SLM——一种安全分层组播协议

陈 越,兰巨龙,郭云飞,赵昭灵
(信息工程大学,河南郑州 450002)

摘 要: 流媒体分发的一种典型实现方法是采用具有接收方驱动拥塞控制机制的分层组播.由于目前分层组播拥塞控制协议缺乏对用户行为的限制,接收方可违规订阅上层组播组发起自利型攻击,导致非公平的带宽利用.本文提出了一种较通用的安全分层组播协议 SLM (Secure Layered Multicast).在路由器辅助拥塞控制条件下,在边界路由器采用基于 Shamir秘密共享体制的拥塞状态相关访问控制 (CR-AC, Congestion state Related Access Control)算法,管理用户组订阅行为,避免了用户自利型攻击,并使服务提供商可根据其与用户的协约限定不同用户的最高订阅级别.分析和仿真实验表明,该协议可实时保证网络流量安全共享带宽并具有较好的可扩展性.

关键词: 分层组播; 拥塞控制; 自利型攻击; Shamir's秘密共享体制
中图分类号: TP393 文献标识码: A 文章编号: 0372-2112 (2006) 03-0413-06

SLM – A Secure Layered Multicast Protocol

CHEN Yue, LAN Ju-long, GUO Yun-fei, ZHAO Zhao-ling
(Information Engineering University, Zhengzhou, Henan 450002, China)

Abstract Layered multicast with receiver driven congestion control is a typical way for media stream distribution. The congestion control protocols in current layered multicast methods lack the limitations to users' behaviors. The receivers may violate the protocol regulations and join upper groups to initiate self-beneficial attacks, which leads to unfair bandwidth usage. This paper presents a general secure layered multicast protocol, SLM. On condition that the routers can assist with congestion control, CR-AC (Congestion state Related Access Control) algorithm based on Shamir's secret sharing scheme is used in edge routers to regulate the users' group subscription behaviors and avoid their self-beneficial attacks. And different users can be confined to different highest subscription levels according to their agreements with service providers. Analysis and simulation results show that SLM can ensure the network flows share the bandwidth safely in real-time, and has preferable scalability features.

Key words layered multicast; congestion control; self-beneficial attack; shamir's secret sharing scheme

1 引言

在基于 IP组播实现流媒体分发时,为适应 Internet的带宽不均匀性和流量动态性,使高带宽和低带宽接入用户均可得到与其可用带宽相适应的服务,多采用分层组播技术[1~3,6~9].在分层组播协议中,发送方将数据编码到几个有序的层中,每层由一个组播组以不同的速率(一般较低层速率较低)发送数据;接收方检测网络拥塞状况,并据此自低层向高层逐级订阅发送方发送的多个组播组,这种方法称为接收方驱动拥塞控制 (RDCC, Receiver Driven Congestion Control);接收方的订阅级别定义为当前最高订阅层及其下层的所有组播组,接收方订阅级别越高,接收到的层数越多,解码所得到的数据质量越高.

RDCC类协议建立在对用户信任,即假定接收方遵守协议规定的拥塞控制规则.然而,接收方可以出于自利的目的发起自利型攻击,它可以不响应网络拥塞信号,在网络发生拥塞时仍然保持当前的订阅级别甚至请求更高层的组播流量,造成路由数据平面的带宽竞争和控制平面处理开销增加,最终排挤其他网络业务流量,达到非公平占用带宽、以高速率接收流量的目的[10~13].Sergey Gorinsky等通过 NS-2仿真分析了自利型攻击所带来的影响[10,12],并提出了 DELTA (Distribution of Eligibility to Access)与 SIGMA (Secure Internet Group Management Architecture)方案[13],但该方案只适用于拥塞状态定义为出现一个包丢失的 FLID-DL协议[3],不具有通用性;另外, DELTA进行订阅级别授权升级时,所有子网和用户得到的授权相同,

收稿日期: 2005-02-28;修回日期: 2005-05-16
基金项目:国家 863信息技术领域重大专项项目 (No. 2003AA103510)

不能根据用户的带宽状况或付费情况由服务提供商限定不同用户的最高订阅级别. 目前, 尚没有一种通用、高效、可结合用户接入控制与拥塞控制的安全分层组播方案.

