对于特定的 x，攻击者只有找到 $f(x')$，使 $f(x')=f(x)$ 且 $x'\neq x$，才能攻击成功。然而 $f(x)=H(s_{ij}')$，攻击者只有找到 s_{ij}'，使得 $H(s_{ij}')=H(s_{ij})$ 才可实现对消息伪造。而根据哈希函数的不可碰撞性，寻找哈希碰撞是不可行的。因此攻击者的伪造不可行。综上，算法有效，组内可以成功认证，且具有安全性。

3.2.2 链式安全性的证明

(1)消息有效性的证明

(a)签名包的证明(证明消息的来源) 算法发送的第 1 个包为：$a_{11}\|a_{10}\|T_i\|\mathrm{Sig}_{S_k}(a_{11}\|a_{10}\|H(a_{14}\|a_{13}\|a_{12}\|a_{11}\|a_{10})\|T_i)$ 其中包含经过发送方私钥进行过数字签名，因此只要签名算法是安全的，该包就是安全的，它同时也证明了消息来源的真实性。

(b)链式有效性及消息真实性的证明(包括抗修改特性证明) 假设在签名包具有真实性的情况下，攻击者能够篡改后续数据包内容。在基于门限密码的链式组播源认证算法中，发送方消息为 $a_i=s_{i,1}\|a_{i+1,0}\|a_{i+1,1}\|H_{i+1}$，其中 $i\in\{1,2,\cdots,n\}$。$\beta_j\alpha_i=\beta_{j+1}\alpha_i=V(H_{i+1})$。

由于数据包的验证条件是 $H(a_{i4}\|a_{i3}\|a_{i2}\|a_{i1}\|a_{i0})$ 与 $H(a_{i'4}\|a_{i'3}\|a_{i'2}\|a_{i'1}\|a_{i'0})$ 是否相同；且第 1 组数据的对应差值多项式系数的哈希值 $H(a_{14}\|a_{13}\|a_{12}\|a_{11}\|a_{10})$ 是真实的。再考虑到每一组消息所确定的差值多项式的唯一性，即系数 a_{i4}，a_{i3}，a_{i2}，a_{i1}，a_{i0} 的唯一性，一旦攻击者修改了后续的第 1 组数据包，则解得的 a_{i4}'，a_{i3}'，a_{i2}'，a_{i1}'，a_{i0}' 与 a_{i4}，a_{i3}，a_{i2}，a_{i1}，a_{i0} 不全相同。攻击者要寻找一组 a_{i4}'，a_{i3}'，a_{i2}'，a_{i1}'，a_{i0}'，得使：$H(a_{14}'\|a_{13}'\|a_{12}'\|a_{11}'\|a_{10}')=H(a_{14}\|a_{13}\|a_{12}\|a_{11}\|a_{10})$。因哈希函数的不可碰撞性导致计算上不可行，所以签名包真实的情况下攻击者无法对后续数据包进行有效篡改。篡改的消息无法通过验证，这样第 1 组数据包来源真实且具有真实性，即 $\beta_2\alpha_1=V(H_2)=1$。依此类推，在规定传输迟延门

限内，对每个 i, j，有 $\beta_j\alpha_i = \beta_{j+1}\alpha_i = V(H_{i+1}) = 1$，后续数据包均具有真实性。

综上，算法具有有效性、安全性。

(2)算法新鲜性的分析　算法的新鲜性主要是指消息被非法延迟转发或者被重放。首先看消息延迟问题。如果消息延迟超过了接受端在协议规范框架下的滑动窗口则自然被丢弃，如果在滑动窗口内，不影响手段的正常接收。因而传输延迟攻击不影响消息的新鲜性。其次看消息重放问题，如果重放消息是在同一组消息内发生，即收方同时收到多个属于同组消息的相同拷贝，这时收方只要保留一个拷贝作为接收数据包，并进行认证即可，丢弃所有其它重复的消息。如果重放消息不是当前收方处理组内的消息，则直接丢弃。这些都可通过查看消息中的时间戳 T_i 来判断。因此重放消息也无法影响消息的新鲜性。

