计算机科学2000Vol. 27№. 6

基于 IP Security 的安全多播体系结构的研究与分析*)

Research and Analysis of Secure Multicast Architecture based on IP Security

许 强 李信满 赵 宏
(东北大学软件中心 沈阳 110006)

Abstract On the base of analyzing the security problem of the current IP multicast research and application, this paper introduces an architecture of secure IP multicast based on IPSec, identifies the basic components and functions and specifies how these components interact with each other and the surrounding systems. Especially, the group key management mechanism is analyzed and compared in detail. This architecture takes advantage of the IPSec mechanism and expands it. Therefore, the simplicity, flexibility, and ease of incorporation within existing systems are its main features.

Keywords Multicast, Security, IPSec, Architecture

1 引言

随着分布式多媒体及分布式处理的发展、多播逐渐成为构建面向群组服务平台的一种重要通信模式，并且得到了成功的应用。然而，目前的多播平台对于安全问题考虑得比较少，在一定程度上存在着安全隐患。例如，在 Internet 及 ATM 等集成网络中，多播流量与其他网络流量共享网络资源。这样虽然能够快速地建立并维护多播会话，但是也产生了严重的安全与信任问题。在基于 Internet 的 IP 多播中，普遍缺乏会话访问的安全控制机制及安全管理机制，不能对群组成员动态地加入和删除一个会话进行处理、不能对支持多播的主机和路由器进行安全管理。因此，迫切需要构建一种安全 IP 多播体系结构。目前，安全 IP 多播体系结构应该提供如下的基本安全保证。

1)群组成员控制与机密性：保证了只有合法的群组成员才能访问群组通信。

2)群组数据的认证：保证了群组成员能够对与之通信的群组内数据源进行验证。

3)个体数据源认证：群组成员能够验证向群组发送数据的发送者标识。

由于不同多播应用特征及安全需求的不同，也就不可能存在一种单一的解决方案能够处理所有可能的应用。因此，这里给出了一种适于大多数 IP 多播应用的基于 IPSec 的基本体系结构框架。

2 体系结构框架

安全 IP 多播体系结构设计的基本目标是简单性和灵活性，并且易于集成到已存在系统中。为了实现该目标，这里采用了如下的设计策略：

1)安全体系结构应该尽量独立于下层的路由机制。数据包可以通过任何多播或单播路由来传输。为了设计上的简单和模块化，这里假设密钥管理机制建立在可靠通信基础上，并不需要说明获得可靠性的相应机制。

2)尽量利用已有安全技术与组件，保证操作系统内核修改最小，在体系结构设计上，采用 IPSec[1~3]中将数据处理模块与密钥管理模块尽量分离的策略。对于安全组件，本框架采用了 IPSec 的 AH[2]和 ESP[3]协议进行数据的认证与加密。此外，新的多播安全组件主要放在应用层中并与操作系统本身具有的 IPSec 组件一起实现多播安全。

3)加密算法和密钥管理方案选择的灵活性。通过采用 IPSec 的数据传输机制，本框架在数据加密和认证算法方面保持了较好的灵活性。此外，本文定义的新安全组件，如：多播密钥交换模块(MIKE)和源认证模块(SAM)为大多数的群组密钥管理和源认证方案提供了足够的灵活性。

安全 IP 多播主要涉及两类对象：一种是参与安全多播通信的群组成员；一种是管理群组密钥和访问控

*)国家"863"高科技计划资助项目。许 强 博士生，研究领域：网络安全、电子商务。李信满 在职博士生，研究领域：网络安全。赵 宏 博士，教授，博士生导师，主要研究领域：分布式多媒体技术、网络安全。

制的管理员。其中，管理员依赖于群组管理控制和密钥管理机制。

本安全多播框架分为控制平面和数据平面两个功能部分，如图1所示，控制平面的主要功能是管理群组成员关系，执行优先访问控制；数据平面主要处理多播数据分布和加密操作。从应用的角度看，安全多播框架为安全多播提供了一个简单的 API。该 API 逻辑上简单地分为数据 API 和控制 API；其中，数据 API 主要处理多播数据的安全接收和发送；控制 API 主要负责安全多播群组的加入和离开处理以及相关访问控制和密钥更新功能。

