IP 组播不可否认数据源认证研究进展

张海波[①②] 周贤伟[①] 宋存义[①]
[①](北京科技大学 北京 100083)
[②](北京服装学院计算中心 北京 100029)

摘 要 数据源认证是组播安全体系中重要的一部分，数据源认证可以分为可否认的和不可否认的两种。该文按照协议分类分别概述了几个具有代表性的不可否认数据源认证协议，并对每一个协议的优缺点和存在问题进行了讨论。对目前IP组播不可否认数据源认证协议进行了总结，并讨论了不可否认数据源认证未来的研究方向和还需要解决的问题。

关键词 IP 组播，数据源认证，不可否认
中图分类号：TP393 **文献标识码**：A **文章编号**：1009-5896(2006)11-2205-04

Progess of the Research on IP Multicast Data Origin Authentication with Non-repudiation

Zhang Hai-bo[①②] Zhou Xian-wei[①] Song Cun-yi[①]
[①](*University of Science and Technology Beijing, Beijing* 100083, *China*)
[②](*Computer Center of Beijing Institute of Clothing Technology, Beijing* 100029, *China*)

Abstract Data origin authentication is an important part in the multicast security architecture. Data origin authentication can be classified as repudiation and non-repudiation. In this paper, several typical data origin authentication protocols with non-repudiation are summarized according to the taxonomy of data origin authentication with non-repudiation. The advantages and shortcomings of these protocols are discussed respectively, also the problems existed are anatomized in depth. This paper is a sum-up of the protocols of data origin authentication protocols with non-repudiation at the present time. The future trend and the remaining problems of data origin authentication with non-repudiation are also discussed.

Key words IP multicast, Data origin authentication, Non-repudiation

1 引言

IP组播(Multicast)是一种允许一个或多个发送者(组播源)一次同时发送单一的数据包到多个接收者(组播组)的网络技术。自从 20 世纪 80 年代Deering提出了组播的概念[1]，并指出IP组播的可能性，20 多年以来，IP组播技术有了很大的发展。IP组播技术被应用到网络视频会议、网络音频/视频广播、AOD/VOD、股市行情发布、多媒体远程教育、CSCW协同计算、远程会诊等方面。

文献[2]认为IP组播的安全一般包括：数据保密、组管理和访问控制、源认证、完整性和不可否认几个方面。数据保密需要保证非组成员不能访问到组播数据。组管理和访问控制要求只有合法的参与方才能获得发给这个组的数据。源认证是本文要讨论的。完整性确认收到的数据并没有在传输过程中被修改过。不可否认是指接收到数据的接收方有能力向第三方证明接受到的数据确实是由发送方发送的，发送方不能否认。

2 数据源认证

数据源认证是 IP 组播安全急需解决的重要问题之一。尽管目前已经存在很多数据源认证方法，但数据源认证仍然在数据传输、完整性、有效性和运行能力方面面临着挑战。实际上，散列(hash)函数、消息码和数字签名分别是数据完整性、数据源认证和数据传输不可否认的密码学方法。但是这些方法已经被设计成点到点的传输，如果应用到组播中会产生无效性和不适合性。这些认证方法的不适合之处主要有两个方面：大规模组播组时组成员的大量增加和实时传输时要求数据的连续性。

在组通信时可以把认证分为两种[3]：一是组认证，即确保组成员接收的组播消息来源于有效的组成员(而不考虑它的身份)。为了保证组认证，一般情况是组成员采用一个共享的密钥，这个密钥一般叫做组密钥。二是数据源认证，即确保组成员接收到组播消息来源于一个有特定身份的源。一般情况下，数据源认证分为两个层次。

第 1 层次仅仅保证组播数据源认证，在这种情况下，一个发送者需要利用不对称机制允许接收者去验证组播消息，而不用可信认的第三方对消息的有效性进行证明。目前一些方法建议利用不对称密钥来认证消息，但这种方法容易受到共谋的攻击，而且不能做到不可否认。

第 2 层次除了确保数据源认证外，还确保不可否认。由

2005-04-07 收到，2005-12-30 改回
国家自然科学基金项目(60573050)和北京市优秀人才培养专项基金(20042D0500103)资助课题

