# 基于 PIM-SM 协议 IP 组播安全技术①

黄 舒[1,2], 董喜明[2], 郭云峰[2]

[1](武汉邮电科学研究院, 武汉 430074)
[2](武汉烽火网络科技有限公司, 武汉 430074)

**摘 要**: 伴随着互联网的高速发展, Internet 上涌现了许多需要高带宽支持的应用. 组播技术能有效的利用网络带宽资源. 组播的安全性一直是一个热点问题, 也是阻碍组播发展的一个主要问题. 本文针对虚假组播源产生垃圾消息恶性攻击提出了一个基于 PIM-SM 组播协议的预防方案, 实验结果表明, 该方案能提高组播系统的可靠性.

**关键词**: 组播; IP; 网络协议; PIM-SM; 安全

## PIM-SM Based Multicast Security

HUANG Shu[1,2], DONG Xi-Ming[2], GUO Yun-Feng[2]

[1](Wuhan Research Institute of Post and Telecommunications, Wuhan 430074, China)
[2](Wuhan FiberHome Network Co., Ltd, Wuhan 430074, China)

**Abstract:** With the rapid development of the network technology, more bandwidth is required. Multicast transmission offers efficient network resource consumption. Multicast security is a hot issue. Multicast security problem hinders the development of multicast technology. This paper discusses the principles of multicast protocol PIM-SM and makes a detailed description of a method to prevent vicious multicast source attacking. The method can improve the reliability of multicast system.

**Keywords:** multicast; IP; network protocol; PIM-SM; security

随着社会信息化建设日益完善, Internet 在人们生活中扮演着越来越重要的角色, 信息网络很大程度上改变了人们的生活和工作方式. 人们对网络的需求由单一的消息传送向综合的多媒体业务发展. IP 组播概念的引进能满足数据传输的需求并提供更多的增值服务. 用组播技术收发信息可以从本质上解决整个网络的带宽需求. 组播技术作为网络中主机之间通信的一种模式, 不论组成员数量的多少, 在共享网络上, 相同的信息都只发送一份数据拷贝, 能够很好地控制流量, 减少主机和网络的负担[1].

目前 IP 组播技术的研究集中于组播流量的控制, 可靠性传输和安全性问题上. 相比于组播安全问题其他两个方面已经取得了不少研究成果. 由于组播加入不受限制的特点, 组播比单播通信更容易受到攻击, 具有更大的风险. 组播的安全性是阻碍组播发展的一个主要问题. 病毒/蠕虫能伪装组播数据流往组播网络发送没有接收者的数据流量, 造成对 RP 结点或网络中其他结点的攻击[2].

本文提出了一种基于 PIM-SM 协议恶性组播流量过滤方案. 全文的内容框架如下: 下一章介绍组播特性与安全问题, 第二章讨论 PIM-SM 组播协议的工作机制, 第三章详细描述本文所提出的方案并在第四章进行总结.

## 1 组播特性与安全问题

IP 组播使用 UDP 进行传输, 任何主机都能向某个组播组发送 UDP 报文, 组播组成员可以随时加入/退出组播组. 组播具有三个关键特性: 组成员关系的开放性, 组播接收的同一性以及组播数据发送的开放性. 这些特性使组播更灵活, 更易扩展也更易配置, 但同

①收稿时间:2013-10-25;收到修改稿时间:2013-12-09

时, 这些特性也在不同程度上带来了安全隐患. 接收者自己决定加入或者退出组播网络. 实现如此安全便捷的加入退出机制的代价是组播安全性的牺牲. 在没有安全约束的情况下, 任意的加入/退出使得通信的秘密性无法得到保证, 对机密数据的窃听十分容易发生. 同时, 对于处理组播组成员加入协议 IGMP/MLD 报文的路由转发设备发起的拒绝服务 DOS(Denial of Service)攻击也是很大的安全隐患[3][4]. 组播接收的同一性导致了在单播中的很多安全机制无法实现. 每个组播成员接收到的组播数据都是相同的, 而接收数据的独特性在单播中正是某些安全机制实现的基础. 组播数据发送的开放性使得组播对任意数据源都是开放的, 任意源都可以往组播网络中发送组播数据而不受限制. 组播数据发送的开发性引起的安全隐患是本文下面章节要重点解决的问题.

