组播分组数据源鉴别综述

陈 慧 熊光泽 刘 璟
(电子科技大学计算机科学与工程学院 成都610054)

摘 要 对组播分组数据源鉴别领域的现有研究成果进行了系统的分类和总结,指出了它们各自存在的优缺点;提出了一个公开问题——分组Hash有向图鉴别问题;指出了该领域的一些可能发展方向。

关键词 组播安全,分组数据源鉴别

Multicast Packet Source Authentication

CHEN Hui XIONG Guang-Ze LIU Jing
(University of Electronic Science and Technology of China, Chengdu 610054)

Abstract As for multicast packet source authentication, systematically classifying and summarizing the current research results on multicast packet source authentication and recognizing their benefits and limitations; proposing an open problem--Authentication of Packet Hash Directional Graph; indicating many possible research directions.

Keywords Multicast security, Packet source authentication

1 简介

通过分组数据源鉴别可以确认所接收到的分组数据是否来自所声称的发送者,并且分组数据在发送过程中没有被修改和替换(完整性实际上是分组数据源鉴别的副产品)。组播分组数据鉴别可以分为两类:一类是组内分组数据鉴别,其任务是鉴别分组数据是否来自组内部某个发送者,但不能鉴别具体是谁;另一类是分组数据源鉴别,其任务是鉴别分组数据是否来自所声称的发送者(该发送者可以是组内成员也可以是非组内成员)。组内分组数据鉴别利用消息鉴别码MAC(例如HMAC)就可以实现。MAC码的生成和验证都相当快,而且MAC码的密钥为全组成员所共享(可以是组会话密钥),可以快速鉴别分组数据是否来自组内,从而实现组内分组数据鉴别。在单播方式中,分组数据源鉴别完全可以简单地利用MAC码来实现,因为MAC码的密钥仅为单播双方所共享。但是在组播方式中,发送者发送的数据将为数目巨大的接收者所接收,接收者需要确认分组数据是否来自合法的发送者而且分组数据的完整性也需要得到保障(例如股票实时信息发布),在这种情况下,简单地利用MAC码是完全不行的(2.3节,我们将看到一些变通的MAC码技术确实可以在组播环境下实现分组数据源鉴别),因为MAC码密钥(可以使用组会话密钥)为所有接收者所共享,每个接收者都可以使用这个MAC码密钥对分组进行签名(这里的签名运算是指对每个分组计算其MAC码)从而伪装成原来的发送者发送组播数据。一种很自然的方式是使用基于非对称密码体制的数字签名技术(例如RSA),但是由于必须对每一分组进行签名和验证,使用一般的数字签名技术将带来巨大的计算开销和通信开销,同时签名和验证时的较大时延(软件实现时,RSA在签名方面比MAC码慢近10000倍,在验证方面比MAC码慢近300倍)也将大大影响发送者和接收者对分组数据的处理速度,特别是在实时信息传送的场合(现场转播,视频会议等),如果直接使用一般的数字签名技术,很难实现高效的分组数据源鉴别,为此人们提出利用其它的数字签名技术,例如一次性签名技术等,来实现组播分组数据源鉴别。

组播系统中的分组数据源鉴别问题是所有组播安全问题中最为棘手也是最有趣和最具挑战性的一个问题。在设计一个理想的组播分组数据源鉴别系统时,我们所要面临的挑战是:

1. 鉴别信息生成和验证的高效性:生成和验证鉴别信息所带来的系统开销应当足够小。由于组播系统中存在大量的接收者在接收数据,有些接收者的计算能力可能非常有限,验证鉴别信息的计算开销对这些接收者而言就变得至关重要。

2. 实时/立即签名和鉴别:许多应用,例如股票实时信息发布、在线转播和视频会议等需要实时的信息鉴别。因此,不论发送者或接收者在发送或验证前都不应该对数据进行缓存,而应该立即签名或鉴别。

3. 单个分组数据鉴别:接收者需要鉴别他所接收到的单个分组。

4. 对分组丢失的完美鲁棒性:由于IP组播系统利用不可靠的UDP/IP协议(在MBone上,IP/UDP分组的丢失概率大致为10%~20%)。理想的鉴别协议应该能够忍受很高的分组丢失率。