2 SLM 协议设计

2.1 SLM 的基本思想和前提假设

SLM 的基本思想是: 在支持具有路由器辅助拥塞控制机制的分层组播协议框架下, 将通信过程分为若干个时隙, 在 s时隙发送的组播包中附加 s+ 2时隙的组访问控制密钥片段; 利用 *Shamir's* 秘密共享方案, 分别设计各层的 (k, n)秘密共享模式; 发生拥塞的网络节点下游的接收方将不能还原以后加入当前订阅级别较高层组播组所使用的访问控制密钥; 在源到接收方组播树路径上未发生拥塞的接收方, 将可保持当前订阅级别或尝试加入上一层组播组, 从而实现拥塞状态相关的访问控制. 采用一个标识位, 实现与基于用户身份认证的访问控制的接口. 通过保密 *Shamir's* 秘密共享体制中的大素数 P 和虚拟局域网 (*VLAN*)技术, 限制不同用户的最高订阅级别.

SLM 的前提假设如下:

(1)设在一个时隙内, 第 i层和第 j层 (i< j)发送的数据包的个数分别为 n_i 和 n_j, i层和 j层丢包阈值分别为 n_i-k_i 和 n_j-k_j, 要求网络在将 i层和 j层的数据包传送到某个接收方时, 若 j层丢包数 $LOSS_j < n_j$-k_j, 则必有 i层丢包数 $LOSS_i < n_i$-k_i. 该前提假设降低了路由器优先级丢包策略的要求, 也就是说, *SLM* 并不要求网络中的路由器均支持绝对优先级 (上层组播组的包丢完, 才丢弃下层组播组的包), 只要网络可保证上层组播组丢包数比下层组播组丢包数先超过相应的阈值即可. 目前许多分层组播协议 (如文[6~9])中提供的路由器优先级丢弃机制均可满足此要求;

(2)信息源和网络基础设施是安全可靠的, 它们总是遵循协议的规定完成相应的动作;

(3)接收方仅试图发起自利型攻击, 而不发起纯恶意的 *DoS* 攻击, 对付 *DoS* 攻击需要其他的特定机制;

(4)边界路由器的本地接口是用户的唯一接入点.

2.2 SLM 的拥塞状态相关访问控制算法 CR-AC

设一个分层组播业务流由 L个组播组 $G_1, G_2 \cdots, G_L$ 承载, *CR-AC (Congestion state Related Access Control)* 设计基于 *Shamir's* (k, n)秘密共享体制[17]. 其细节描述如下.

2.2.1 发方与收方的秘密共享方案 设每层在单位时隙发送组播包的个数分别为 $n_1, n_2, \cdots, n_L$, 各层丢包阈值分别为 n_1-k_1, n_2-k_2, …, n_L-k_L. 构造 L个秘密共享模式:

Shamir's (k, n_i): $h_i(x) = (\tau_i + a_{i1}x + a_{i2}x^2 + a_{i3}x^3 + \cdots\cdots + a_{ik-1}x^{k-1}) \bmod P_i$ (1)

其中, i= 1~ L τ_i为第 i层的访问控制密钥, a_{i1}, a_{i2}, $a_{i3}\cdots\cdots a_{ik-1}$为选用的随机系数, P_i为一大素数, 它大于 n_i, τ_i, a_{i1}, a_{i2}, $a_{i3}\cdots\cdots a_{ik-1}$中的任一个, t_i, a_{i1}, a_{i2}, $a_{i3}\cdots\cdots$, a_{ik-1}均对接收方保密.

2.2.2 发方的处理 发方在发送第 s个时隙的第 i层组播包前, 事先将 t_i, 即 $h_i(0)$, 分发到边界路由器.

发方在发送第 s个时隙的第 i层第 j个组播包 PT_{ij} 时, 产生随机数 x_{ij} (1≤ j≤ n_i), 用公式 (1)实时计算 $y_{ij} = h_i(x_{ij})$, 并将秘密片段 (x_{ij}, y_{ij})附加到 PT_{ij} 中.

2.2.3 收方的处理 收方在收到 s时隙的第 i层组播包时, 用目前收到的 k个数据包, 使用公式 (2), 试图还原第 i层组播组在 s+ 2时隙使用的访问控制密钥.

$$z_i = \sum_{j=1}^{k} y_{ij} \prod_{m=1, m\neq j}^{k} \frac{-x_{im}}{(x_{ij} - x_{im})} \bmod p_i \qquad (2)$$

收方在第 s+ 2时隙订阅第 i层组播组的流量时, 需将〈s+ 2, z_i〉附加在订阅消息中.