## 2 PIM-SM协议[5]

### 2.1 邻居发现

在 PIM 域中, 路由器通过周期性的发送 Hello 报文来学习邻居信息并维护邻居关系[6]. 邻居间通过 Hello 报文中的信息选举出 DR(Designed Router, 指定路由器). 发送端网络和接收端网络, 都需要进行 DR 选举, 组播源侧的 DR 通过向 RP 发送注册消息, 建立从 RP 到组播源的最短路径树. 接收者侧的 DR 通过向 RP 发送加入/枝减消息, 建立从 RP 到接收者的共享树.

### 2.2 RP 发现

RP 在 PIM-SM 域中起着至关重要的作用. 在组播信息量较少的小型网络中, 可以通过手动配置的方式在域内每台路由器上指定静态 RP. 在拓扑结构较复杂的大型网络中, 通过 RP 转发的数据流量巨大, 此时需要在 PIM-SM 域内配置多个 C-RP(Candidate-RP, 候选 RP)来缓解 RP 的负担. 通过自举机制从众多 C-RP 中选取出 RP, 使不同的 RP 服务于不同的组播组. 此时需要配置 BSR(BootStrap Router, 自举路由器). 类似的, 一个 PIM-SM 域可以配置多个 C-BSR(Candidate-BSR, 候选 BSR). 一旦 BSR 发生故障, 其余 C-BSR 能够通过自动选举产生新的 BSR, 从而确保业务免受中断. BSR 收集 C-RP 发来的宣告报文后汇总成 RP-SET, 并封装在 BSM 报文中发往整个 PIM-SM 域.

### 2.3 构建 RPT

RPT 树是以 RP 为根, 以 DR 为叶子节点的共享树. 当有接收者对发往组播组 G 的消息感兴趣时, 通过组管理协议通过给与其直连的 DR. 当接收者加入组播组 G 时, 与其直连的 DR 向组 G 对应的汇聚点 RP 发送(*, G)加入报文. “*”表明对组播源没有限制, 即接收来自任意组播源的消息. 所途径的路由器在其组播转发表中增加相应的路由表项. 从接收者到汇聚点 RP 形成了以 RP 为根, 以接收者为叶子节点的共享树. 当接收者不再对发往组播组 G 的消息感兴趣时, 通过组管理协议发送离开消息, 与其直连的 DR 向汇聚点 RP 方向发送剪枝报文. 上游节点收到剪枝消息后, 从出接口列表中删除与其相连的下游接口. 如果下游没有接收者, 则从其路由转发表中删除相应的路由表项, 并向上游 RPF 邻居继续发送剪枝消息.

### 2.4 组播源注册

通过组播源注册过程, 可以向汇聚点 RP 通告组播源的存在. 与组播源相连的 DR 收到组播源 S 发往组播组 G 的组播数据包, 会把数据包封装在注册消息中以单播消息的形式发送给汇聚点 RP. RP 收到注册报文后会解封装注册报文, 获取其中的组播数据包, 将其沿着建立好的 RPT 树转发给接收者. 同时会向组播源方向逐跳发送(S, G)加入报文. 这样便建立了从组播源 S 到 RP 的最短路径树. 最短路径树以组播源 S 为根节点, 以 RP 为叶子节点. 最短路径树上所有途径的路由器都会在其路由转发表中增加相应的(S, G)路由表项. 组播源 S 发出的数据包会沿着最短路径树发送到 RP. 当 RP 收到组播源 S 发来的数据包, 一方面沿着建立好的 RPT 树向接收者转发数据包, 另一方面向组播源 S 发送注册停止消息.

## 3 恶性组播流量过滤方案

本章将详细介绍提出的恶性组播流量过滤方案. 方案的宗旨是提出一种简洁有效的方法来防止伪装组播源对组播系统进行恶性攻击. 提出的方案与 PIM 协议独立, 能在不影响 PIM 协议机制的基础上改进方案.