5. 可伸缩性:组播系统存在数目巨大的潜在接收者,理想的鉴别协议应该具有良好的可伸缩性。

6. 短小的鉴别信息:由于接收者必须能够鉴别每一个分组,每个分组都携带了相关的鉴别信息,理想的鉴别协议应该具有最低的通信开销。

目前,虽然已经出现一些非常优秀的研究成果,但是还没有任何一个方案能够同时满足以上六大挑战。这仍然是组播安全学术界的一个公开问题。

2 研究进展

我们认为分组数据源鉴别领域的研究成果可以分为以下

陈 慧 博士研究生,主要研究方向为计算机网络技术与应用。熊光泽 博士生导师,主要研究方向为实时计算系统及应用。刘 璟 博士研究生,主要研究方向为计算机网络技术与应用。

四类[22]:①基于分组 Hash 有向图的方案;②基于一次性数字签名技术的方案;③基于 MAC 码技术的方案;④基于前向纠错码 FEC 的方案。下面就这四个方面分别展开论述。

2.1 基于分组 Hash 有向图的方案

首先,给出分组 Hash 有向图(Packet Hash Graph)的概念。该概念是作者对已有研究结果进行总结后提出的。既然一般的数字签名技术不适于为单个分组进行签名,人们很自然地想到在一段分组数据流中能不能只对其中一个分组进行签名,其它分组都通过某种方式和签名分组关联从而便于接收者验证所有的分组。这样,签名和验证的计算和时间开销以及签名信息的通信开销就均摊给这段分组数据流中的每个分组。

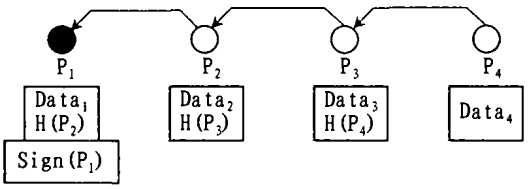

图1 使用分组 Hash 链的鉴别方式

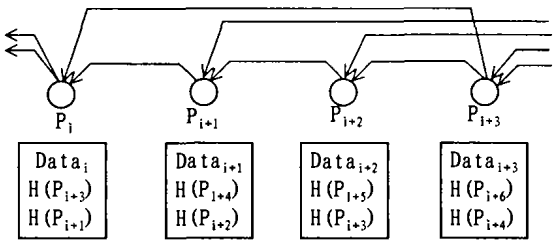

图2 使用分组 Hash 有向图的鉴别方式

人们想到使用如图1所示的 Hash 链方式,分组1为签名分组,发送者对分组 P_4 的数据 $Data_4$ 使用单向散列算法(例如 MD5)得到 Hash 值 $H(P_4)$ 并附在分组 P_3 的数据 $Data_3$ 后;对分组 P_3 的数据 $Data_3$ 和 $H(P_4)$ 使用单向散列算法得到 Hash 值 $H(P_3)$ 并附在分组 P_2 的数据 $Data_2$ 后;对分组 P_2 的数据和 $H(P_3)$ 使用单向散列算法得到 Hash 值 $H(P_2)$ 并附在分组 P_1 的数据 $Data_1$ 后;使用一般的数字签名算法(例如 RSA)对分组 P_1 的数据 Data1 和 $H(P_2)$ 进行签名,得到数字签名 Sign (P_1)。接收方的分组鉴别是这样进行的,首先接收方验证分组 P_1 携带的数字签名 Sign(P_1),若验证通过,$Data_1$ 和 $H(P_2)$ 得到鉴别;然后接收方再对分组 P_2 的数据 $Data_2$ 和携带的 $H(P_3)$ 使用单向散列算法得到一个 Hash 值,将该 Hash 值与已经通过了鉴别的 $H(P_2)$ 进行比较,若相等,$Data_2$ 和 $H(P_3)$ 得到鉴别;接收方再对分组 P_3 的数据 $Data_3$ 和 $H(P_4)$ 使用单向散列算法得到 Hash 值,将该 Hash 值与已经通过了鉴别的 $H(P_3)$ 进行比较,若相等,$Data_3$ 和 $H(P_4)$ 得到鉴别;最后接收方对分组 P_4 的数据 $Data_4$ 使用单向散列算法得到 Hash 值,将该 Hash 值与已经通过了鉴别的 $H(P_4)$ 进行比较,若相等,$Data_4$ 得到鉴别;至此整个分组链都得到了鉴别。以图1为例,分组 Hash 链鉴别方式存在的问题是:一旦其中某个分组丢失(例如 P_2),该分组后的所有分组(P_3 和 P_4)将得不到鉴别。于是人们提出了类似图2的分组 Hash 有向图的思想,例如图2中,若分组 P_{i+2} 丢失,只要分组 P_i 没有丢失并且已经得到鉴别,分组 P_{i+3} 仍然可以得到鉴别,因为分组 P_i 中也含有 P_{i+3} 的 Hash 值。

