疫情下面向大规模直播教学的组网技术研究

林俏伶[1],胡曦明[1,2*],李 鹏[1,2]
(1. 陕西师范大学 计算机科学学院,陕西 西安 710119;
2. 现代教学技术教育部重点实验室,陕西 西安 710119)

摘 要:针对疫情防控期间线上直播成为在线教学主模式的发展现状,深入分析了大规模线上直播教学对数据承载网络提出了持续大规模高密度同步传输、分组式成员动态管理和资源跨域共享安全控制等组网性能新需求。以需求为导向,提出了将 VPN 的安全性与组播数据传输的高效性相结合的“VPN+组播”组网技术,具体给出了域内组播、全域组播和域间混合组播等三种方案设计并从数据传输控制层面详细分析了工作过程。在此基础上,基于 eNSP 仿真平台通过组成员管理、GRE 隧道搭建、IPSec 安全协商以及安全策略调用等步骤给出“VPN+组播”组网技术的仿真实现,并进一步通过数据测量与性能分析验证该组网技术具有组成员管理、交互式安全协商和数据加密传输等性能,从而为大规模线上直播教学提供了切实可行的关键性基础网络技术支撑。

关键词:直播教学;组网技术;虚拟专用网;组播;网络仿真
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2021)06-0140-06
doi:10.3969/j.issn.1673-629X.2021.06.025

Research on Networking Technology for Large-scale Live Teaching under Situation of Epidemic

LIN Qiao-ling[1], HU Xi-ming[1,2*], LI Peng[1,2]
(1. School of Computer Science, Shaanxi Normal University, Xi'an 710119, China;
2. Key Laboratory of Modern Teaching Technology, Ministry of Education, Xi'an 710119, China)

Abstract: Aiming at the development status that online live is regarded as the main mode of online teaching during the epidemic prevention and control period, the in-depth analysis of large-scale online live teaching puts forward new networking performance requirements such as continuous large-scale high-density synchronous transmission, grouped member dynamic management, and cross-domain sharing security control of resources for data carrier networks. Guided by the requirements, the "VPN plus Multicast" networking technology that combines the security of VPN with the efficiency of multicast data transmission is proposed, and the intra-domain multicast networking scheme, all-domain multicast networking scheme and hybrid multicast networking scheme are specifically given while the working process of three schemes is analyzed in detail from the data transmission control level as well. On this basis, based on the eNSP simulation platform, the simulation implementation of "VPN plus Multicast" networking technology is given through the steps of multicast member management, GRE tunnel construction, IPSec security negotiation and security policy invocation. It is further verified through data measurement and performance analysis that the networking technology has the capabilities of group member management, interactive security negotiation, and data encryption transmission, thereby providing practical and feasible key basic network technical support for large-scale online live teaching.

Key words: live teaching; networking technology; VPN; multicast; network simulation

0 引 言

疫情防控期间,全国高校按照教育部《关于在疫情防控期间做好普通高等学校在线教学组织与管理工作的指导意见》(以下简称《指导意见》)的统一部署,全面实施网上教学;各地中小学按照教育部、工信部联合印发的《关于在中小学延期开学期间“停课不停学”有关工作安排的通知》(以下简称《通知》)要求,各地各校因地制宜实施多样化远程教学。从湖北[1]、山

收稿日期:2020-08-13 **修回日期**:2020-12-17
基金项目:国家自然科学基金项目(61877037);陕西省科技计划重点研发项目(2020GY-221)
作者简介:林俏伶(1999-),女,研究方向为计算机科学与技术;通讯作者:胡曦明(1978-),男,博士,讲师,教育硕士导师,研究方向为智慧教育、计算机教育。