由于这里面时间戳的主要作用是表明每组消息的顺序号，且收方可以根据本地时间计算接收消息分组之间的延迟，所以不需要精确的时间同步，只需要松散的时间同步即可。

综上，算法的新鲜性具有保证。

4　基于门限密码的链式组播源认证算法的性能分析

4.1 计算复杂度分析

假设需要传输 m 个数据包，每 5 个数据包一组，最后一组不足 5 个时进行填充。

4.1.1 发送方的计算复杂度　签名算法中行列式包括两种：

(1)预计算 $\boldsymbol{D}$ 的值　由于$|\boldsymbol{D}|=|\boldsymbol{D}^{\mathrm{T}}|$，其中 $\boldsymbol{D}^{\mathrm{T}}$ 是一个 n 阶范德蒙行列式，$\left|\boldsymbol{D}^{\mathrm{T}}\right| = \prod_{1\le i\le j\le n}(x_i - x_j)$。则行列式 $\boldsymbol{D}$ 的计算量是 $(n-1)!$ 次减法和 $(n-1)!$ 次乘法。其中减法的计算量可以忽略；乘法中 n 较小(例中 n=5), x_i 不需要很大(例中 x_i 为 8 bit 长)，计算量较小。以上是预计算内容，只有在更换 x_i 时才需要计入计算复杂度。

(2)行列式 $\boldsymbol{D}_q$ 的计算　在 m 个数据包里，行列式 $\boldsymbol{D}_q$ 的计算出现 $m+((n-m) \bmod n)$ 次。因为行列式 $\boldsymbol{D}_q$ 为 n 阶，故需要 $n!$次乘法计算。同样，乘法中，n 较小且 x_i 不需要很大，所以计算量不大。如果事先计算出 $\boldsymbol{D}$ 的伴随阵，则根据克莱姆法则，只需要 m 次乘法，而不需要计算行列式。综上，发送方的计算复杂度包括一次数字签名、$m+((n-m) \bmod n)$ 次行列式 $\boldsymbol{D}_q$ 的计算、$m+((n-m) \bmod n)$ 次除法运算和 $m+\lceil m/n \rceil$ 次 hash 运算。

4.1.2 接收方的计算复杂度　接收方计算复杂度为 1 次数字签名、不多于 $m+((n-m) \bmod n)$ 次行列式 $\boldsymbol{D}_q$ 计算、不多于 $m+((n-m) \bmod n)$ 次除法运算和 $m+\lceil m/n \rceil$ 次哈希运算。

4.2 抗丢包率分析

算法以分组为单位组成哈希链，在每个组中进行验证。验证信息 $H(a_{i4} \parallel a_{i3} \parallel a_{i2} \parallel a_{i1} \parallel a_{i0})$ 传输次数为 n，为防止组内丢包传输的附加信息 a_{ij} 为 k 个。

信道中丢失包的情况可分为单一包的随机丢失及多个包的连续丢失两种情况。算法中只要一组内的丢包数目少于 k 就可以抵抗丢包。普通网络的丢包率一般为 10%到 30%，该算法的抗丢包率为 $(1-k/n)\times 100\%$。在 n=5, k=2 的情况下，抵抗的丢包率为 60%，可以满足普通网络要求。

4.3 算法的性能比较

假设共 m 个数据包，分组时以 n 个为一组，共有 $l=\lceil m/n \rceil$ 个组。基于门限的链式组播源认证算法与其他链式算法的性能比较如表 1 所示，其中计算量以“次”为单位，存储负荷以“数据包”为单位。本文算法中计算开销不因丢包率不同而变化，由于 n 和 x_i 的取值较小且预计算存在，实际计算量并不大，且在抗丢包率方面充分地表现了其优点。通过调整(n,k)，该算法能够更灵活地适应各种网络环境，接收方和发送方的存储负荷都为 n。又由于 n 通常较小，因此该算法在存储负荷上比 MALC 具有一定优势。另一方面，该算法附加 1 组哈希值和两个长度较小的参数值，即使丢包率增加，也仅是增加少量的开销用于传送增加的 1~2 个较小的系数，在通信量上具有一定优势。

在 NS2 环境下，我们对本文方案几种典型链式组播源认证方案(MHC, RMLCC, EMSS)的性能在不同丢包率条件下的认证成功率和平均传输迟延进行了比较，如图 3 和图 4 所示。丢包率 ρ 分别选择了 0(无丢包)、0.05, 0.10, 0.15, 0.20 和 0.25 这 6 种情况。在本文采用的门限方案中，取 n=5，即 5 个数据包 1 组，门限 k 满足 $1-k/n>\rho$，以保证足够的冗余度来抗丢包，所以对应上述 6 个丢包率所选择的门限 k 的值依次是 5, 4, 4, 4, 3, 3。其中 k=5 时表示无丢包。