该方法的优点在于, 收方无需知道 k_i, 仅需随接收到包的个数 k的增加按公式 (2)不断计算 z_i, 直到两次连续计算的结果相等时 (此时 k≥ k_i), 即可还原第 i层组播组 s+ 2时隙的访问控制密钥 t_i, 即 $h_i(0)$.

2.2.4 将组访问控制密钥分发到直连路由器 类似文献[13], *SLM* 使用一个可靠组播组 G_0 将分层组播各层的访问控制密钥分发到有接收方的边界路由器. G_0 的源是分层组播的源, 接收方在 s+ 2时隙加入分层组播的最低层组播组之前, 必须先在 s时隙加入 G_0, 以将 G_0 的组播包分发到边界路由器. G_0 的组播包中包含组访问控制密钥信息〈s+ 2, G_i, t_i〉(1≤ i≤ L), G_0 的组播包的 *IP* 头部携带 1位信息指示路由器截取该包而不向本地接口转发. 边界路由器在收到这种包后, 存储相应的〈时隙, 组地址, 密钥〉元组, 以用于相应时隙的访问控制. 为避免密钥分发和组成员管理不同步 (例如, 组成员加入时使用〈s, *G-address*, t_i〉, 而路由器目前保存的是〈s+ 1, *G-address*, t_i〉), 路由器需保存最新两个时隙的〈时隙, 组地址, 密钥〉元组. 在整个分层组播应用会话期间, 接收方应维持 G_0 组的组成员身份, 以使边界路由器获取后续时隙的组访问控制密钥.

2.2.5 组成员管理协议 除常规组成员管理协议 (如 *IGMP*[14])要求的数据结构之外, 边界路由器每个接口 I需要存储访问控制密钥和组成员管理所需的数据结构, 该数据结构中各域的描述如表 1所示.

表 1 边界路由器每接口数据结构中各域描述

域名	描述
Lmid	分层组播会话标识符
CurrL	该接口的当前订阅级别
TS1, TAO [1……L]	最新时隙的〈时隙, τ_1, τ_2, ……, τ_L〉值
TS2, TAO [1……L]	次新时隙的〈时隙, τ_1, τ_2, ……, τ_L〉值
GON	是/否 (True/False)组播组 G_0 的成员
Testtimer	加入尝试定时器
Testnum	加入尝试次数
Allowtimer	允许无条件向本接口输出的限时定时器
Waittraffic	是/否 (Ture/False)正在等待 CurrL+ 1组流量的到达