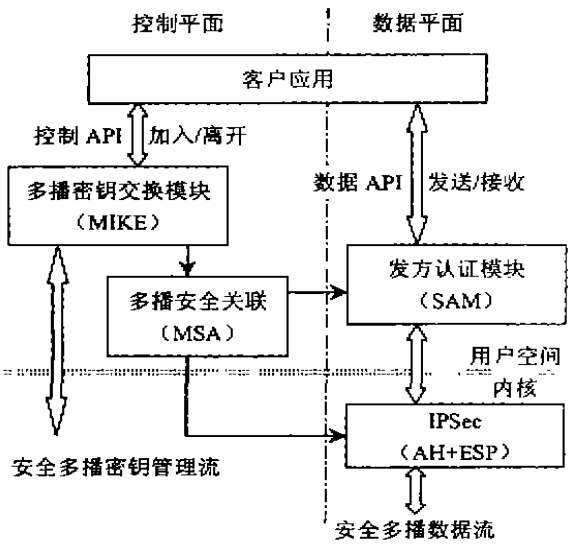

图1　安全多播框架

2.1　安全多播框架构成模块

安全多播体系结构主要由以下模块构成：

1. 多播密钥交换模块 MIKE　该模块主要负责密钥管理，实现允许加入/离开安全多播群组的控制 API。该模块位于应用层，不在操作系统内核中。成员的 MIKE 与群组管理员的 MIKE 交互以产生和维护一个多播安全关联（MSA）。该安全关联包括：数据加密/解密及认证的群组密钥，数据的源认证签名/验证密钥，及其他与连接相关的信息。MIKE 的另一个功能是当 SAM 的群组密钥改变时，周期性地更新 MSA。

2. IPSec 模块 AH/ESP　驻留在操作系统内核中的 IPSec 模块主要负责数据包的加密/解密和认证。这些模块提供了输入/输出多播数据的加密/解密和群组认证。ESP 头部与在单播条件下定义的一样：位于 ESP 头部前的协议头部在 IPv4的 Protocol 域或 IPv6 的 Next Header 域的值为50，而其目标 IP 地址为 IP 多播群组地址。因此，数据包将被具有多播传输功能的路由器前向转发到群组的所有成员。ESP 可以与 ESP 的认证选项协作使用，理论上，多播流量的 ESP 可以运行在传输和隧道两种模式下。

多播数据认证根据认证对象的不同（即：对于群组发送者还是个体发送者）而采用不同的认证技术。对于群组认证，针对单播的 AH 协议和 ESP 协议就已经足够了。群组管理员产生一个为所有成员共享的公开、对称的认证密钥。该密钥用于产生消息认证码（MAC）。AH 协议保留了单播情况下的定义：位于 ESP 头部前的协议头部在 IPv4 的 Protocol 域或 IPv6 的 Next Header 域的值为51，而其目标 IP 地址为 IP 多播群组地址。SPI 值由群组管理员为 ESP 选择。

3. 源认证模块 SAM　该模块主要负责接收数据源的认证和防止重放攻击。大规模的源认证涉及多个输入/输出数据包的操作。其中，UDP 数据包是理想的认证单元。因此，SAM 模块应位于协议栈的高层，即位于 UDP 上的应用层。另外，将 SAM 放在应用层避免了操作系统内核的修改。

SAM 的内部结构很大程度上依赖于所采用的源认证机制。目前，主要存在两种源认证机制。一种是采用公开密钥签名，一种是采用多密钥对称认证机制。SAM 另一个潜在的功能是提供数据的重放保护。这主要是因为 IPSec 的重放保护机制在多发送者条件下不能使用。