于是我们可以给出分组 Hash 有向图的概念。

分组 Hash 有向图——分组 Hash 有向图是同时满足如下三个条件的一个有向无环图:①图中的所有节点代表分组,存在唯一一个出度为零的节点(图论中称为 sink,即汇点),其代表的分组含有数字签名(称为签名节点);②对图中的有向边(或称为 Hash 边),该有向边终节点所代表的分组内含有该有向边始节点所代表的分组的 Hash 值;③除签名节点外,对每一个节点,从该节点到签名节点存在着至少一条有向路径;④图中节点从左到右的排列顺序同时代表了发送方发送分组的先后顺序(越靠左越先发送)。

图3就是一个经过抽象后的分组 Hash 有向图。图中的黑色节点为签名节点。可以看出每个节点和签名节点间存在着至少一条有向路径。在分组 Hash 有向图中,我们称一个分组是可鉴别的,当且仅当代表该分组的节点和签名节点间存在一条有向路径。

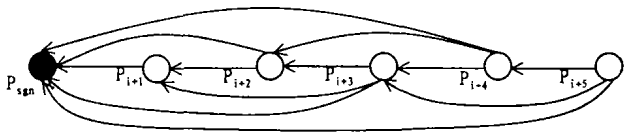

图3 抽象后的分组 Hash 有向图

分组 Hash 有向图鉴别问题 所有利用分组 Hash 有向图实现分组数据源鉴别的方案需要解决的核心问题都围绕着如何设计分组 Hash 有向图以提高其对各种分组丢失情况的鲁棒性,即:在有分组丢失的情况下,每一个收到的分组仍然是可鉴别的。分组数据源鉴别问题的实质就是这样一个复杂的数学图论问题:在分组随机丢失概率一定的情况下(对应的是分组 Hash 有向图中相应节点的随机丢失概率一定),如何设计分组 Hash 有向图以确保剩下的所有节点和签名节点之间仍然存在至少一条有向路径,同时又使得该图中的总边数(Hash 边)尽可能最少。这就是本文提出的一个公开图论问题,我们称为分组 Hash 有向图鉴别问题[22]。解决该问题需要图论、概率论和最优化方面的知识。希望数学家们来解决这个问题。如果分组 Hash 有向图鉴别问题得到很好解决,我们将能够得到最优的基于分组 Hash 有向图的分组数据源鉴别方案。文[10,20]实际上就是在类似图3的分组 Hash 有向图上研究该图论问题。

Wong 和 Lam[21]利用文[9]的思想提出了一个基于鉴别树的鉴别方案。数据流中每个分组的 Hash 值是该鉴别树的叶节点,所有父节点是对其所有子节点的 Hash 值再求 Hash 值而得到的(例如,可以是把各子节点的 Hash 值连接成一个字串,再对该字串求 Hash 值而得到父节点),根结点是一个数字签名。这种鉴别树和分组 Hash 有向图有相似之处,故列入本节讨论。每个分组都携带了额外信息用于在鉴别树中所有分组到达之前鉴别整个数据链。可以利用缓存技术来加快验证过程。在接收方,该方案没有鉴别时延,需要签名的分组数据也较小。但该方案具有很大的通信开销,因为对每一个分组需要附加一个数字签名和 O(logn)个 Hash 值。Wong 和 Lam 同时提出了一种 Feige-Fiat-Shamir(FFS)签名方案[4,5]的扩展方案 eFFS(extension FFS),在对 eFFS,RSA 和 Rabin 等多种签名算法进行了比较后,Wong 和 Lam 指出 eFFS 具有最好的性能,但是 eFFS 的安全性尚未得到严格证明。