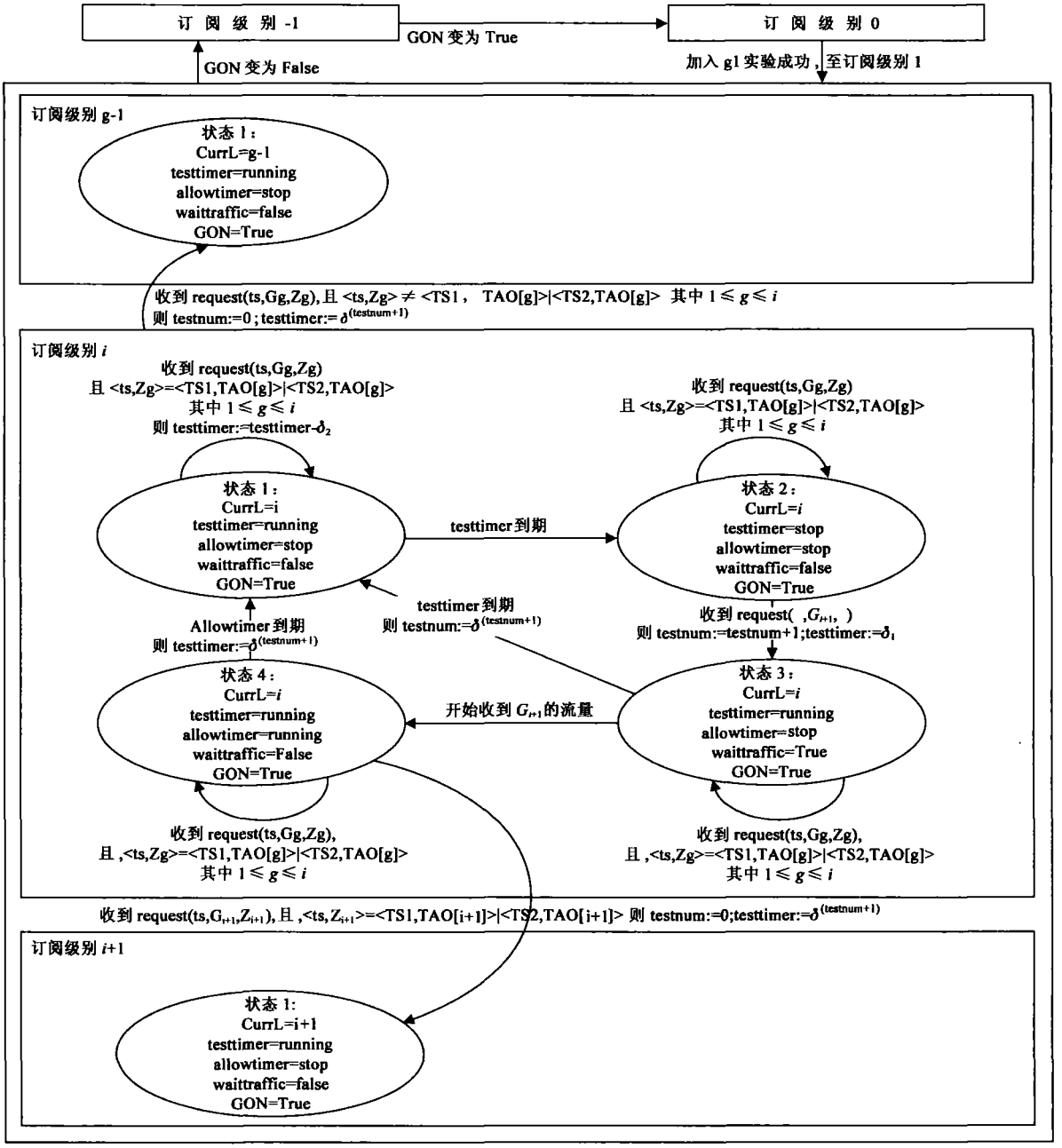

图 1 订阅级别管理状态迁移图

CR-AC 通过组成员管理实现访问控制, 该算法分为以下几个部分:

(1)限制主机加入会话: 规定加入会话必须首先要加入 G_0. 这可以通过安全 *IGMP*[15] 或 *Gothic*[16] 等组播用户认证和安全访问控制结构实现对 G_0 的访问控制, 本文不再赘述. 当主机通过认证并加入 G_0 后, *CurrL* 设定为 **0** (进入订阅级别 **0**), *GOV* 设为 *true*.

(2)订阅级别的升级和降级: 组播会话的订阅级别管理状态迁移图如图 **1** 所示. 对于某个订阅级别 i(**0**≤ i≤ L), 在状态 **1**, 只接受 G_0 以及 G_1, ……G_i 的加入消息, 不允许加入上一层组播组的加入尝试. *testtimer* 到期时, 转换到状态 **2** 允许主机进行加入上一层组播组 G_{i+1} 的尝试, 并马上向该接口发出成员关系查询 (*Membership Query*) 消息, 在该消息中增加一个指示位提示该接口上的主机可以进行加入上一层的尝试. 当接收到加入 G_{i+1} 的加入尝试请求时, 转换到状态 **3**, 同时将 *testtimer* 启动为 δ1 秒 (δ1 大于在状态 **3**、**4** 的停留时间), 以屏蔽加入尝试期间的新的加入尝试, 并通过 *testtimer* 限制等待组 G_{i+1} 流量的最长时间. 当 G_{i+1} 的流量到达时, 启动 *allowtimer* 进入状态 **4**, 在 *allowtimer* 停止运行前, 若主机能在后续的加入 G_{i+1} 的消息中, 提供相应的访问控

制密钥, 则路由器组播会话的订阅级别升为 $i+1$, 进入其状态 1, 否则转换到本订阅级别的状态 1. 在状态 3, 若直到 *testtimer* 到期仍没有 G_{i+1} 的流量到达 (上游路由器丢弃了 G_{i+1} 流量), 则转换到状态 1. 在订阅级别 i 的任何状态, 如果接收到的订阅 1~ i层的某个组播组 g($1 \leqslant g \leqslant i$)的消息中包含的访问控制密钥不正确, 则路由器的订阅级别降级到 g-1级. 最高订阅级别 L仅有状态 1, 无升级过程. 订阅级别-1表示该接口上的主机未通过认证, 订阅级别 0表示该接口上已有主机通过认证, 目前可申请最低层组播组的流量. 当某接口从订阅级别-1转换到订阅级别 0时, 直接进入订阅级别 0的状态 2, 以快速允许主机加入第 1层组播组的尝试. 在订阅级别 0, 不因加入某个组的加入消息中未提供有效密钥而退回到订阅级别-1.