2.2　安全多播框架的数据流和控制流

假设数据发送/接收可以通过可靠/不可靠的 IP 多播。群组成员通过调用控制 API 的加入操作来初始化一个会话。这使得成员以发送者/接收者或者两者兼得形式在群组中注册。随后，成员使用数据 API 的发送/接收功能安全地发送和接收数据包。群组密钥管理，数据加密/解密及群组/源认证等所有功能由安全多播框架管理，并且对于成员是透明的。如果在某一时刻一个成员要离开安全多播群组，那么将调用控制 API 中的离开操作。

1. 控制流

——客户加入：应用程序调用 MIKE 来加入一个多播群组。至少该应用程序应该标识希望加入的群组，并提供认证服务所需要的信息，例如，是否需要源认证。

MIKE 接下来执行向群组管理员的注册机制：建立一个多播安全关联，调用 IP 多播群组的标准注册机制，并使 ESP/AH 和 SAM 模块开始处理数据。

注册过程将不可避免地包含与群组管理员的通信，并且该通信将需要参与方的认证机制和确保交换信息的机密性。这种通信，认证和加密机制应该在

MIKE 模块内部处理。

在加入过程的最后，需要建立一个多播安全关联，则来自 MSA 的相关信息将被传入 ESP/AH 和 SAM 模块。

——密钥更新：密钥更新消息是 MIKE 的内部消息，而不是高层体系结构的一部分。它们被单独地认证和加密。一种特定类型的密钥更新消息包含有成员排斥消息，即：群组管理员将某一成员驱逐出群组。该过程是独立于密钥管理协议的，但是将导致被加密的成员不能发送/接收来自安全多播群组的消息。在这种情况下，MIKE 模块应该将排斥消息作为成员在没与群组管理员协商的情况下离开群组来处理。

——客户离开：首先，MIKE 调用群组管理员的注销例程。其次，删除多播安全关联。最后，主机执行离开 IP 多播群组的标准例程。

2. 数据流

——发送数据：如果不需要源认证，那么数据将直接通过 UDP(或其他可靠多播层)和 IP 层的 IPSec 模块传输给 IP 多播群组内的目标地址。

如果需要进行源认证，那么数据首先传输给 SAM 进行源验证。接下来，数据直接传输给内核中的 AH/ESP 变换。这些变换与 MSA 中的群组密钥一起执行。最后，数据包以标准方式发送到通道上。

——接收数据：输入数据包首先由内核中 IPSec 的 AH/ESP 变换处理，主要进行解密和群组认证的验证。接下来，数据流由 SAM 处理，并且源标识被认证。最后，数据由调用应用例程处理。

2.3 多播密钥交换模块 MIKE

多播密钥管理模块作为该安全多播框架的核心应该满足如下的设计需求：

1)MIKE 应该既支持单一群组管理员与所有群组成员的通信情况，也应该支持具有中间服务器中继通信的复杂情况。

2)MIKE 应该支持为所有群组成员共享的密钥集合。此外，MIKE 将帮助前传群组中管理员和发送者的公共验证密钥以支持源认证。

3)MIKE 应位于通信模型的应用层，而不是位于操作系统内核中。

4)MIKE 应具有广泛的灵活性，支持任何合理的多播群组密钥管理解决方案。

因此，一种满足上述安全需求的 MIKE 体系结构框架如图2所示。该框架为不同的群组密钥管理模块提供了一个即插即用的接口。这样，基于不同群组密钥管理技术的模块可以灵活地集成到 MIKE 框架中，例如：下面将要介绍的多播密钥管理模块(MKMM)。

2.4 群组密钥管理

群组密钥管理主要研究如何为所有群组成员建立和管理一个公共密钥，目前主要有五种基本方法：GKMP[4,5]协议，SMKD[6]方案，安全分布树[7]，MKMP 协议及 MKMM 机制。

