

一种光接入网的组播隔离方案

侯林林, 马 勇

(武汉市公安局 视频侦查支队, 武汉 430000)

摘要:针对传统组播技术无法进行有效隔离和监控视频泄露隐患十分突出等问题,提出了一种基于软件定义网络(SDN)方式的光接入网组播隔离方案,并对该技术方案的实际系统组成及视频组播业务的具体处理过程进行了详细描述。最后描述了该方案相比组播虚拟专用网络(VPN)、软件授权认证等传统技术,由于结合了公有域、私有域的概念,能够有效解决非法用户窃取合法视频及合法用户窃取非授权视频的问题,具有明显的技术与成本优势。

关键词:光接入网; SDN; 组播隔离

中图分类号: O436; TN929.11 文献标识码: A 文章编号: 1002-5561(2018)02-0056-03

DOI: 10.13921/j.cnki.issn1002-5561.2018.03.015

Multicast isolation scheme for optical access networks

HOU Linlin, MA Yong

(Wuhan City Public Security Bureau video investigation detachment, Wuhan 430000, China)

Abstract: In view of traditional multicast technology can't do effective isolation and monitoring video leakage is very prominent, an optical access network multicast isolation scheme based on SDN is proposed, and the actual system composition and specific multicast process is described in detail. Finally, this paper describes that scheme has obvious cost and technical advantages compared with multicast VPN and software authentication due to the use of public and private domain, and it can effectively solve the problem of illegal users stealing legitimate video and legitimate users stealing unauthorized video.

Key words: optical access networks; SDN; multicast isolation

0 引言

目前视频监控网络中视频流占用的带宽越来越高,标清的码流达到 2Mb/s 左右,单播转发机制已无法满足视频监控业务的开展,需要充分运用组播技术来有效地利用当前有限的带宽。而在无源光网络(PON)中,光链路终端(OLT)采用广播的方式将组播数据传送给每个光网络单元(ONU),这种方式非常适合于直播业务,但并不适合视频监控业务。OLT 和 ONU 不加限制地将视频流的组播报文广播出去,不仅浪费大量带宽,还非常不利于监控视频的保密工作,严重影响视频监控业务的正常开展。因此,视频监控系统迫切需要在光接入网中实现组播隔离,保证合法用户可以正常获取监控视频,非法用户则被限制在隔离区域内

无法获取监控视频。因此,本文提出一种基于软件定义网络(SDN)方式的光接入网组播隔离方案^[1],能够有效解决监控视频泄露的问题,并极大节省带宽。

1 基于 SDN 的组播隔离方案

本文所提出的组播隔离方案在功能上与虚拟专用网(VPN)类似^[2]。VPN 通过三层隔离技术保证每个 VPN 的外部用户无法访问 VPN 内部的内容,而 SDN 组播隔离方案不仅通过私有域具备了 VPN 的独立区域访问限制功能,还创造性地提出了公有域和私有域 0 的概念,即公有域内的内容可以被所有用户访问,而私有域 0 内的用户则无法与任何公有域或私有域通信。

1.1 系统组成

相比于传统的 PON 系统,本文提出的 SDN 组播

收稿日期: 2017-10-23。

作者简介: 侯林林(1985-),男,硕士研究生,主要研究方向为光接入网络与软件定义网络方面。

隔离方案技术框架如图 1 所示,增加了中央控制器用于处理域管理及组播表项生成问题。在目前的实现方案中,受制厂商设备的功能实现,中央控制器只能通过 PON 网管控制 OLT 与 ONU 设备。随着 SDN 技术在光接入网的应用,特别是白盒 OLT 及虚拟 OLT(vOLT)技术的引入,在不久的将来,中央控制器可以通过 OpenFlow 等南向接口协议直接控制 OLT 与 ONU 设备。