从图 3 可以看出本文方案由于采用了基于门限的结构，并可根据信道丢包率有效调整，可以有效适应不同的信道丢包率，因此认证成功率相比于其他方案具有明显的优势，除非有大量的突发连续错误，才会出现认证失败的情况。该认证方法以小的代价换取了尽可能大的认证成功率。从图 4 可以看出，本方案中发放的计算量很小，而且不依赖于丢包率的变化，所以延迟相对于其他方案来说也是很小的。

表 1 链式组播源认证算法的性能比较

算法	计算量	抵抗丢包率	发送方存储负荷	接收方存储负荷	通信量
SHC (在线)	公钥签名：1 单钥加解密运算：$m+l$	0%	1	1	初始包：数据+密钥+公钥签名 普通包：数据+密钥+对称加密
EMSS /RHL	公钥签名：1 哈希运算：m	$1/(P+1)$	3	3	初始包：数据数据+hash 中间包：数据+hash+hash 结束包：公钥签名
MALC	公钥签名：l 哈希运算： $l\times n^2+n$ 纠错码编码：l 认证计算：$(n-1)\times l$	与纠错码相关	$m+((n-m)\bmod n)$	$m+((n-m)\bmod n)$	初始包列：数据+编码+公钥签名 普通包列：数据+认证信息+编码+公钥签名
门限算法	公钥签名：1 行列式运算： $m+((n-m)\bmod n)$ 除法运算： $m+((n-m)\bmod n)$ 哈希运算：$m+l$	k/n	n	n	初始包：签名+本地时钟 普通包：数据+hash+附加认证信息

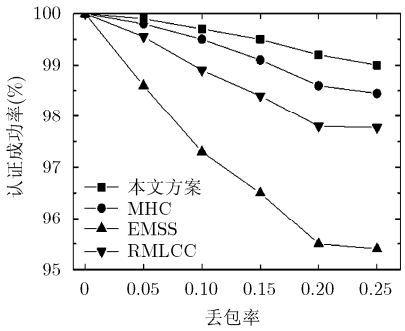

图 3 认证成功率比较

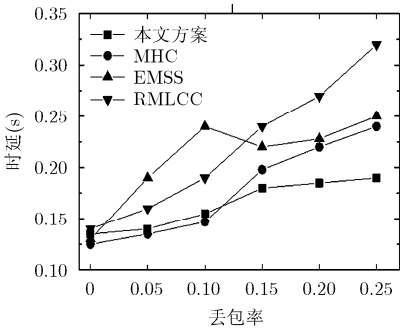

图 4 时延比较

5 结束语

本文从解决有扰信道上的组播源认证问题的目标出发，提出了一种基于门限密码的链式组播源认证技术。首先，本文基于组播源认证的安全需求和 Dolev-Yao 模型给出了链式组播源认证的安全假设和安全模型；然后结合 Shamir 的门限秘密共享技术设计了一种适合于有扰信道的组播源认证协议并对其进行了安全性分析。对协议的仿真结果表明，本文设计的组播源认证方案与现有典型方案相比在保证了较好的通信性能的前提下具备良好的抗丢包能力。

参 考 文 献

[1] Babamir, S M. Specification and verification of reliability in dispatching multicast messages[J]. *Journal of Supercomputing*, 2013, 63(2): 612–635.

[2] 胡敏, 胡博, 黄红梅. 基于免疫 Memetic 算法的网络组播路由优化[J]. 计算机工程与应用, 2013, 49(2): 105–108.
Hu Min, Hu Bo, and Huang Hon-gmei. Multicast routing optimization based on immune Memetic algorithm[J]. *Computer Engineering and Applications*, 2013, 49(2): 105–108.

[3] 王慧, 王铮. 基于关键节点时延约束低代价组播路由算法[J]. 计算机应用研究, 2013, 30(2): 585–587.
Wang Hui and Wang Zheng. Delay-constrained and low-cost multicast routing algorithm based on key node[J]. *Application Research of Computers*, 2013, 30(2): 585–587.

[4] 陈华胜, 齐勇, 李伟华. 一种基于多维节点属性层次聚类的应用层组播生成树算法[J]. 计算机应用研究, 2012, 29(12): 4688–4690.
Chen Hua-sheng, Qi Yong, and, Li Wei-hua. Hierarchical clustering multi-dimension host properties based application layer multicast spanning tree construction algorithm[J]. *Application Research of Computers*, 2012, 29(12): 4688–4690.

[5] Xu Shou-huai and Ravi S. Authenticated multicast immune to denial-of-service attack[C]. Proceedings of the 2002 ACM Symposium on Applied Computing, Madrid, Spain, 2002:

196–200.