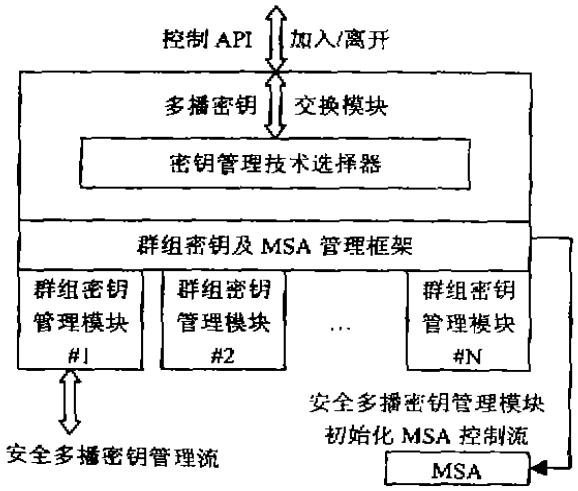

图2 多播密钥交换模块

GKMP 协议是一个为多播群组成员产生并维护相应密钥的应用层协议。在该协议中，每个多播群组具有一个指定的群组管理员(GC)，主要负责管理群组密钥。该 GC 在一个选定的群组成员加入时产生一个群组密钥。此后，该 GC 与每个群组成员接触以确认其有效性，并将群组密钥经 GC 与其成员之间互斥共享的密钥加密发送给成员。由于只有一个单一实体 GC 负责向所有的群组成员发送密钥，所以该方法不适于大规模群组的情况。

SMKD 是基于 CBT 路由协议的密钥分配方案，提供了如何在大规模群组条件下安全地加入一个 CBT 群组树的解决方案。当一个 CBT 群组初始化，树的核心象群组管理员 GC 那样操作以产生群组会话密钥及密钥分布密钥。由于路由器加入了传输树，所以路由器就被委托对于加入的成员进行认证并提供群组密钥。该方法具有高度的规模性。但是，由于位于传输树中的每个路由器获得了具有与群组管理员一样的密钥，所以该方案不能保证当群组树中出现不可靠路由器时的高度安全性。

Iolus 系统采用了"安全分布树"的方法来处理大规模性的问题。多播群组被分解成若干层次的子群组。由一个群组安全管理员(GSC)管理顶层群组，而由群组安全中介(GSI)负责管理不同的子群组。每个子群组具有自己的子密钥。一个 GSI 只知道自己子群组的密钥和上级子群组的密钥，因此就能够在上下子群组

之间"传译"消息。该方法的一个缺点是由于 GSI 对于数据包的解密和加密所带来的时延，而且删除一个不信任的 GSI 也是十分复杂的。

MKMP 密钥管理协议使得初始群组密钥管理员将密钥分配授权以一种动态的形式委托给其他方。它首先产生一个群组密钥，接下来通过发送一个征求消息给多播群组中的各方以确定接受密钥分配授权的委托方。该消息包含了仅由被征求方能够解密的密钥和访问列表。这样委托方就能够象群组密钥管理员一样工作了，这种动态方法具有群组拓扑能够适应在线变化的优点。MKMP 在整个群组中使用了单一密钥，也就不能支持负载的跳-跳之间的解密/重加密。

最后，讨论一种独特的群组密钥管理机制——MKMM 机制。MKMM 尽可能地采用了 IPSec 和 IKE 等已存在的解决方案和标准，如图3所示。例如，该模块使用了 IPSec 为所有的主机与管理员之间的点到点通信建立安全通道。

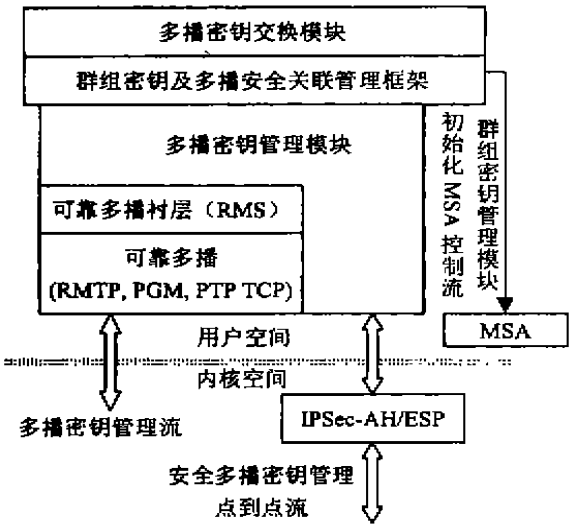

图3 群组密钥管理模块

群组成员与管理员之间的点到点通信由 IKE 建立的标准 IPSec 连接来保证其安全性。该连接既保证了交换信息的机密性，又保证了认证性。特别地，群组密钥及附加信息将以数据的形式在安全连接中传输，群组成员与管理员之间 IPSec 的 SA 将不会持续到多播群组的整个生命期。