为限制接收主机尝试加入 $i+1$组的频度, 增强路由状态的稳定性, 当从订阅级别 i-1升级到订阅级别 i的状态 1时, 加入尝试次数 *testnum* 设置为 0, *testtimer* 设置为 δ秒 (δ为一常量); 在订阅级别 i, 当从订阅级别的状态 2转换到状态 3时, *testnum* 赋为 *testnum* + 1, 以记录加入尝试次数; 如果加入尝试失败, 当从状态 3或状态 4转换到状态 1时, 将 *testtimer* 重启为 $\delta^{(testnum+1)}$ 秒, 以在加入尝试失败时, 延长下次加入尝试的间隔时间; 在状态 1, 每收到一次符合〈ts, Zg〉= 〈TS1, TAO[g] 〉| 〈TS2, TAO[g] 〉条件的 *request*(ts, G g Zg) (其中 $1 \leqslant g \leqslant i$), 则认为网络拥塞的可能性降低, 将 *testtimer* 减去 δ_2秒.

(3)限制接收方的最高订阅级别: 在 *Shamir* 秘密共享体制中, 选用的素数 P是公开的. 为授予不同用户不同的最高订阅级别, *CR-AC* 采用如下授权方式: 若系统规定某一用户最高订阅级别为 i, 授权服务器将 $P_1, P_2, \cdots, P_i$ 公开给该用户, 而 $P_{i+1}, \cdots, P_L$ 对该用户保密. 这样, 该用户不能实时还原 $t_{i+1} \sim t_L$, 也就不能发出合法的组 $G_{i+1} \sim G_L$ 的订阅请求. 考虑局域网为共享介质网络, 在同一局域网中, 将不同最高订阅级别的用户划分到不同的 *VLAN* 中, 从而限定不同用户的最高订阅级别.

(4)退出组播会话: 在 0~ L任一订阅级别的任何状态, 如果某主机在后续的认证中未通过, 则将订阅级别状态中的 *GOV* 域置为 *False*, 并使订阅级别降为-1, 使该接口退出组播会话.

3 验证与分析

3.1 安全性与响应性分析及仿真实验

路由器在本地接口收到有效的 〈时隙, 组地址, 密钥〉时, 才向该接口转发该组播组的流量. 非法主机有可能通过直接猜测密钥, 在两个时隙内进行加入组的尝试. 假设密钥有 b位组成, 则通过猜测密钥得到组访问权的概率为 $y/2^b$, 其中 y是一个时隙内接收方可以与边界路由器通信的 〈组地址, 密钥〉对的个数, 如果 b值稍大, 就可使攻击方成功的概率很小. 由于密钥片段的长度与密钥长度相同, 攻击方通过猜测密钥片段然后再计算出正确密钥的可能性, 比直接猜测密钥的可能性更小.

在限制接收方最高订阅级别时, *CR-AC* 通过保密 P_i 使接收方无法还原 t_i, 攻击者很难在在两个时隙内猜测许多大素数 P_i, 用公式 (2)计算 $s+2$时隙的 Z_i, 并进行多次加入组的尝试以验证 Z_i 的有效性. 另外, 在边界路由器的某个订阅级别 i当 *testtimer* 处于 *running* 状态时, 来自主机对 $i+1$之上的层的加入尝试将被拒绝, 有效防止了主机的多次在短时间内的加入尝试.