图 1 描述了整个方案处理流程. PIM 协议的 RP 节点维护两张表, 一个攻击者列表(Attacker List), 一个候选攻击者列表(Candidate Attacker List). 攻击者列表中包含攻击者的信息, 列表上攻击者源发来的数据流

都不予转发. 候选攻击者列表上罗列了可疑攻击者信息. 并不阻止候选攻击者列表上可疑攻击者发送的组播数据流量. 这样设计是因为不能轻易断定一个组播数据流是否为恶性组播流量. 攻击列表管理函(Attacker List Management Function)通过管理两张列表来控制组播源恶性攻击.

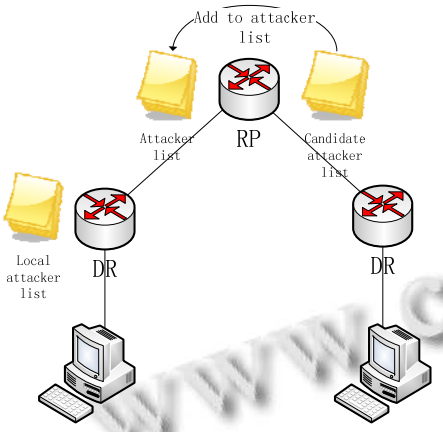


图 1　方案处理流程

组播消息发送端路由器维护一张本地攻击者列表. 攻击者伪装组播源在网络拓扑中发送组播数据, 发送者端DR每收到一份数据报文便向RP发送封装组播数据的注册报文, RP 依据特定的恶性组播流判定准则来判定组播报文是否是攻击者伪装发送的. 初次判定一个组播报文为可疑攻击者伪造, 把组播报文信息加入到候选攻击者列表中. RP 往发送者 DR 单播注册停止消息. 再次判定则确认一个组播流为恶性攻击者伪造, 将组播流信息从候选攻击者列表中注册到攻击者列表中, 并将组播流信息同步到发送者处的本地攻击者列表. 发送者侧 DR 接到该组播数据流后不再向 RP 发送注册消息, 并向源侧用户发送告警消息.

RP 结点和发送者侧 DR 包含的函数模块如图 2 所示.

RP 结点除了包含 PIM 路由协议 RP 结点的功能, 还包括攻击者列表管理函数(Attacker List Management Function), 组播攻击者判定准则函数(Multicast Attacker Policy)和组播攻击者滤除处理函数(Multicast Attacker Filtering Process). 列表管理函数用于管理控制组播源伪装者的两张列表. 组播攻击者判定准则函数定义滤除组播源攻击者的准则. 组播攻击者滤除处理函数通过组播攻击者判定准则函数来处理滤除过程. 发送者侧 DR 结点, 除了包含 PIM 组播路由功能, 还包括组播攻击者数据包处理函数

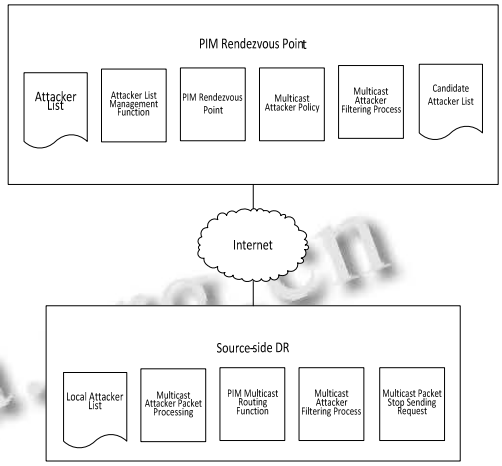


图 2　RP 结点和源侧 DR 结点函数模块

(Multicast Attacker Packet Processing), 组播攻击者滤除处理函数(Multicast Attacker Filtering Process)和组播数据发停止发送请求函数(Multicast Packet Stop Sending Request). 组播攻击者数据包处理函数依据本地攻击者列表信息来阻止相对应的数据流量转发. 组播攻击者滤除处理函数需要和 RP 共同作用来滤除攻击者发送的组播数据流. 通过组播数据发停止发送请求函数向用户主机发送告警消息提示停止发送相应组播数据流.