[6] 刘传才, 郭文忠. 基于消息认证码的安全有效的组播源认证[J]. 微电子学与计算机, 2002, 19(6): 13–17.
Liu Chuan-cai and Guo Wen-zhong. Secure and efficient source authentication for multicast based on message authentication codes[J]. *Microelectronics & Computer*, 2002, 19(6): 13–17.

[7] Gennaro R and Rohatgi P. How to sign digital streams[R]. Advances in Cryptography-Crypto' 97, 1997: 180–197.

[8] Rohatgi P. A compact and fast hybrid signature scheme for multicast package authentication[C]. Proceedings of the 6th ACM Computer and Communications Security Conference, Singapore, 1999: 93–100.

[9] Zhu L, Yang H, and Yang Z. The adaptive multicast data origin authentication[C]. Second CCF Internet Conference of China, Zhangjiajie, China, 2013: 109–121.

[10] Singh K, Yadav R S. Integrated approach for multicast source authentication and congestion control[C]. The 9th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, QSHINE 2013, Greader Noida, India, 2013: 16–30.

[11] 黄海平, 戴庭, 王汝传, 等. 基于(t, n)门限和划分树的可再生散列链构造方案[J]. 通信学报, 2013, 34(4): 70–81.
Huang Hai-ping, Dai Ting, Wang Ru-chuan, *et al.*. Novel self-renewal hash chain scheme based on (t,n) threshold and division tree[J]. *Journal on Communications*, 2013, 34(4): 70–81.

[12] 戴卫国, 孙乐昌, 单洪. 组播安全研究[J]. 安徽电子信息职业技术学院学报, 2004, 3(5): 41–42.
Dai Wei-guo, Sun Le-chan, and Shan Hong. Multicast security research[J]. *Journal of Anhui Vocational College of Electronics & Information Technology*, 2004, 3(5): 41–42.

[13] 黄秀姐, 李进, 王燕鸣. 标准模型下可证明安全的广义指定验证者签名(证明)方案[J]. 计算机应用, 2006, 26(12): 2938–2940.
Huang Xiu-jie, Li Jin, and Wang Yan-ming. Universal designated verifier signature (proof) schemes without random oracles[J]. *Journal of Computer Application*, 2006, 26(12): 2938–2940.

[14] Perrig A, Canetti R, Tygar J, *et al.*. Efficient authentication and signing of multicast streams over lossy channels[C]. IEEE Symposium on Security and Privacy, Oakland, USA, 2000: 56–73.

[15] 朱辉, 李晖, 王育民. 可证明安全的多信任域认证密钥协商协议[J]. 华中科技大学学报(自然科学版), 2009, 37(5): 53–56.
Zhu Hui, Li Hui, and Wang Yu-min. Security-proved authenticated key agreement protocol for multi-domain[J]. *Journal of Huazhong University of Scienve and Technology* (*Nature Science Edition*), 2009, 37(5): 53–56.

[16] 李兴华, 马建峰, 文相在.基于身份密码系统下 Canetti-Krawczyk 模型的安全扩展[J]. 中国科学 E 辑: 信息科学, 2004, 34(10): 1185–1192.
Li Xing-hua, Ma Jian-feng, and Wen Xiang-zai. The security extensions based Identity cryptosystem Canetti-Krawczyk model[J]. *SCINCE IN CHINA Series E: Information Sciences*, 2004, 34(10): 1185–1192.

[17] Jeong Y, Lee S, and Shin S, Efficient and secure source authentication scheme for multicast user authentication[J]. *Journal of Central South University*, 2013, 20: 2741–2746.

[18] Dolev D and Yao A. On the security of public key protocols[J]. *IEEE Transactions on Information Theory*, 1983, 29(2): 198–208.

[19] 葛荣亮, 高德智, 梁景玲, 等. 无证书签名方案的分析及改进[J]. 计算机工程与应用, 2013, 49(5): 96–98.
Ge Rong-liang, Gao De-zhi, Liang Jing-ling, *et al.*. Security analysis and improvement of certificateless signature scheme[J]. *Computer Engineering and Applications*, 2013, 49(5): 96–98.

黎剑兵：男，1975 年生，博士生，讲师，研究方向为网络安全、智能信息处理.

李　庆：女，1991 年生，硕士生，研究方向为密码学、网络与信息安全.

董庆宽：男，1974 年生，博士，副教授，研究方向为密码学、网络与信息安全.

李小平：女，1961 年生，博士，教授，博士生导师，研究方向为智能信息处理.