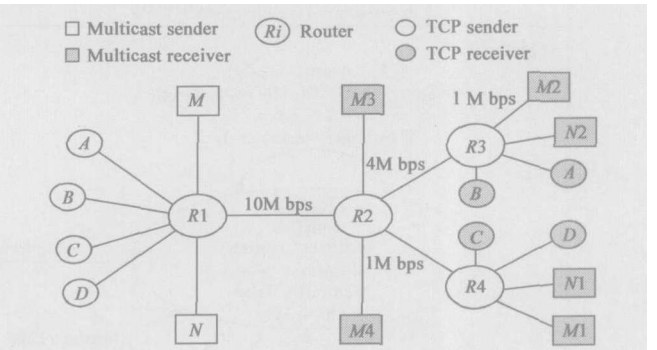

图 2 SLM 仿真实验拓扑结构

为验证 *SLM* 抗自利性攻击效果和对动态可用带宽的响应能力, 本文采用 *NS-2* 27软件进行了仿真实验. 为便于比较, 仿真拓扑结构及其网络基本参数与文献 [12]基本相同, 如图 2所示, 标识出带宽的链路为瓶颈链路, 未标识出的链路带宽均为 100*Mbps*, 各链路的延迟均为 10*ms*, 路由器与该链路连接的接口有一个两倍于带宽乘延迟的缓冲区. 网络节点转发数据包延迟为 10*ms*, 协议处理延迟设为 20*ms*. 组播会话 M有四个接收方 M1、M2、M3、M4, 组播会话 N有两个接收方 N1、N2. M、N均使用 *SLM* 并采用如文献 [7]的路由器辅助拥塞控制策略 (由接收方通过加入组播组形成两级优先级, 当前订阅级别最高层组播组优先级较低, 以下各层优先级相同且较高, 路由器优先丢弃优先级较低的数据包); M、N的层次设置为 L= 5个层次, 并采用 *CBR-5*编码算法编码; M 各层编码后的数据速率为 {64*Kbps*, 128*Kbps*, 256*Kbps*, 512*Kbps*, 1*Mbps*}, N 各层编码后的数据速率为 {32*Kbps*, 64*Kbps*, 128*Kbps*, 256*Kbps*, 512*Kbps*}; M、N的时隙长度取 300*ms*, M 的 δ、δ_1、δ_2 分别取 2*s*、3*s*、0. 1*s*, N 的 δ、δ_1、δ_2 分别取 3*s*、3*s*、0. 1*s*, 各层丢包的阈值 n_i-k_i 设定为 *round*(n_i* 20%). M1、N1分别于第 0秒时刻和第 50秒时刻通过认证, 分别达到会话 M 和会话 N的订阅级别 0, 并假设在之后的会话期间 M1、N1均保持通过认证状态. 单播会话 A、B、C、D 传输层使用 *TCP Reno*, 其 IP 包优先级与分层组播较高优先级相同. 每个发送方以协议允许的最大速率发送数据, 均发送 1500字节的定长数据包.

设第 100秒之后, M1试图违规订阅更高层的组播组. 记录 200秒的通信过程中会话 M、N、C、D的流量在路由器

R2至路由器 R4的链路上的带宽占用情况, 仿真结果如图 3所示. 可以看到, *SLM* 可有效防止接收方违规订阅更高层的组播组, 抵抗了自利型攻击, 可保证分层组播流量与其他流量公平使用带宽. 在第 50秒后, N1动态加入组播会话 N, *SLM* 可迅速响应这种变化, 重新调整带宽并稳定到较为公平的状态, 具有很好的响应性. 另外, 由于采用路由器优先丢弃机制, 与文献[13]的实验结果相比, 会话 M、N 在 R2-R4链路的流量平滑性明显提高.

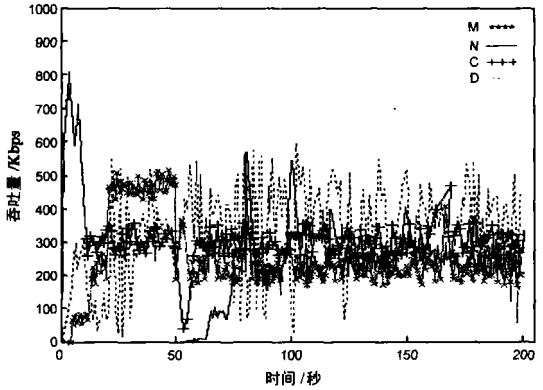

图 3 SLM 的抗自利型攻击效果

3.2 组成员动态性与 SLM 可扩展性分析

IP组播的组成员是动态的, 可随时加入或离开组播组, 组播拥塞控制机制必须具有可扩展性, 以在组成员数量增多时, 不会造成组播拥塞控制任务过重. 由于分层组播拥塞控制是一种开环控制方法, 即接收方并不向发送方反馈任何信息, 发送方也无需对分组丢失进行响应, 因此, 不存在单速率组播拥塞控制算法难以克服的反馈内爆、丢失路径多样性 (LPM, loss path multiplicity)[18] 等影响可扩展性的因素.