经观察发现 Internet 上大多数分组丢失情况是以类似脉冲串的形式发生[2,13],基于此,Golle 和 Modadugu[7]构造了一个基于分组 Hash 有向图的方案,其目的是在有脉冲式的分组丢失发生的情况下,仍然能够鉴别收到的分组。签名信息包含在待鉴别数据流的最后一个分组中,除签名分组外,每个分组的 Hash 值都存在于数据流中的其它多个分组中。作者证明了对于该种类型的分组丢失模式,其方案是最优的。

Perrig 等提出的 EMSS[14]同样基于分组 Hash 有向图。该方案面向更一般的分组丢失模式，而且提出了解决签名分组丢失问题的方法。与 Golle 和 Modadugu 方案中数据分组之间确定的 Hash 边联系不同的是，EMSS 方案使用随机分布的 Hash 边。而且分组之间的 Hash 链接可以跨越分组块，这样即使属于特定分组块的所有冗余签名分组都丢失了，下一分组块中的签名分组仍然可以用来鉴别分组数据。作者根据数据流的分组丢失特性，进行了多个仿真模拟以得到包含在每个分组中的分组 Hash 值的合适数目。根据网络传输特性，每个分组块中的签名分组都被发送多次，以提高其到达接收方的概率。

Miner 和 Staddon 将 EMSS 方案进行了推广，并提出了一种分组 Hash 有向图：p-随机图[10]。她们给出了依赖于 p 的可鉴别概率的理论下界。在她们的方案中，大部分的分组都携带了 $O(pn)$个 Hash 值(这里的 n 是数据流中的分组数目)，这使得其方案的通信开销很大且可伸缩性较差。她们还提出根据分组的在数据流中的重要程度(例如 MPEG 中的 I 帧，对视频效果至关重要)来区分不同的分组。为了减少通信开销，可以只给地位重要的分组以更高的鉴别概率。

Song 和 Zuckerman 等提出了一个基于 Expander 图的分组 Hash 有向图来鉴别不可靠(有分组丢失)网络上的数据流[20]。其鉴别图中的节点具有恒定的度数同时确保了很高的鉴别概率。通过证明，作者给出了分组到达时，其可鉴别的概率的下界。该下界独立于 Expander 图的大小。

分别基于 p-随机图和 Expander 图的两种方案都利用图论和概率论等相关知识，对基于分组 Hash 有向图的分组数据源鉴别问题作了理论上的研究，但都没有最后解决前面提出的分组 Hash 有向图鉴别问题。

基于分组 Hash 有向图的分组数据源鉴别方案存在如下问题：

1. 不能满足第1节所阐述的挑战之二，即分组的实时/立即签名和鉴别。因为基于分组 Hash 有向图的方案要求在发送方或接收方必须对分组或分组 Hash 值进行缓存，如果签名分组位于 Hash 有向图之首时(例如图1～3)，发送方为了计算数字签名需要将签名分组之后的所有分组进行缓存，然后再逐一计算其 Hash 值，最后得到数字签名值，然后才可以发送签名分组以及其后的所有分组；如果签名分组位于 Hash 有向图之尾，发送方不需要缓存，但是在接收方，需要将其它分组先缓存下来，等签名分组抵达以后再验证是否存在一条从待鉴别分组到签名分组的有向路径(即待鉴别分组是可鉴别的)。有的研究者认为，签名分组位于 Hash 有向图之尾，更容易导致 DoS 拒绝服务攻击[16]。

2. 不能完全满足第1节所阐述的挑战之四，即对分组丢失的完美鲁棒性。在分组丢失频繁的网络中，Hash 图不可能百分之百保证每个分组和签名分组之间都存在一条有向路径(即分组是可鉴别的)。

