【信息科学与控制工程】　　doi：10.11809/scbgxb2015.07.029

专网组播应用设计与安全策略

李乃振

（92493 部队 辽宁 葫芦岛　114200）

摘要：介绍了测通专网主要拓扑结构、业务应用情况，分析研究了组播关键技术、特点及面临的安全问题，对专网的组播协议选择、路由设计、组播安全策略设置方面提出了具体的设计方案和建议。

关键词：专网；组播设计；安全策略

本文引用格式：李乃振. 专网组播应用设计与安全策略[J]. 四川兵工学报，2015(7)：113－116.

Citation format：LI Nai-zhen. Multicast Application Design and Security Strategy in Special Network[J]. Journal of Sichuan Ordnance，2015(7)：113－116.

中图分类号：TP393　　**文献标识码**：A　　**文章编号**：1006－0707(2015)07－0113－05

Multicast Application Design and Security Strategy in Special Network

LI Nai-zhen

(The No. 92493rd Troop of PLA, Huludao 114200, China)

Abstract: This paper mainly introduced special network topology structure and service application, and analyzed and researched on the key technology, characteristic and security multicast. Based on the above analysis, detail design proposal and suggestions of special network, multicast protocol of choice, route design, multicast security policy setting and so on were put forward.

Key words: special network; multicast design; security policy

相对于单播点到点的传输机制，组播以单点发送多点接收的优势在单位专网中保障数据、话音、图像等业务流通信传输得到了越来越重要应用。其优点在于：优化了网络性能，提高网络传输效率（减少网络传输开销，占用更少组播源主机、路由器处理资源、降低网络带宽使用量、无需知道接收者地址，减少接收者观测到的延迟）；分布式交互、可扩展性好（发送者将数据“一次”发送给“无限个”接收者）。

1　专网概况

1.1　专网组网拓扑

单位专网网络拓扑是以一、二级控制中心及外测控站的三层局域网组成的城域网网络拓扑结构，局域网一般呈星型结构，如图 1 所示。

1.2　专网业务应用分析及下步需求

单位专网为实现数据传输实时、可靠传输，网络业务应用主要以组播形式进行。主要有：实时语音、实时图像、指挥显示、时间统一、实时测量数据、实时安全控制数据等。

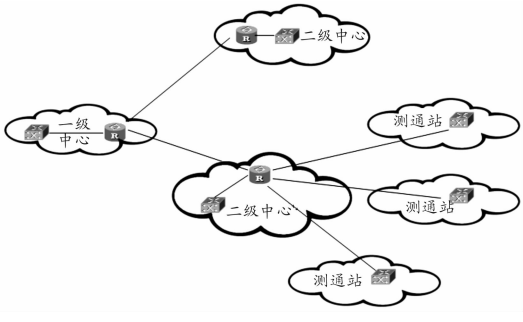

图 1　专网拓扑示意图

其业务应用数据流特性如下：实时突发小数据流（语音）；实时突发大数据流（安全控制数据）；稳定小数据流（指挥显示、时间统一）；实时稳定大数据流（图像、测量数据）。

收稿日期：2015－01－16

作者简介：李乃振（1975—），男，工程师，主要从事计算机网络、网络安全研究。

数据流向为:多个外测控站向二级中心传输交互(图像、测量数据、安全控制数据等);二级中心向一级中心、外测控站传输(语音、指挥显示、时间统一等)。

随着专网网络规模不断扩大,测量设备逐年增加,各测量设备接入 IP 化建设改造不断深入,网络业务应用在向更多、更大的实时稳定大数据流(测量数据)保障需求发展,同时也给专网网络性能、组播业务组织带来很大压力。

2 专网应用业务组播传输设计

2.1 组播传输关键技术

2.1.1 关于组播模型

组播传输有任意源(ASM)、指定源(SSM)二种模型,按实现层次可分为网络层 IP 组播和应用层组播[1],本研究中涉及都为网络层 IP 组播。

在 ASM 组播模型中,任意主机都可以成为组播源,其他接收主机通过加入组播组地址标识的主机组,获得组播信息。该模型中接收主机无法预先知道组播源的位置,并且可以在任意时间加入或离开该主机组。