SLM通过组播组管理和组播路由机制间接实现拥塞控制. 组播组管理协议 IGMP具有报告响应抑制功能[15], 当主机检测到同一局域网内的其他主机发出的对同一组的 REPORT消息时, 将抑制自己的 REPORT消息, 因此同一子网内新成员的加入造成的边界路由器处理开销增长很小; 主流组播路由协议, 如特定源组播 SSM (Source Specific Multicast)[19], 具有加入 (JOIN) 消息的汇聚功能, 当组播树上的路由器某段时间内收到多个下游路由器发来的 JOIN消息时, 并不马上对每个收到的 JOIN消息响应, 而是至定时器到期才向上游发出一个 JOIN消息, 因此, 因新成员加入仅在原来不在组播树上的路由器和链路上造成了新的开销, 并不造成每路由器和每链路处理和传送 JOIN消息开销的增大. 组播组管理协议与组播路由协议良好的可扩展性保证了 SLM 协议的可扩展性.

SLM 利用了路由器辅助的拥塞控制机制, 当网络节点发生拥塞时, 路由器优先丢弃上层的组播包, 当下游主机因某层组播包丢失过多而不能还原其访问控制密钥时, 其发出的订阅该组播组的消息将被边界路由器阻断. SLM 这种基于拥塞状态的访问控制机制不但防止了用户违规订阅, 还避免了路由器负担加重, 比其他无此安全机制的分层组播协议相比具有更好的可扩展性.

3.3 时效性分析

若组播包的长度为 λ, 发方某层组播组发送速率为 ω, 则需要发送方以至少 λ/ω的频度产生密钥片段 (x_i, j; y_i, j). 当包长取 1500字节, 发送速率达 1*Mbps*时, 要求产生一个密钥片段的时间达到 12*ms*即可. 根据在 *Intel Pentium 4 CPU 2.80GHz*、内存为 256*M* 的微机上的实测结果, 当 n= 100, k= 80, 密钥片段长度为 32时, 主机根据 x_{ij}计算 y_{ij}的时间仅为 8μs, 可满足实时产生密钥片段的需要. 同样, 当接收方得到某一个时隙内若干密钥片段时, 也可实时计算 z_t.

3.4 通信开销分析

设承载流媒体的 *IP* 包长为 *B* 字节 (*8B* 位), 附加在 *IP* 包 P_{ij}的随机数 x_{ij}和密钥片段 y_{ij}均由 b位组成, 则 (x_{ij}, y_{ij})消耗的带宽开销的比例 C_{XY}为: $2b/(2b+8B) = b/(b+4B)$. 设 x_{ij}, y_{ij}为 32位, *IP* 包长为 1500字节, 此时, C_{XY}仅为 $32/(32+4*1500) \approx 0.53\%$. 随着 *IPv6*的发展, 流媒体业务将采用更大的 IP包传送, 该开销会进一步减小.

4 结论

SLM 在边界路由器实施 CR-AC算法, 规范了用户的组订阅行为, 避免了恶意主机在控制平面和数据平面造成的自利型攻击; 可根据不同用户的带宽状况或付费情况由服务提供商限定其最高订阅级别; 可快速有效地响应可用带宽的变化. 同时, SLM 易于实施, 对核心节点仅要求具有有限的优先级丢弃能力, 在边界路由器仅需改造 IGMP协议即可实现. 该协议开销较小, 尤其适用于大 IP包流媒体传输应用.

如果将 CR-AC中的拥塞检测和控制机制引入路由器的控制平面, 以直接触发组播路由协议的相应动作, 将会进一步减少路由协议的消息开销, 但这样也会增加路由器的复杂度, 该问题尚有待于进一步研究.

参考文献:

[1] S McCanne, V Jacobson, M Vetterli. Receiver-driven layered multicast[A]. Proc of ACM SIGCOMM′96 [C]. New York, USA: ACM Press, 1996. 117-130.

[2] L Vicisano, L Rizzo, J Crowcroft. TCP-like congestion control for layered multicast data transfer[A]. Proc of the IEEE INFORCOM′98[C]. San Francisco: IEEE Press, 1998. 996-1003.