从群组管理员到群组成员的密钥更新消息采用了一种抽象传输机制——可靠多播衬层(RMS)。这种抽象机制提供了可靠的多播机制，即保证了任何经过 RMS 传输的消息能够到达所有的群组成员。该 RMS 机制可以由任何可靠的多播机制或者点到点的可靠通信(TCP)来实现。

管理员发送的密钥更新消息具有特殊的格式，特别地，密钥更新消息通过可验证的公开密钥签名进行认证。MKMM 具有自己的签名验证机制，主要在成员注册时使用公钥进行处理。

3 IKE 和 IPSec 的相关问题

3.1 IKE 的使用

通常情况下，群组密钥管理协议与点到点通信的密钥管理不同。因此，IKE 不能用于群组密钥管理中，但是，当需要在两个实体之间建立点到点安全关联时，多播的密钥交换模块可以采用 IKE。

类似地，多播的源认证问题需要采用与 IPSec 不同的解决方案。这里，框架中的源认证模块(SAM)尽量采用已存在的数字签名和数字证书标准。

P3.2 MSA 的标识

在 Internet 协议中，安全关联(SA)由目标地址，安全参数索引(SPI)和所用协议(AH,ESP)唯一标识。由于目标地址既可以是单播地址又可以是多播地址，所以 MSA 的定义与 SA 是一样的。

3.3 SPI 的分配

在单播 SA 中，为了避免 SPI 值潜在的冲突，接收者主要负责 SPI 的分配。由于多播中存在着多个目的地并且属于相同的多播地址，所以上述方法就需要所有的接收者相互协调，难以实用。而由发送者选择也存在着问题，特别是在多群组发送者的情况下。

在本框架中，充分利用中心管理员的作用，使得群组管理员为每个多播群组选择 SPI 并在注册阶段传递给成员，发送者和接收者。这就保证了 SA 由 SPI 值，多播群组地址及所用协议合并的唯一标识。

RFC2401[1]中规定到一个多播群组的多个发送者应该为到该群组的所有流量使用单一的 SA。在这种情况下，接收者只能知道消息来自一个已知多播群组安全关联数据的系统。多播流量也应该为到多播群组的每个发送者使用一个不同的安全关联。发送者 SA 的分配由群组管理员负责。

3.4 序列号的处理及重放攻击的预防

根据最近的 ESP 和 AH 草案，ESP 和 AH 的头部包含有一个强制、单调增长的序列号域以提供反重放攻击。序列号的处理主要由接收者来完成，但是发送者必须经常传输序列号。发送者和接收者的计数器在 SA 建立时必须初始化为0，而且 SA 的第一个数据包的序列号将为1。

在使用同一个安全关联的多个发送者情况下，序列号的一致性和单调性将难以保证。因此，在ESP的

(下转第54页)

4 实验结果

基于邮局模型的消息传递代理中间件系统已在自主车辆体系结构仿真中得到应用，分别在 SGI 的 IRIX、Sun 的 SunOS 及 Microsoft 的 Windows NT 操作系统中开发了相应的软件，连接异质平台，形成统一的分布式计算环境。实验结果表明，系统的稳定性和实时性均达到预期的效果。表1和表2分别列出了中间件在网络传输及客户端应用 Agent 的消息响应时间。

表1 网络传输时间(单位：毫秒)

	O2↔Sun	Sun↔Pentium	Pentium↔O2
1K 字节	1.034	1.273	1.227

表2 客户端 Agent 消息响应时间(单位：毫秒)