SSM 组播模型的特点是接收主机已经通过预置信息知道组播源的具体位置,直接在组播源和接收主机间建立最短路径树(SPT),而不是像 ASM 那样先建立共享树(RPT)而后再根据需要转换到最短路径树。SSM 组播模型具有非常突出的优越性,网络中不再需要汇聚点(RP),也不再需要共享树或汇聚点的映射,具有极高的分发树建立效率,同时网络中也不再需要组播源发现协议(MSDP)以完成汇聚点与汇聚点之间的源发现。

2.1.2 关于组播协议

组播协议主要有:用于主机注册的互联网组管理协议(IGMP)和用于组播选路转发的组播路由协议,常见的如协议无关组播协议(PIM)、组播源发现协议(MSDP)和组播扩展边界网关协议(MP - EBGP)等。其在网络中的应用位置图 2 所示。

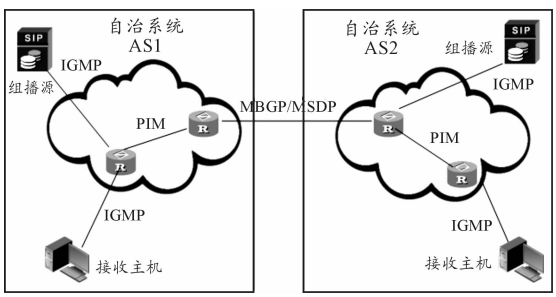

图 2 网络组播协议应用位置示意图

IGMP 是组播管理的基础,它运行于主机和主机相连的组播路由器之间,主要用于管理维护组播成员的关系。它目前有 3 个版本,IGMP v1 中定义了基本的组成员查询和报告过程,IGMP v2 在此基础上添加了组成员快速离开的机制,IGMP v3 中增加的主要功能是成员可以指定接收或指定不接收某些组播源的报文。3 个版本都适用于 ASM,IGMP v3 可以直接应用于 SSM,IGMP v1 和 v2 需要在相关特性(SSM - Mapping)的支持下才可以应用于 SSM。另外,IGMP 组播成员管理机制是针对 OSI 模型第三层设计的,在第三层路由器可以对组播报文的转发进行控制,只要进行适当的接口配置和对 TTL 值的检测就可以了。在二层交换设备为避免组播报文转发设备所有接口,应启用 IGMP 监听特性(IGMP Snooping)[2]。

组播路由协议用于建立和维护组播路由,正确、高效地转发组播数据包,主要运行在组播路由器之间。组播路由建立了一个从数据源端到多个接收端的无环数据传输路径,即构建分发树结构。在 ASM 模型里组播路由分为域内和域间二大类,常用的域内路由协议 PIM 分为密集模型(PIM-DM)、稀疏模型(PIM-SM)二种。常用的域间组播路由协议有组播源发现协议(MSDP)和组播扩展边界网关协议(MP-EBGP)等。SSM 模型没有域内和域间的区分,由于接收主机预先知道组播源的具体位置,因此只需要借助稀疏 PIM SM 构建的通道即可实现组播信息传输。

PIM 工作原理是在单播路由协议基础上,使用单播路由表实现逆向路径转发(RPF)机制,与协议无关,没有独立的组播路由表,不必发送组播路由的更新,这样就节省系统资源。PIM-DM 采用基于源构建分发树,叫做源树,原理是在路由器上对每个源和组播组建立最优路径,使用最短路径的方式(SPF)选择路径,优点是延时小,但保存的路由信息大,消耗系统资源高,适用于小型网络。PIM-SM 基于 RP 构建分发树,也就是 RPT。其原理是在网络中会选取一个点作为公共根,所有的组播报文都需要从这个点来进行传送。它选择的路径不一定是网络中的最优路径,但占用网络资源较少,适用于大型网络。