于目前的数字签名机制计算成本非常高。因此，把每一个组播流的包都进行签名非常不实用。大多数提出的方法都基于把每个组播包都分组后用单个数字签名进行签名。这种签名和它的分期性导致了一些额外的信息叫认证信息。由于大多组播数据流的应用没有使用可靠的传输层，因此，一些包也许会在传输过程中被丢失。所以，刚才提到的方法就产生了认证信息的冗余，利用这个方法，即使有些包被丢失，为了认证接收到包的真实性，必需的认证信息可以被恢复。在这种情况下，被冗余认证信息导致带宽增加。目前提议的方法用来对付如何在带宽和忍受包丢失之间取得均衡。

由以上可知，数据源认证协议可以大体上分为两类：一是可否认的，一是不可否认的。本文重点讨论不可否认的数据源认证。

3 不可否认数据源认证

为了对一个消息确保数据源的不可否认，发送者不得不用它的私钥对消息进行签名。因此，为了确保组播不可否认的数据源认证，一个很自然的方式就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个分组进行签名和验证，使用一般的数字签名技术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，特别是在实时传输的场合(例如现场直播、视频会议等)，如果直接使用一般的数字签名技术，很难实现高效的数据源认证。而不可否认数据源认证协议试图对这些问题进行改进或解决，目前提出的协议可以分为 3 类：递归签名、分散签名、不同签署。

3.1 递归签名

这类方法是仅仅签署一小块信息，这样就减少了数据源认证包的数量。后面的包依次携带校验其他包的数据源真实性的信息。每一个包携带可以校验其他数据包的认证信息。这种包之间递归的关系在某种程度上使得这个单一的数字签名的影响普及覆盖到所有的有关系的包，故这种方法可以被称作递归签名。

递归签名可以分为可以容忍包丢失和不能容忍包丢失的两种。不能容忍包丢失的协议目前典型的有文献[4,5]提出的简单离线链协议(simple off-line chaining)和在线签署(on-line signing)协议；能容忍包丢失协议的有文献[6]提出的 EMSS 协议(Efficient Multi-chained Stream Signature)、文献[7]提出的 p 随机认证协议(The p-random authentication scheme)，文献[8]提出的周期链方法(periodic chaining approach)，文献[7]提出的 piggybacking 协议。

简单离线链协议把数据流分成若干个块(block)，并假定发送者提前在离线状态就知道全部数据流。利用这个方法，发送者仅仅需要对第一个块进行签名，然后发送者在当前数据块插入随后数据块的 hash 值，也就是说把第 i+1 个块的认证信息插入到第 i 个块中，然后发送出去。接收者首先验证第 1 个块的数字签名，然后就可以对随后的块进行依次验证，也就是说认证第 i+1 个块需要它在第 i 个块中的认证信息。这个方法的优点：一是提出了仅仅利用 hash 链的方法对第一个块进行签名；二是接收者可以及时对接收到的块进行验证。缺点是不能容忍包丢失和发送者需要提前知道全部的数据流。

为了让发送者不需要提前知道所有的数据流，在线签署被提了出来。该方法假定发送者事前不知道全部数据流，每一个数据块携带着随后数据块一次签名的一次公钥。这样只要签署了第一个数据块，整个流随后的数据块就可以被验证。这个方法的优点：一是采用了一次签名，计算量减少；二是支持接收者及时对数据流进行验证；三是发送者不需要提前知道全部数据流。缺点是不能容忍包丢失和一次签名数据量比较大。

EMSS 协议引入了“冗余 hash 链接”(redundant hash-chaining)的概念，也就是说数据流的每一个包和其他几个包进行 hash 链接，而这几个包是该包的目标包(target packet)。这样即使有一些包被丢失，一个接收到的包可以通过哈希链接路径把链接的丢失包恢复过来。EMSS 提供了一种对付包丢失的随机的稳健性。最大的缺点是接收者为了验证需要缓存数据包，这样数据包就不能得到及时验证；另外周期性的签名不适合计算能力限制的设备。

p随机认证协议提供了一种冗余和随机的hash链接，该链接用来容忍网络中独立丢包概率为q的包丢失，原作者假定发送者事先知道关于传输内容的知识，在数据流的第一包发出前建立“hash链接拓扑”，这个任意冗余拓扑被原作者称为“p随机图”，数据流的包可以假设为$P_1,\cdots,P_n$。P_1是签名包，对所有的包(P_i，P_j)(i<j)，P_i的hash值以概率p被插入包P_j中。一旦“p随机图”建立起来，数据流的包就被分别发送出。一个接收者通过签名包开始接收数据包，假如这个包是有效的，接收者通过检查接收到的数据包与签名包之间hash链接的存在来验证随后的包。原作者证明在一个独立随机包丢失的网络中，每一个包P_i认证的可能性与该包在数据流中的位置i有关(详见原文)。接收者可以及时验证接收到的包，而发送者为了建立“p随机图”需要提前缓存所有的数据流。认证信息的多少依赖于参数p。