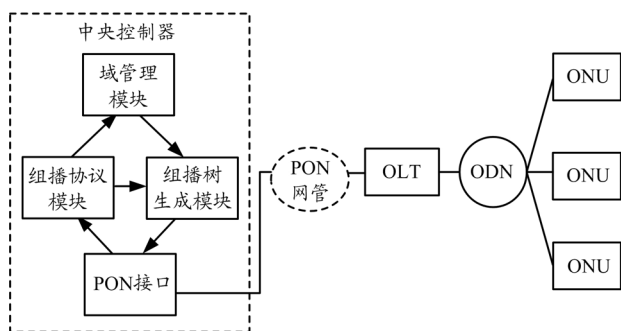


图 1 基于 SDN 的组播隔离方案技术框架

1.2 中央控制器组成

中央控制器包括组播协议模块、域管理模块和组播树生成模块。其中,组播协议模块用于处理 ONU 上报的因特网组播管理协议(IGMP)组播报文^[3],并生成相应的组播表项;域管理模块根据 ONU 上报的 IGMP 组播报文提取用户的位置信息,包括用户所在的 ONU 编号、用户所使用的 ONU 端口和用户的源 IP 地址等,并根据用户的位置信息生成其所属的域,最后由用户所在的域与组播源所在的域确定用户是否能够接收其想接收的组播数据;组播树生成模块根据域管理模块给出的连通信息和组播协议模块生成的组播表项,最终将组播转发规则下发至 OLT 及各 ONU 设备。

上述的组播域分为公有域与私有域,公有域只有一个,私有域可以有多个。公有域可以与所有私有域互通组播数据(私有域 0 除外),所有公共区域的监控视频可以放置在公有域;而私有域之间组播数据不能互通,私有域内的节点只能访问私有域内部的数据,小区或楼宇的内部视频可以放置在私有域内,只允许加入私有域或公有域的用户查看和调阅;未经授权的非法用户会被限制在私有域 0 中。私有域 0 是一个特殊的私有域,除了不能访问其它私有域外,也不能访问公有域,是一个与其它域完全隔离的封闭域,不能确定用户合法性的所有用户都被限制在私有域 0 内,无法访问网络内任何合法主机。

根据用户所在的 ONU 编号、用户所使用的 ONU 端口和用户的源 IP 地址无法确定用户所属的域,以及上述信息与已知用户信息不符的,都会被划入私有域 0,不允许与其它域进行通信。用户所请求的组播源的主机地址不在公有域内或与用户不在同一个私有域内,则中央控制器不会建立组播源至请求用户的组播路径,组播数据不会被转发至发出请求的用户。

但是,如果非法用户通过篡改 IP 地址并侵占合法用户的 ONU 端口,此时,通过 ONU 编号、ONU 端口和源 IP 地址均无法对用户的合法性进行甄别,这是目前方案的局限,未来可考虑联动 802.1X 等协议进一步加强用户的身份认证。

1.3 组播处理流程

组播处理流程如图 2 所示。首先,OLT 通过 PON 网管与中央控制器建立通信。然后,用户发送 IGMP 加组报文,该请求经 OLT 与 ONU 后转发至中央控制器的组播协议模块,组播协议模块根据组播报文生成组播记录表项,向域管理模块发送组播生成请求,其中,