2.2 基于一次性数字签名(one-time signature)技术的方案

最早的一次性数字签名方案是由 Rabin 提出的[17]，其数字签名的验证需要签名者和验证者之间进行多次交互，而不像其它签名方案，验证过程仅需在验证方执行一次验证操作。Lamport，Diffie，Winternitz 和 Merkle 提出了一些改进方法，参见文[8]。由于一次性数字签名方案基于一般的单向函数并且不使用陷门函数，所以其签名和验证速度远远超过一般的数字签名技术。单向函数(例如 DES 或 SHA-1)的效率远远超过陷门函数(例如 RSA)。然而，一次性数字签名方案并不像传统的数字签名方案(RSA 或 DSA)，一个私钥可以用来对任意数目的信息进行签名，而只能对预定数目(通常是一条)的信息进行签名，其公/私钥对需要不断更新，否则签名可能被伪造。由于大多数一次性数字签名方案的签名和验证都非常高效，因此，其主要应用于智能卡和芯片板卡等计算能力较低的场合。

Gennaro 和 Rohatgi 在文[6]中提出的一种利用一次性数字签名算法鉴别在线数据流的方案。该方案存在如下问题：①当有分组丢失时，随后的所有分组将无法验证。因为后一个分组的验证是利用前一分组提供的一次性公钥来验证。一旦丢失一个分组，整个信任关系的传递过程就被打破，从而导致后续的所有分组无法得到验证。②一次性签名算法的签名密钥(私钥)和数字签名信息太大。

在后续的文[19]中，Rohatgi 扩展了文[6]中的方案，提出使用 k 次数字签名(k-time signature)，其中一对密钥可以在 k 个而不是一个数字签名中使用，同时其签名和验证仍然保持较快的速度。通过离线计算可以进一步提高系统的效率。一个 k 次数字签名的公钥，在多个而不是一个分组中传送，一定程度上克服了文[6]方案存在的问题①。

Perrig 提出了 BiBa 一次性签名算法和广播数据鉴别协议[15]。BiBa 利用无陷门的单向函数，并基于组合数学中球盒问题的思想构造了签名算法。和现有的一次性数字签名算法比较，BiBa 具有很低的验证计算开销(快至少两倍，Perrig 认为 BiBa 是迄今为止在验证速度上最快的签名算法)和较小的数字签名信息。BiBa 分组数据源鉴别协议存在如下问题：①存在和 TESLA 一样的时钟同步问题。在大型组播系统中，由于存在数目巨大的接收者，要保证每个接收方的时钟都和发送方的时钟同步，这本身就是一个富有挑战性的问题。②BiBa 数字签名算法的公钥太大，为了增强算法的安全性，需要增加 SEALs 值，从而也增大了公钥。③虽然 BiBa 签名算法在签名验证方面非常优秀，但是其生成签名的开销较大。

Mitzenmacher 和 Perrig[11]基于球盒问题的思想构造了一个通用的签名方案框架，并提出了几种相关算法，并在此基础上提出了 Powerball 签名方案，该方案对 BiBa 作了稍许改进，稍微提高了 BiBa 的验证速度并减小了 BiBa 的数字签名信息，但是，这些提升的代价是更大的公钥和更高的签名计算开销。

L. Reyzin 和 N. Reyzin[18]提出的方案可以看作是对 BiBa 方案更好的改进，在保持和 BiBa 一样快的验证速度的同时，该方案大幅度提高了 BiBa 的签名效率，其签名速度甚至比验证速度更快，在和 BiBa 相同的安全级别下，密钥和签名信息的大小也有稍许减小。因此看来，该方案应该是利用一次性数字签名算法实现组播分组数据源鉴别的最好选择，其缺点是公钥太大。

利用一次性签名算法实现组播分组数据源鉴别存在的共同问题是：对不同的分组(或一个时间段)，需要使用不同的公/私钥对，这样不断更新公/私钥对的开销是相当大的。

2.3 基于 MAC 码的方案

2.3.1 *基于非对称 MAC 码的方案* 第1节阐明了：MAC 码可以直接应用于组播组内分组数据鉴别，却无法直接应用于分组数据源鉴别。但通过一些变通的方法，人们确实提出了基于 MAC 码的分组数据源鉴别方案。Canetti 等[3]基于 MAC 码提出了一个组播数据流鉴别方案，其中每个分组可以独立地得到验证。发送者从包含 K 个 MAC 密钥的全集中分别选取含有 k 个 MAC 密钥的互不相同的子集分配给每个接收者。发送者在发送每个分组的同时，附加上分别使用 K