2.1.3 关于 PIM-SM 协议中 RP 的选择

在 PIM-SM 部署的网络中,RP 的选择、架设位置非常重要,其选择主要有 3 种方式:静态 RP、BSR RP、Anycast RP。

静态 RP 网络中,RP 选择是由配置指定的,需要在网络中每台路由器上指定 RP 的地址。这种方式配置最简单,比较适合在小规模的网络中使用。这种方式不支持备份。

一般情况下 PIM-SM 组网规模都很大,通过 RP 转发的组播信息量巨大,为缓解 RP 的负担同时优化共享树的拓扑结构,不同组播组应该对应不同的 RP,此时就需要自举机制来动态选举 RP,此时需要配置自举路由器 BSR(BootStrap Router)或者 Anycast RP。在自动 RP 方式下,使用多个 RP 来做备份、负载分担,不过在一个组播组只有一个 RP 实时起作用。

Anycast RP 是对自动 RP 的全新扩展,它必须与 MSDP 协议配合,用虚拟 RP 地址代替网络中多个 RP 地址,这样在配置设备时只需知道虚拟 RP 地址,就近选择实际 RP。这样就同时实现负载分担、冗余备份,也增强了网络系统的健壮性,易用性,提升了系统性能。3 种 RP 部署方式的对比,如表 1 所示。

表 1 3 种 RP 部署方式的对比

	静态 RP	BSR RP	Anycast RP
收敛速度	优秀	很好	优秀
易用性	在小网中好,大网中差	优秀	优秀
部署难度	优秀	优秀	优秀
安全性	优秀	很好	优秀
冗余备份	差	很好	优秀
负载分担	差	差	优秀

2.1.4 关于 Anycast RP 的实现机制

Anycast RP 的机制概括为:多个 RP 配置一个相同的 Anycast RP 地址,这个地址使用 RP 上的一个接口(通常是逻辑接口,即 LoopBack 接口)。之后 RP 使用这个接口地址对外发布组到 RP 的映射信息。由于使用的是 Anycast RP 地址,所以组成员在加入时,会向拓扑距离最近的一个 RP 发起。在这些 RP 之间使用各自不同的地址建立 MSDP 连接,利用 MSDP 实现组播源信息在所有 RP 之间的同步。Anycast RP 实际上是 MSDP 在域内的一个特殊应用。

如图 3 所示,PIM-SM 网络采用单自举路由器(BSR)管理域方式,拥有多个组播源和多个接收者。在 PIM-SM 域内配置 Anycast RP,当新成员加入组播组时,与接收者直接相连的路由器能够向拓扑距离最近的 RP 发起加入。PIM-SM 网络中运行 OSPF 提供单播路由。在 Rb 和 Rd 的 Loopback0(Lo:0)接口上配置 MSDP 对等体;Loopback1(Lo:1)接口上配置 C-BSR ;Loopback10(Lo:10)接口上配置 C-RP。

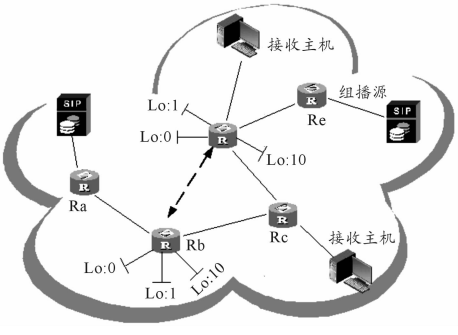

图 3 Anycast RP 配置组网示意图

2.1.5 关于 PIM-SSM 协议的原理及部署

SSM 模型主要解决了 ASM 模型分发树建立过程效率较低的问题。SSM 服务模型是 PIM-SM 协议机制的子集,普通 IP 组播和 SSM 都可以用 PIM-SM 协议实现,它无需 RP 节点,无需构建 RPT 树,无需源注册过程,同时也无需 MSDP 来发现其他 PIM 域内的组播源。

当共存于同一台路由器的时候,SSM 只处理组地址为 232/8 的组播数据和协议。它可以和 PIM-SM 共存于同一台路由器,根据数据和协议报文中的组播地址来决定使用 SSM 还是 PIM-SM。IANA 为 SSM 分配了地址段 232/8,此地址段的组播组不会加入共享树,而是由 SSM 处理。SSM 同样需要通过周期性地发送 HELLO 报文来实现邻居发现和 DR 选举。