	O2工作站	Sun Sparc 工作站	Pentium 166/NT 平台
阻塞被唤醒	0.140	0.960	0.253
事件类消息	0.250	1.906	0.379

其中阻塞被唤醒的响应时间是指客户端进程在因信箱为空被挂起后又因为新消息到来而被唤醒的时刻与消息传递代理将此消息放入信箱时刻的差值；事件类消息的响应时间则是指客户端进程调用事件类消息函数时刻与收信 Agent 收到事件类消息时刻的差值。

网络传输时间是在带宽为10Mbps 的以太网中测试得到，每条消息的大小为1K 字节。在这里，串口通讯的时间没有给出，这是因为串口通讯是点到点的，不存在传输冲突问题，其速度与串口的传输波特率基本吻合。

上述实验结果表明，消息传递代理系统保证了 I-RASO 体系结构中的 Agent 实现实时通信，去除了异质平台给通信带来的影响，构成了方便系统集成的分布式计算环境。

参 考 文 献

1 Shoham Y. Agent Oriented Programming. Artificial Intelligence，1993，60

2 Decker K S Distributed problem-solving techniques. A survey. IEEE Transactions on Systems, Man, and Cybernetics, Vol. 17(5)

3 Sahota M K Reactive deliberation: An architecture for real-time intelligent control in dynamic environments. In: Proc of 12th National Conf on Artificial Intelligence, AAAI'94

4 Sunderam V S, et al. The PVM concurrent computing system: evolution, experiences and trends. Parallel comput, 1994, 20(4)

5 Object Management Group. The Common Object Broker, Architecture and Specification, Object Management Group, Framingham, Mass, 1998

6 吴春明，张友军，朱淼良. 分布式自主移动机器人集成环境. 软件学报，1997，8(10)

7 张友军，吴春明，朱淼良. 自主式移动机器人流水线调度模型的设计与实现. 电子学报，1998，26(2)

8 Lewandowski S M. Frameworks for Component-Based Client/Server Computing ACM Computing Surveys, 1998, 30(1)

9 Tanenbaum A S. Operating Systems: Design and Implementation, Prentice-Hall International, Inc., 1997

(上接第67页)

最近草案中声明采用单一 SA 的反重放攻击服务将不能应用于多个发送者的环境中，多播安全的实现应该保证接收者不执行序列号的处理和验证。

为此，给出两种重放攻击的保护机制：(1)使用多个 SA，即：所有的 SA 是单一 MSA 的一部分，而且每个发送者具有一个 SA。(2)将反重放攻击保护放到诸如 SAM 等高层模块中。该方案就需要对于多播消息进行应用层成帧。

3.5 IPSec 对于多播包的处理

目前，现有的 IP 协议栈的实现将丢弃任何目标地址为 D 类且协议域不是 UDP 的 IP 包。所以，需要对其加以改进以便支持由 IPSec 保护的 IP 多播包。

结束语 从分析目前 IP 多播通信的安全需求出发，本文在对 IPSec 安全机制进行深入研究的基础上，讨论了一种安全 IP 多播体系结构框架，标识了其基本组成部件及功能，并说明了这些部件之间以及与运行环境之间的操作关系。进而，结合我们在 IPSec 上的研究成果，将该体系结构框架在 Linux 平台上进行了设计与实现。实验表明，该体系结构框架扩展性强，具有简单性，灵活性，及与现有系统易融合的特点。

参 考 文 献

1 Kent S. Security Architecture for the Internet Protocol. RFC2401, Nov 1998

2 Kent S. IP Authentication Header. RFC2402, Nov. 1998

3 Kent S IP Encapsulating Security Payload (ESP) RFC2406, Nov. 1998

4 Harney H. Group Key Management Protocol (GKMP) Specification. RFC2093, July 1997

5 Harney H Group Key Management Protocol (GKMP) Architecture RFC2094, July 1997

6 Ballardie A Scalable Multicast Key Distribution. RFC 1949, May 1996

7 Mittra S. Iolus: A Framework for Scalable Secure Multicast In: Proc. of ACM SIGCOMM'97, Cannes, France, Sep. 1997