个 MAC 密钥对该分组进行 MAC 计算得到的 K 个 MAC 码。每个接收者验证其中对应于其 k 个 MAC 密钥的 k 个 MAC 码，如果其中任何一次验证失败，接收者就拒绝该分组；否则，在假定不存在超过某个阈值数目的接收者进行合谋攻击的情况下，接收者就能确信分组的真实性。该方案具有如下特性：分组的实时/立即鉴别，不需要缓存；每个分组都独立于其它分组单独得到鉴别。但是每个分组的鉴别计算开销可能很大，如果要确保至多 ω 个($\omega \leqslant k$)用户不能实施合谋攻击，那么需要计算 $O(m^{\omega/k})$ 个 MAC 码(这里 m 是接收者的数目，ω 是最大合谋数)。人们称上述方案为非对称 MAC 码或 MMAC。Boneh 等[1]推动了非对称 MAC 码方面的分析工作。非对称 MAC 码不能满足第1节所述的挑战之五和挑战之六，即缺乏可伸缩性，当用户数目巨大时，非对称 MAC 码的计算开销将变得非常大；鉴别信息也将变得非常大(增加了通信开销)。

2.3.2 *基于时间 MAC 码的方案* TESLA 由 Perrig 等提出[14,16]。TESLA 基于 MAC 码，并且能够容忍无界和随机的分组丢失。发送者使用一般的数字签名技术(如 RSA)对数据链的第一个分组进行签名的同时，对一条 MAC 密钥链作出承诺。发送方使用 MAC 密钥 K_i 对分组 P_i 进行 MAC 计算得到 MAC 值，每个 K_i 在数据流中随后的分组中向接收方揭示。该方案的缺陷是需要发送方和每个接收方的时钟保持同步，因为接收方必须确认分组 P_i 是在发送方发送含有 MAC 验证密钥 K_i 的分组之前被接收到，否则 P_i 可能是伪造的。由于时钟同步对于 MAC 密钥链至关重要，故我们统称这类方案为时间 MAC 码方案。在大型组播系统中，由于存在数目巨大的接收者，要保证每个接收方的时钟都和发送方的时钟同步，这本身就是一个富有挑战性的问题。TESLA 不能满足第1节所述的挑战二和挑战四，即实时/立即鉴别和对分组丢失的完美鲁棒性。同时 TESLA 中的签名不具有不可抵赖性。

2.4 基于前向纠错码 FEC 的方案

EMSS 方案中曾利用前向纠错码 FEC(Forward Error Correction)来提高签名分组的接收可靠性。Pannetrat 等[12]提出了一个完全基于 FEC 技术的数据流鉴别方案。该方案可以根据信道的误码特征选取特定的阈值，在分组丢失率低于该阈值的情况下，接收方就可以鉴别数据块。和以前的数据流鉴别方案相比，该方案具有更小的通信开销。该方案存在的问题是：①当分组丢失率很高时，为了避免整个数据块丢失必然增加每个数据块的分组数目，这样必然导致：接收方的鉴别延迟以及发送方的发送延迟增大；发送方和接收方的缓存增大；每个数据块的鉴别标签的计算开销(鉴别标签生成算法)增大。②如果每个数据块的分组数目太小，将导致：数字签名(RSA)的生成和验证过于频繁，为此发送方和接收方将付出巨大的计算开销；同时也增大了发送和验证的延迟。所以在分组丢失率一定的情况下，需要对数据块中包含的分组数目作一个恰当的权衡。

结论 目前，在组播分组数据源鉴别领域，还没有任何研究结果可以同时满足第1节提出的所有六大挑战。每种方案都各有其利弊。如果基于陷门函数的数字签名技术(例如 RSA，ECC 等)获得突破(签名和验证时间很短；签名数据很小)，加上不需要解决公/私钥对的更新问题(常规数字签名技术的一个私钥/公钥对可以用来对无穷条信息进行签名和验证)，就完全可以利用该类数字签名技术对单个分组进行签名(签名计算开销和签名信息的通信开销小)从而构造出满足第1节所提出的全部六大挑战的完美组播分组数据源鉴别方案。但是，短期内想在基于陷门的数字签名技术上获得突破是不可能的。而一次性数字签名算法的研究有可能在近期获得突破性进展(签名和验证时间很短；签名数据很小；一次性公钥很小)，加上再解决好如下问题：在分组丢失频繁的信道上，解决一次性私钥/公钥对的可靠频繁更新问题。完全可以构造出一个同时满足六大挑战的基于一次性数字签名算法的组播分组数据源鉴别方案。只要计算和通信开销等都足够小，完全可以利用这样的一次性数字签名算法为单个分组进行签名。BiBa 一次性数字签名算法和鉴别协议的提出，为我们展示了利用一次性数字签名算法构造完美组播分组数据源鉴别协议的美好前景。