SSM 组播路由器和主机之间相互作用是通过 IGMP v3 实现的。当路由器相关接口接收到所连接网络有主机的加入组播组 G(来自源 S)数据报后,根据单播路由向连接组播源的路由器逐跳朝源的方向发送 PIM(S,G)源组加入报文,从而在组播源和连接接收者的最后一跳路由器之间建立起最短路径树。当组播源发送组播数据的时候,这些数据就沿着最短路径树直接到达接收者。在仅支持 IGMPv1/IGMPv2 主机的网络中,可以采用 SSM-Mapping 技术,通过在主机连接的路由器上配置 SSM-Mapping,将 IGMPv1/IGMPv2 发送的组加入报文映射为源组加入,从而应用 SSM 技术。

SSM 具体部署实例如图 4 所示,接收者通过组播方式接收组播信息,来自不同方向的一个或多个接收者主机组成末梢网络。

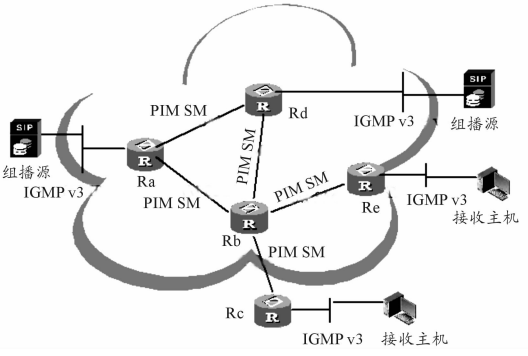

图 4 PIM-SSM 典型配置组网示意图

2.2 专网组播传输设计

通过上述分析,结合专网实际网络拓扑、主机规模、业务数据流大小及流向,建议实施组播传输设计如图 5 所示。

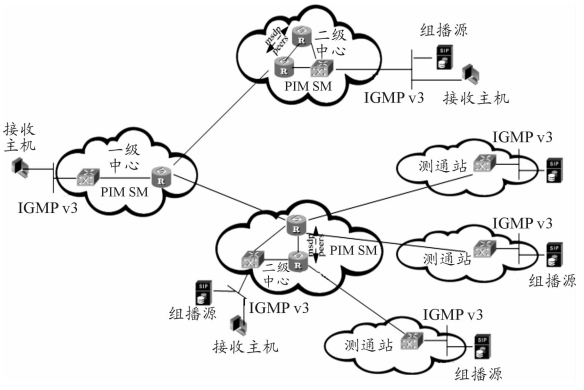

图 5 专网组播应用设计示意图

根据组播主机分布广泛,地域较广,但是设备实际可控,所以只设一个组播域,一、二级中心、测通站都在域内。

组播模型采用 ASM、SSM 混合组网,组播路由协议采用 PIM-SM、PIM-SSM 路由协议混合实施。

在 ASM 模型,实施有备份的环境里采用 Anycast RP 技

术,结合应用 MSDP 协议,实现 RP 的负载分担,其他路由器实施指定静态 RP。

对于部分已知大部分应用业务,采用 SSM 模型,如:指显数据,组播地址 232/8 按不同 2 级节点进行划分。在不支持 IGMP v3 的路由器采用 SSM-Mapping 技术

用户端主机尽量采用组播管理协议 IGMP v3 版本,在 2 层交换机端采用 IGMP Snooping 技术。

3 专网组播应用安全策略

3.1 组播问题分析

在前期专网建设,组播传输保障中,发现专网组播应用存在问题如下:

1) 组播特性方面:由于实时测量遥测数据传输基于 UDP,以尽力方式(best-effort)转发[3],而无重传机制,所以存在因未送达、乱序、重复包等可靠性差问题。由于采用 ASM 模式,存在开放的组成员关系:即任何一个人都可以查看组中的数据或者向组中插入数据;每个人收到的都是相同的数据包:不具备个性化,不可定制;发送者不必具有成员资格:不能对流入组中的信息进行控制,存在访问控制缺乏、RP 单点瓶颈风险、组播转发不经济安全性差缺点。