方案的工作流程如图 3 所示. 当组播数据流到达发送者侧 DR, DR 遍历本地攻击者列表, 如果列表中没有该源信息, DR 向 RP 发送注册消息. RP 收到封装组播数据的注册消息后, 解封装, 获取相应组播消息. RP 会遍历攻击者列表, 如果列表中有该组播源信息, 则 RP 直接丢弃该数据包. 如果攻击者列表中没有相应信息, 则遍历候选攻击者列表, 如果有相应信息, 则将候选攻击者列表中攻击者的信息同步到攻击者列表中, 并同步到 DR 处本地攻击者列表中. DR 向用户终端发送告警信息. 如果 RP 候选攻击者列表中没有相应消息, RP 依据组播攻击者判定准则来判断此数据流量是否是攻击者伪造发送的. 如果判定是攻击者伪造数据流量, 则向 DR 发送注册停止消息, 并把攻击者信息加入到候选攻击者列表中.

候选攻击者列表包含的参数如表 1 所示. 计数器

用于记载所接收的相应源的注册消息的个数, 如果计数器达到组播攻击者判定准则规定的上限, 则 RP 需要处理攻击者阻止进程. 定时器记载着最后一次注册消息发送的时间间隔. 如果定时器老化, 则从列表中删除相应信息.

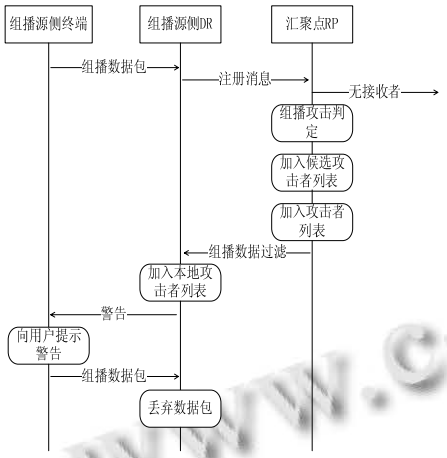


图 3 方案的工作流程图

表 1 候选攻击者参数

| 参数 | 参数说明 |
|---|---|
| 组地址(Multicast Address) | 组播数据流的组播组地址 |
| 源地址(Source Address) | 攻击者伪造组播源地址 |
| DR 地址(DR Address) | 组播源侧 DR 地址 |
| 计数器(Counter) | 攻击者发送消息个数 |
| 定时器(Timer) | 最后一次注册消息发送时间间隔 |

攻击者列表包含的参数如表 2 所示. 当攻击者列表中信息发生变化，启动同步定时器，将列表信息同步到本地攻击者列表中.

表 2 攻击者参数

| 参数 | 参数说明 |
|---|---|
| 组地址(Multicast Address) | 组播数据流的组播组地址 |
| 源地址(Source Address) | 攻击者伪造组播源地址 |
| DR 地址(DR Address) | 组播源侧 DR 地址 |
| 同步定时器(SyncTimer) | 同步定时器 |

本地攻击者列表包含的参数如表 3 所示. RP 告知发送者侧 DR 攻击者组播信息, DR 将此信息加入到本地攻击者列表中, 并向组播源终端发送告警消息. 对于候选攻击者列表, 攻击者列表和本地攻击者列表, 如果源地址为空, 则阻止匹配组地址的数据流, 如果源地址存在, 则阻止匹配源地址和组地址的数据流.

表 3 本地攻击者参数

| 参数 | 参数说明 |
|---|---|
| 组地址(Multicast Address) | 组播数据流的组播组地址 |
| 源地址(Source Address) | 攻击者伪造组播源地址 |
| 标识定时器(Timestamp Timer) | 最后一次注册消息的发送时间标识 |
| 同步定时器(SyncTimer) | 同步定时器 |

## 4 方案实现及结果分析

本文中所采用的实验环境为烽火网络 F-engine 5828 系列交换机, 软件采用 Vxworks 操作系统, 使用 Sprient 测试仪表模拟恶性组播源发送组播数据包. 测试拓扑图如图 4 所示[8].

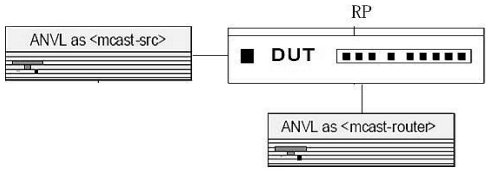


图 4 方案验证测试拓扑图

改进方案和原始方案注册消息个数对比图如图 5 所示. 由图中可以看出, 注册包的数量明显减少, 能有效减少网络资源浪费.