[3] J W Byers, et al. FLID-DL: congestion control for layered multicast[J]. IEEE Journal on Selected Areas in Communications, 2002, 20(8): 1558-1570.

[4] D Rubenstein, J Kurose, D Towsley. The impact of

multicast layering on network fairness[J]. IEEE/ACM Transactions on Networking, 2002, 10(2): 169-182.

[5] R Gopalakrishnan, J Griffioen, et al. Stability and fairness issues in layered multicast[A]. Proc of the NOSSDAV'99[C]. Basking Ridge, NJ, USA: ACM Press, 1999. 31-44.

[6] S Bajaj, et al. Uniform versus priority dropping for layered video extended version[EB/OL]. http://citeseer.ist.psu.edu/bajaj98uniform.html

[7] R Gopalakrishnan, J Griffioen, et al. A simple loss differentiation approach to layered multicast[A]. Proc of IEEE INFOCOM 2000[C]. Tel-Aviv, Israel: IEEE Press, 2000. 461-469.

[8] K Kang, et al. NLM: network-based layered multicast for traffic control of heterogeneous network[J]. Computer Communications, 2001, 24(5-6): 525-538.

[9] J Y Son, et al. Router-assisted TCP-Friendly traffic control for layered multicast[J]. Lecture Notes in Computer Science, 2003, 2662: 202-211.

[10] S Gorinsky, S Jain, H Vin. Multicast congestion control with distrusted receivers[A]. Proc of NGC'02[C]. Boston, MA, USA: ACM Press, 2002. 19-26.

[11] V Arya, T Turletti. Dealing with receiver misbehavior in multicast congestion control[R]. INRIA Research Report, July, 2003. ftp://ftp.inria.fr/INRIA/publication/publi-pdf/RR/RR-4899.pdf.

[12] S Gorinsky, S Jain, H Vin. Robust congestion control for multicast: challenges and opportunities[EB/OL]. http://www.arl.wustl.edu/~gorinsky/pdf/TR2003-02.pdf 2003-02/2005-02.

[13] S Gorinsky, et al. Robustness to inflated subscription in multicast congestion control[A]. Proc of SIGCOMM'03[C]. Karlsruhe, Germany: ACM Press, 2003. 87-98.

[14] W Fenner. Internet group management protocol, Versinn[S]. RFC 2236, 1997.

[15] A F Gomez-Skarmeta, et al. IGMPv3-based method for avoiding DoS attacks in multicast-enabled networks[A]. Proc of the IEEE Computer Society LCN2000[C]. Tampa, Florida, USA: IEEE Press, 2000. 94-95.

[16] P Judge, M Ammar. GOTHIC: a group access control architecture for secure multicast and anycast[A]. Proc of IEEE INFOCOM'02[C]. New York, USA: IEEE Press, 2002. 1547-1556.

[17] A Shamir. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[18] S Bhattacharyya, et al. The loss path multiplicity problem in multicast congestion control[A]. Proc of IEEE INFOCOM'99[C]. New York, NY, USA: IEEE Press, 1999. 827-836.

[19] S Bhattacharyya, Ed. Sprint. An overview of source-specific multicast (SSM)[S]. RFC 3569, 2003.

作者简介:

陈 越 男, 1965年出生于河南开封, 解放军信息工程大学副教授, 硕士生导师, 1990年获国防科技大学计算机软件专业工学硕士学位, 解放军信息工程大学通信与信息系统专业在读博士研究生, 主要研究方向为网络路由理论与技术、信息安全等.

E-mail: cy@mail.ndsc.com.cn

兰巨龙 男, 1962年出生于河北张北, 解放军信息工程大学国家数字交换系统工程技术研究中心教授, 博士生导师, 1988年获西安电子科技大学通信与电子系统专业工学硕士学位, 2001年获解放军信息工程大学通信与信息系统专业博士学位, 主要研究方向为网络路由理论与技术、并行交换结构和 IPv6技术等.

郭云飞 男, 1963年出生于郑州, 国家数字交换系统工程技术研究中心主任, 信息工程大学教授, 国家 863计划通信高技术主题专家组组长, 博士生导师, 主要研究方向为信息网络与交换技术.

赵昭灵 男, 1976年出生于湖南京山县, 博士, 国家数字交换系统工程技术研究中心讲师, 主要研究方向为网络交换与传输.