周期链接方法利用一个和 EMSS 类似的策略，但是一个给定包的目标包选择是确定的，而不是随机的。这种确定的拓扑机制被设计成抵抗突发丢失(burst loss)。实际上网络上连续的包更趋向于突发丢失。该方法的目标是使认证方法可以忍受最长的单个突发丢失的范围最大化，当一些包在突发丢失后被接收到，这个方法可以恢复并在进一步包突发丢失时维持认证。为了建立包之间的 hash 链接，发送者需要缓存一些包来创造它们之间的 hash 链接。该方法的优点是可以抵抗包的突发丢失。缺点一是限制较死；二是发送者需要缓存 P 个数据包，不太适合实时组播。

Piggybacking 协议也基于 hash 链接技术，设计专门用来对付多重的突发丢失，这个协议适合这样的情况：不同包携带的数据对应用层具有或多或少的重要性。因此，包被构成不同级别的组。于是，hash 链接在某种程度上做在优先级越高的组，那些包就有越多的冗余 hash 链接，这些都是为了更好地对付突发丢失。优点是可以对付包丢失。缺点一是不容易实现；二是要求发送者和接收者都要缓存，不适合多媒体实时传输。

3.2 分散签名

这种方法的思想是仅仅签署一小块信息，并把发生的认证信息都分散到一系列包中。然后，每一个接收到的包拿出它分配的认证信息去重建校验数据源认证的整个必需的信息。分散签名典型的有文献[9,10]提出的树链协议(tree-chaining)和文献[11,12]提出的 SAIDA(Signature Amortization using IDA)协议。

树链协议要求每一个包携带要求认证的信息，这样就可以单个认证。也就是说即使 n 个包中 n–1 个包丢失了同样可以认证。数据流的签名是一块一块进行的。一个块含包的数量 m 的大小依赖于在周期 T 中能够传输的包的数量。正如以上介绍的事例，为了阻止一个包携带认证信息的全部拷贝，块中包的摘要通过“额外 hash 处理”被构成“树”。该协议优点是可以容忍包丢失。缺点是每一个包携带的认证信息量较大和需要计算量大的数字签名。

SAIDA协议是为了减少每一个包携带认证信息的量，采用了IDA(Information dispersal Algorithm)[13]来分散n个块的n个hash值，又把块签名分成n片，以这样的一种方式，n片中的n–m个片丢失的情况下也可以被重建。这个协议实现了在认证信息和带宽之间得到平衡。缺点一是由于IDA处理量大，所以需要较高的计算量；二是为发送者和接受者都带来延迟。

3.3 不同签署

这种方法是仅仅签署一小块使用的信息(密钥)，然后利用这个密钥去依次签署数据包，但是这时使用的是一次签名(one-time signing)，一次签名被认为是计算成本不高的一种密码学方法。不同签署典型的有文献[14,15]提出的在线/离线数字签名(on-line/off-line digital signature)协议。

在线/离线数字签名协议是离线签署密钥，然后高速缓冲起来以备将来使用。被缓存起来的密钥利用一种快速的密码学方法(比如一次签名)在线认证消息。故此，离线签署不干扰多媒体流实时传输。优点是可以容忍包丢失和消息可以及时验证。缺点是接受者不得不验证一个传统的数字签名，这个传统的数字签名也许对很多计算能力限制的设备是不太适合的；另外一次签名需要较大的带宽。

4 结束语

数据源认证是IP组播安全的一个重要方面。但是面临的很多问题限制了数据源认证方案的设计和实施，比如：巨大的组播组成员和大量的数据传输要求组播应用具有可伸缩性；容忍包丢失并仍能进行有效的认证；对计算能力限制的设备(比如PDA或笔记本电脑)的适用性；等等。显然满足所有的限制和要求是很困难的，因而目前还没有最好的解决方法，但是学者也提出了针对特殊要求的一些比较好的解决方法。虽然组播技术已经发展了20多年，但是在不可否认数据源认证这个领域仍有难题需要解决。