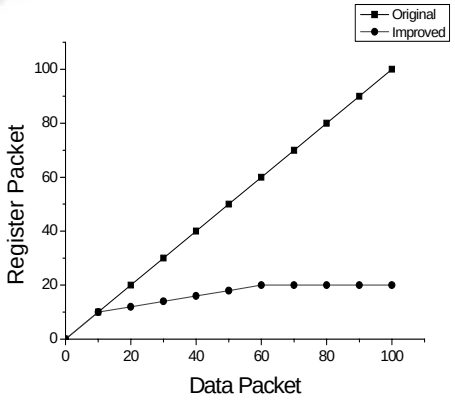


图 5 改进方案和原始方案注册包个数对比图

目前传统的组播源认证方式分为基于数字签名的源认证方式和基于 MAC(Message Authentication Codes, 信息认证码)的源认证方式两类. 数字签名的

源认证方式包括流签名方案， BiBa 方案, 树形散列方案, EMSS 方案等. 基于 MAC 的源认证方案包括非对称 MAC 方案以及热门的 Tesla 方案.

本文提出了一种简单的, 独立于 PIM-SM 协议的源认证方案. 通过判定组播源的 IP 地址合法性以及下游是否有相应的组成员来过滤组播数据. 组播源判定模块可以依据特定的情况进行个性化修改, 制定不同的过滤准则, 扩展性较强. 当下游有组播接收者对组播组感兴趣时, 能及时响应, 恢复组播数据的转发, 认证延迟短. 本方案与传统源认证方案性能对比如表 1 所示.

表 1 组播源认证方案性能对比

| 方案 | 可靠性 | 延迟 | | 开销 | 可扩展性 |
|---|---|---|---|---|---|
| | | 发送端 | 接收端 | | |
| 流签名 | 高 | 小 | 大 | 大 | 弱 |
| BiBa | 高 | 大 | 大 | 大 | 弱 |
| EMSS | 高 | 大 | 小 | 小 | 弱 |
| 非对称 MAC | 高 | 小 | 大 | 大 | 弱 |
| Tesla | 高 | 小 | 小 | 小 | 弱 |
| 本文方案 | 待定 | 小 | 小 | 小 | 强 |

由表 1 可以看出, 本方案的可靠性依据组播源判定函数而定, 需要进一步优化改进.

## 5 结 语

当一个主机发送没有相应接收者数据包的时候会产生数据洪泛. 注册消息不像其他组播进程需要进行 RPF 检查, 主机可以伪造这些数据包, 导致了很多潜在的威胁. 一个病毒/蠕虫可以伪装成组播地址或者通过不同组的封装数据包来使 RP 数据超载, 造成组播网络瘫痪.

本篇论文提出了一种简单易行的恶性组播流量过滤方案. 提出此方案的初衷是为了阻止病毒模拟组播源对组播网络系统恶性攻击. 本协议与 PIM-SM 组播协议相互独立, 互不影响, 可以在不更改 PIM-SM 组播协议的基础上对此方案进行升级. 下一步工作是进一步改进恶性源组播数据判定算法, 提高恶性源判定准确性.

## 参考文献

1 Deering S. RFC1112, Host Extensions for IP Multicasting. 1989.

2 周贤伟.IP 组播与安全.北京:国防工业出版社, 2006:44–64.

3 B.Cain and S.Deering,RFC 3376,Internet Group Management Protocol, Version 3. 2002.

4 Vida R, Costa L. RFC 3810, Multicast Listener Discovery Version 2 (MLDv2) for IPv6. 2004.

5 Fenner B, Handley M, Holbrook H, Kouvelas I. RFC4601, Protocol Independent Multicast-Sparse Mode (PIM-SM). 2006.

6 华为 3com 技术有限公司编著.PIM 技术介绍.北京:清华人学出版社,2005.1:5–9

7 Fenner B, Handley M, Holbrook H, Kouvelas I. draft-ietf-pim-sm-v2-new-11.txt, Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (Revised) . 2004.

8 岩延,郭江涛等.组播路由协议设计及应用.北京:人民邮电出版社,2002:45–79.