2) 管理层面:由于专网初期建设,组播应用较少,没有实施安全策略,存在组播地址、端口不规范,组播服务软件不规范(经常有大包、突发流量)问题。没有实施网络统一规划,应用多种组播协议技术,用户业务流使用较乱现象;目前组播接收主机终端越来越多,路由器设备临近使用年限老化、性能下降严重;

因此,建议在专网新一期的建设中,尽量实现可控组播,因此除了进行统一、优化的设计方案外,尤其应配置合适的安全控制策略。

3.2 组播安全策略

1) 组播组管理协议方面

为组播用户指定组播组,在接入交换机配置组播组过滤策略(IGMP group-policy),只允许收到策略允许的正常 IGMP report 报文。在核心汇聚交换机上进行组播组转发过滤,过滤掉非法组播信息流[4]。

控制组播用户,通过对 2 层交换机的端口或 VLAN 的应用 802.1X 协议对用户的组播权限进行验证。如果验证通过,则 2 层设备接收用户的 IGMP 加入/离开的信息,并建立相应的转发表项,允许用户接收组播流量。否则,丢弃用户的 IGMP 报文,禁止用户接收组播流量。并且认证通过后,通过管理平台为用户建立一个组播访问规则表项,用户只能访问授权的组播服务。

在二层交换机启用 IGMP snooping 或私有协议如思科 CGMP 防止组播报文向所有端口转发,实现组播抑制,二层机制下只有发送 IGMP 请求的主机才能接收到组播数据。值得注意的是开启 IGMP snooping 会占用设备一定的 CPU 资源[5]。

尽量安装使用较新支持 IGMP v3 协议操作系统的主机,尽量使用指定源组播模型,筛选数据信息。

2) 组播路由协议方面

实施 ASM 组播模型中应尽量选择性能较高的靠近核心的网络设备作为 RP,为避免出现多个静态 RP 的出现,选用动态竞选(C-RP)的配置方法[3]。配置该设备优先级最高,并进行备选。

为防止 RP 欺骗,BSR(自举路由器)也应配置 C-RP 策略,在对接收到的 C-RP 消息进行匹配时,只有当报文中的 C-RP 地址与策略规定的地址匹配,并且符合指定的组播地址范围时,才认为匹配成功。因动态竞选机制,需在每个 C-BSR 上进行相同过滤策略。

3) 另外

对专网业务数据流进行组播传输需求分析,点对点通信可以走单播的业务尽量走单播,以减少组播协议占用网络设备资源开销,影响系统可靠性。如:测量数据。

对于优先级要求高的实时业务数据流,应限制业务所占带宽,全局配置 QOS。在组播源端,通过流量监控(car)配置承诺访问速率,以监管入口的组播流量,如果组播实际流量超出,则策略对其整形或丢弃。此外,根据需求,通过流分类规则定义组播报文的优先级,在交换机配置优先队列 PQ 调度策略。

针对外部测量信息流汇聚到中心的特点,应重点考虑发送主机至网络设备之间数据传输匹配能力,其次应考虑多个方向大量数据经网络设备汇至中心接收主机,中心主机是否有能力处理这些汇聚信息。还有注意网络设备中间不应出现带宽瓶颈。

尤其注意传输中数据的分包大小应适当选择,最好与网络设备处理能力、如 MTU 等参数相适应,分包太小会占用网络大量 CPU 资源产生丢包,太大了网络设备频繁拆装数据,时延大也容易产生丢包,影响可靠性[6]。在网络资源有限的情况下,适当分包小一些。另外注意组播应用中分包参数等设置也应注意,例如 TTL 设置不应太小[7]。

工程实施中应考虑到组播模式的选择可能对网络中安全保密设备的架设及设置有更为复杂的要求。

4 结束语

随着专网 IP 化逐渐深入建设,IP 业务逐渐增多,组播技术已经成为点对多点多媒体 IP 业务的基础、重要的 IP 传输保障手段,但组播安全技术尤其是可控组播技术目前还没有成熟的标准的现实,需要我们进一步进行探索、研究、实验。

参考文献:

[1] 蒋东星,郑少仁. IP 网络组播技术的新发展[J]. 电信科学,2003(9):9-13.