⑴ 实时传输时的高效组播问题。很多提出的解决方案在容忍包丢失和带宽之间取得平衡，所有的这些方法无论是对发送者还是接收者来说都需要时延。研究不需要包缓存、把时延减少到最小的影响的不可否认的协议目前仍然是一个焦点问题。

⑵ 在多对多通信时，高效组播的问题变得更加恶劣。根据现有的协议，接收者将不得不管理每一个源的包缓存，另外，保存发送者的公钥对资源限制的设备来说也是一个问题。这些问题只有随着密码学技术的发展才有可能解决。

⑶ 对于包丢失的适应性，包丢失率可以随着时间的推移根据网络的状况和拥塞情况而变化。此外，在整个一个大的网络环境中还不能做到重新统一分配包丢失。因此，为了更好地在容忍包丢失和其他性能之间取得平衡，在设计数据源认证协议时考虑包丢失率的变化是很重要的。

⑷ 在移动网中，当考虑到移动组播接收者时，共谋攻击问题变得更加突出。另外，时间的不对称机制在移动网中根本就没有效率可言，因为包时延随着移动网络的拓扑结构的变化而变化。

参 考 文 献

[1] Deering S E, Cheriton D R. Host groups: A multicast extension to the Internet protocol. (RFC966), Dec,1985.

[2] 赵膺，宋佳兴，徐万鸿，刘卫东. 安全组播综述[J]. 小型微型计算机系统，2003, 24(10): 1873−1877.

[3] Hardjono T, Tsudik G. IP multicast security: Issues and directions. Annales de Telecom, July-August 2000: 324−340.

[4] Gennaro R, Rohatgi P. How to sign digital streams. *Information and Computation*, 2001,165(1):100–116.

[5] Gennaro R, Rohatgi P. How to sign digital streams. Proceedings of the 17th Annual International Cryptology Conference, Advances in Cryptology – Crypto’97, 17–21 August 1997, vol. 1294 of ‘Lecture notes in computer science,’ Springer: 180–197.

[6] 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, May, 2000: 56–73.

[7] Miner S, Staddon J. Graph-based authentication of digital streams. IEEE Symposium on Security and Privacy, Oakland, California, USA, May, 2001: 232–246.

[8] Golle P, Modadugu N. Authenticating streamed data in the

presence of random packet loss. In Proceedings of the Symposium on Network and Distributed Systems Security (NDSS 2001), the Internet Society, San Diego, USA, Feb, 2001: 13–22.

[9] Wong C K, Lam S S. Digital signatures for flows and multicasts. in Progress of IEEE Internet Conference on Network Protocols, AICNP'98, Austin, Texas, USA. Oct. 1998: 198−209.

[10] Wong C K, Lam S S. Digital signatures for flows and multicasts. *IEEE/ACM Transactions on Networking*, 1999, 7(4): 502 – 513.

[11] Park J M, Chong E K P, Siegel H J. Efficient multicast packet authentication using signature amortization. IEEE Symposium on Security and Privacy, Oakland, California, USA, May, 2002: 227–240.

[12] Park J M, Chong E K P, Siegel H J. Efficient multicast stream authentication using erasure codes. *ACM Transactions on Information and System Security*, 2003, 6(2): 258−285.

[13] Rabin M O. Efficient dispersal of information for security, load balancing, and fault tolerance. *Journal of Association for Computing Machinery*, 1989, 36(2): 335−348.

[14] Even S, Goldreich O, Micali S. On-line/off-line digital signatures. Advances in Cryptology——CRYPTO '89, Lecture Notes in Computer Science, (G. Brassard, ed.), Springer Verlag, 1990, vol. 435: 263−275.

[15] Even S, Goldreich O, Micali S. On-line/off-line digital signatures. *Journal of Cryptology*, 1996, 9(1): 35–67.

张海波： 男，1970年生，工程师，博士生，研究方向为信息与网络安全、IP组播、计算机应用，已在核心刊物上发表学术文章十余篇.

周贤伟： 男，1963 年生，博士后，副教授，通信工程系主任，主要从事下一代网络通信、网络安全、密码学的教学和研究.

宋存义： 男，1951 年生，博士后，教授，博士生导师，环境工程系主任.