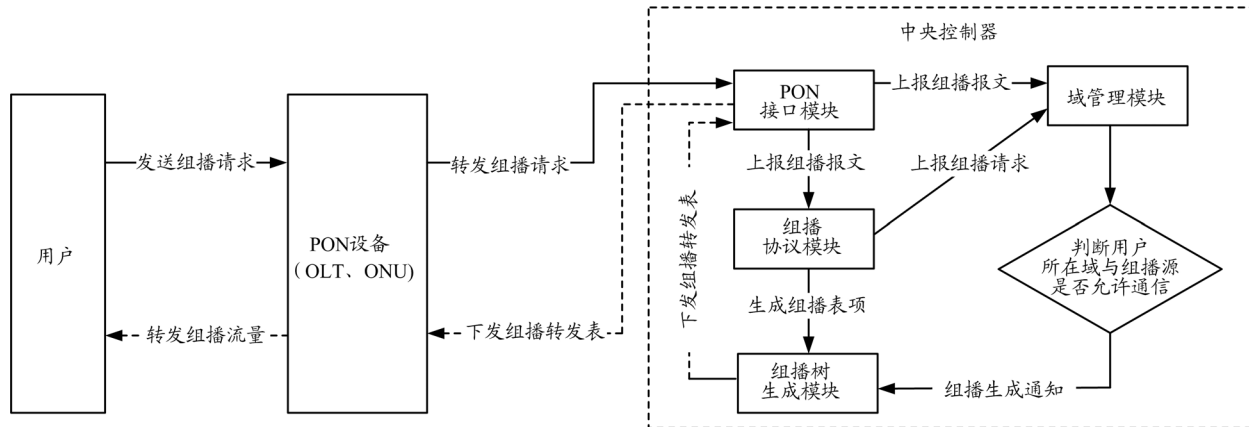


图 2 基于 SDN 的组播隔离方案处理流程

侯林林,马勇:一种光接入网的组播隔离方案

所述组播协议可以是 IGMP 协议或组播侦听发现协议,域管理模块根据从 IGMP 报文中提取的用户位置信息,与所请求的组播数据的域信息,判定用户所请求的组播组中是否有能与用户所在域通信的组播源,如果有,则发送组播生成通知至组播树生成模块,组播树生成模块根据域管理模块发送的组播生成通知和组播协议模块的组播表项信息,生成相应的组播转发表,并通过 PON 接口模块,发送至 OLT 和 ONU,OLT 和 ONU 最终根据中央控制器发送的组播转发表将组播数据转发给用户。如果没有,则丢弃该 IGMP 报文,不做任何处理。

2 基于 SDN 的组播隔离方案的应用

组播隔离方案的具体应用如图 3 所示。街道摄像头 1、街道摄像头 2 与警务用户属于公有域;小区摄像头 1、小区摄像头 2 和小区用户属于私有域 1;非法用户未经授权位于私有域 0 内。在该应用场景中,警务

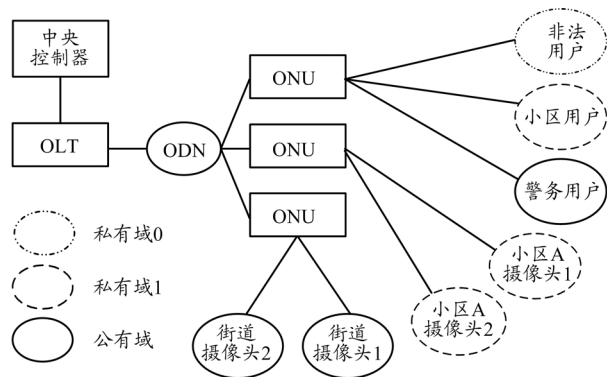


图 3 基于 SDN 的组播隔离方案应用案例

用户可以访问所有街道摄像头与小区摄像头,小区用户只能访问小区摄像头,而非法用户被限制在私有域 0 内,无法访问任何摄像头。

3 结束语

本文提出了一种基于 SDN 方式的光接入网组播隔离方案,并对该技术方案的系统组成、软件构成及组播处理流程进行了详细描述,给出了目前可行的一种实施方案。由于光接入网基本上为二层网络,高端路由器中基于三层网络的组播 VPN 并不适合光接入网,而视频监控系统的用户授权认证方式需要部署配套服务器与软件,成本高昂。本文提出的方案,相比组播 VPN 与视频监控系统的用户授权认证,实现简单、易于部署和使用,具有明显的技术和成本优势。同时相对于目前 PON 系统中的 IGMP Snooping 方案^[4],SDN 组播隔离方案进一步加强了组播授权的功能,非法用户即使发送了组播请求也无法获取到其想要窃取的视频,安全性得到极大提高,这对于视频监控等保密性要求较高的领域具有非常重要的意义。

参考文献:

- [1] 左青云,陈鸣,赵广松,等. 基于 OpenFlow 的 SDN 技术研究[J]. 软件学报, 2013 (5): 1078-1097.
- [2] 陶骏,匡磊,徐旺,等. 基于 MPLS VPN 和 MSDP 的跨域组播网络设计[J]. 计算机科学, 2017, 44(s1): 263-265.
- [3] WILLIAMSON B. IP 组播网络设计开发(第 1 卷)[M]. California: Cisco Press, 2000.
- [4] PARK Wan-Ki, KIM Dae-Young, Convergence of Broadcasting and Communication in Home Network using an EPON-Based Home Gateway and Overlay[J]. IEEE Transactions, 2005, 51(2): 485-493.

会议征文通知

2018年5月22-24日
北京亦创国际会展中心

<http://coina.csoe.org.cn/html/meeting/>

2018年中国（北京）海洋信息网络技术 及产业发展大会

第三轮投稿截止日期:2018年4月15日

稿件提交截止日期:2018年6月30日

稿件接收截止通知:2018年7月31日