[2] 朱加勇,施宇星. 组播技术及其在测量船测控网络的应用[J]. 载人航天,2009(3):44-47.

(下转第 124 页)

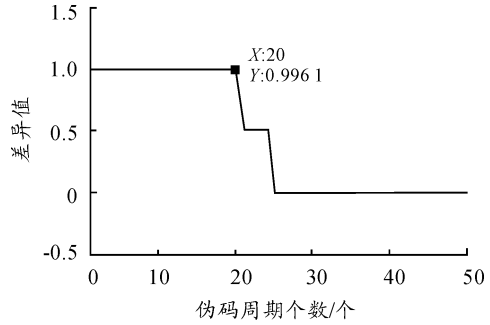

图 4 本地伪码与干扰信号的差异

4 结论

由于无人机在现代战争中地位的迅猛提升,随之出现了多种对抗无人机的软杀伤和硬杀伤手段。本文从电子对抗的角度出发,着重阐述了对无人机的视距测控链路进行牵引干扰。通过研究相关干扰的干扰机理,对 CDL 标准的无人机视距链路实施牵引干扰,并且能够通过重构干扰信号的参数或者调整干扰平台的运动状态,实现对链路终端设备同步跟踪过程的牵引。文中进行了干扰方案的分析,并分析和仿真了整个牵引干扰过程中,接收端本地跟踪伪码分别与合法信号及干扰信号的差异。

参考文献:

[1] 陆文博,刘春生. 对无人机测控系统干扰方法的研究[J]. 舰船电子对抗,2013,36(2):31 - 34.

[2] Shepard Daniel P, Bhatti Jahshan A. Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks [C]//ION-GNSS. Nashville, TN, USA:2012. 3591 - 3605.

[3] 季华益. "全球鹰"及其对抗策略思考[J]. 航天电子对抗,2013,29(1):26 - 30.

[4] Samer S. Saab, Jad G. Hobeika. A Novel Pseudorandom Noise and Band Jammer Generator Using a Composite Sinusoidal Function [J]. IEEE TRANSACTION ON SIGNAL PROCESSION,2010,58(2):874 - 877.

[5] Borio Daniele, O' Driscoll Cillian. Jammer impact on Galileo and GPS receivers [C]//ICL-GNSS. Turin, Italy: IEEE, 2013. 1 - 6.

[6] Qi Zeng, Husheng Li. GPS spoofing attack on time synchronization in wireless networks and detection scheme design [C]//Military Communications Conference. Orlando, FL, USA: IEEE, 2012. 1 - 5.

[7] 许益乔,曾芳玲. 对 M 码信号的转发式干扰技术研究[J]. 火力与指挥控制,2013,38(10):122 - 124.

[8] 郑建忠,易翔. DS-CDMA 信号的动态竞争机制分析[J]. 电子信息对抗技术,2012,27(4):47 - 51.

(责任编辑 杨继森)

(上接第 116 页)

[3] 刘丛,高仲合. IP 组播网络脆弱性分析与安全策略研究[J]. 网络安全技术与应用,2008(5):14 - 16.

[4] 徐俊,陈雪军. 航天测控通信 IP 网中可控组播的实现[J]. 遥测遥控,2012,33(4):61 - 63.

[5] 李光明,游苑,刘佳. IP 通信网组播安全策略分析[J]. 重庆通信学院学报,2013,32(3):23 - 25.

[6] 张海江,于昌民. IP 组播技术在遥测数据传输中的应用分析[J]. 遥测遥控,2011,32(4):70 - 72.

[7] 李康,陈雪军. 航天通信 IP 网组播常见故障解决方法[J]. 遥测遥控,2012,33(2):58 - 62.

(责任编辑 杨继森)