参 考 文 献

1 Boneh D, Durfee G, Franklin M. Lower Bounds for Multicast Message Authentication. Proceedings of Eurocrypt 2001
2 Borella M, Swider D, Uludag S, Brewster G. Internet Packet Loss: Measurement and Implications for End-to-End QoS. In: Proceedings. In: Intl. Conf. on Parallel Processing, Aug. 1998
3 Canetti R, Garay J, Itkis G, et al. Multicast Security: A Taxonomy and Some Efficient Constructions. In IEEE Infocom, March 1999. 708～716
4 Feige U, Fiat A, Shamir A. Zero Knowledge Proofs of Identity. In: Proc. of the 19th Annual ACM Symposium on Theory of Computing, 1987
5 Fiat A, Shamir A. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In Advances in Cryptology-CRYPTO'86, 1987. 186～194
6 Gennaro R, Rohatgi P. How to Sign Digital Streams: [Technical Report]. IBM T. J. Watson Research Center, 1997
7 Golle P, Modadugu N. Authenticating Streamed Data in the Presence of Random Packet Loss. In: ISOC Network and Distributed System Security Symposium, 2001. 13～22
8 Merkle R C. A Digial Signature Based on a Conventional Encryption Funcition, Advances in Cryptology -CRYPTO'87, Pomerance (ed), Lecture Notes in Computer Science, Vol. 293, Springer-Verlag, 1987. 369～378
9 Merkle R. A Certified Digital Signature. In Advances in Cryptology - CRYPTO'89, Lecture Notes in Computer Science, 1990, 293: 218～238
10 Miner S, Staddon J. Graph-Based Authentication of Digital Streams. In IEEE Symposium on Research in Security and Privacy, May 2001. 232～246
11 Mitzenmacher M, Perrig A. Bounds and Improvements for BiBa Signature Schemes: [Technical Report]. Feb. 2002
12 Pannetrat A, Molva R. Authenticating Real Time Packet Streams and Multicasts: [Technical Report]. Institute Eurecom, France, Dec. 2001
13 Paxson V. End-to-End Internet Packet Dynamics. In IEEE/ACM Transactions on Networking, 1999, 7: 277～292
14 Perrig A, Canetti R, Tygar J D, Song D. Efficient Authentication and Signing of Multicast Streams over Lossy Channels. IEEE Symposium on Security and Privacy, 2000. 56～73
15 Perrig A. The BiBa one-time signature and broadcast authentication protocol. In: Proc. of the Eighth ACM Conf. on Computer and Communications Security (CCS-8), Philadelphia PA, USA, Nov. 2001
16 Perrig A, Canetti R, Song D, Tygar J D. Efficient and Secure Source Authentication for Multicast. In: ISOC Network and Distributed System Security Symposium. 2001. 35～46
17 Rabin M O. Digital Signatures, in Foundations of Secure Computation, R. A. DeMillo, et. al. (eds). Academic Press, 1978. 155～168
18 Reyzin L, Reyzin N. Better than BiBa: Short One-time Signatures with Fast Signing and Verifying. In: the Proc. of the 7th Australasian Conf. on Information Security and Privacy (ACISP 2002), July 2002
19 Rohatgi P. A compact and Fast Hybrid Signature Scheme for Multicast Packet Authenticast. In: 6th ACM Conf. on Computer and Communications Security, 1999. 93～100
20 Song D, Zuckerman D, Tygar J D. Expander Graphs for Digital Stream Authentication and Robust Overlay Networks. In 2002 IEEE Symposium on Research in Security and Privacy
21 Wong C K, Lam S. Digital Signatures for Flows and Multicasts. In IEEE/ACM Transactions on Networking, 1999, 7: 502～513
22 刘璟. 大型动态组播系统网络安全服务的若干问题研究: [电子科技大学博士论文]. 2003