西[2]、浙江[3]等省教育主管部门发布的疫情期间教学指导意见并结合在线教学实践来看,线上直播、网络录播和点播是基于互联网开展远程教学的三大方案。据调查显示,最受师生欢迎和线上应用率最高的方案是在线直播。据黑龙江省高校统计,在 29.6 万个在线课堂中直播课堂约 20.6 万余个(占比近 70%),约 70% 的学生表示更喜欢直播课堂和包括直播课堂在内的混合式课堂[4];另据江苏省高等教育学会面向苏南地区 10 所"双高计划"高职院校开展线上教学情况调研发现,教师使用腾讯课堂、钉钉等平台线上教学采用直播授课的占比最高[5];厦门大学通过对 6 所新老不同的地方本科院校在线教学质量报告进行统计分析发现,不论是教师还是学生认可"直播+在线互动"的比例均超过了其他线上教学模式[6]。深入分析疫情下大规模线上直播教学对数据承载网络的组网性能需求,并针对性提出切实可行的组网技术解决方案,不断开拓适宜国内教育需要的信息化技术新路径,从而进一步释放"互联网+教育"巨大潜能和动力,使得主动服务国家教育现代化事业成为富有紧迫性、基础性和应用价值的重要现实课题。

1　大规模线上直播教学的组网需求

1.1　持续大规模高密度同步传输

按照教育部 2020 年 5 月 20 日发布的《2019 年全国教育事业发展统计公报》,国内各级各类学校 53.01 万所,各级各类学历教育在校生规模达 2.82 亿人,其中高校在校生 0.4 亿人,中小学在校生 1.8 亿[7]。面向如此大规模的学生实施群体性的网络教学史无前例,与高校"一校一策、一校多策"在线直播采取分课程分班分阶段的分化分流实施方式不同,基础教育阶段直播教学通常在省级统一部署下按教育部《义务教育课程方案》和《普通高中课程方案》规定的课程和课时,按正常上课时间面向全地区中小学生进行同步课程直播教学。

例如,江西省教育厅印发《江西省中小学 2020 年寒假及春季学期延期开学期间线上教育教学实施方案》,按照全省统一课表、统一课程、统一进度的"三个统一",从 2 月 10 日起开展除初三、高三外的全省 622 万中小学生统一同步在线教学,同步课程通过江西省中小学线上教学平台"赣教云"以及有线电视、江西 IPTV 等渠道进行直播[8];西安市教育局 1 月 30 日印发《西安市 2020 年春季学期中小学幼儿园延期开学"停课不停学"工作方案》由市教育局统一组织,2 月 10 日起全市中小学所有学科课程按统一的直播课表通过西安市优质教育资源共享平台和西安教育电视台向全市中小学生进行同步直播[9]。各地市集中性的同步网上教学给底层承载网络带来了持续性的大规模高密度用户同步数据传输流量,如此前所未有的海量同步数据承载负荷给网络传输服务带来巨大压力,由此造成 2 月 10 日开始线上直播教学当天各地频现网络卡顿、无响应甚至网络崩溃。从技术层面看,区域性大规模成建制在线直播教学业务对网络组网提出了承载持续性大规模高密度同步传输数据的新需求。

1.2　分组式成员动态管理

面对网络拥堵难以保障在线直播教学服务的实际情况,各地加大基于电视的"空中课堂"投放力度,对网络直播教学实施分流。例如,江西广电有线电视和中国电信江西 IPTV 等电视运营商先后安排了 30 个电视频道,总共免费开通 120 个专用频道,同时省教育厅特别推荐使用电视收看同步课程,通过分流用户极大缓解了"赣教云"平台在线直播遭遇的"卡、堵"[10]。通过调整或新开通电视频道架设同步课程教学,"空中课堂"来保障"停课不停学"成为疫情期间全国各地的普遍做法和有益经验。据 5 月 14 日教育部疫情期间大中小学在线教育情况和下一步工作考虑发布会上教育部基础教育司司长吕玉刚介绍,为确保网络畅通,教育部在工信部和国家广播电视总局的大力支持下,于 2 月 17 日正式开通中国教育电视台空中课堂。疫情防控期间,中国教育电视台空中课堂收视率大幅跃升,在全国各大卫视关注度排名中进入前十[11]。由于电视的数据传输方式采用"一对多"的广播方式,网络的数据承载量不会由于用户规模的增加而线性增长,因此可以承载海量用户。但是不论是基于有线电视还是 IPTV 的"空中课堂"都存在处于源端的老师无法对处于电视终端的学生进行个性化学习管理的技术性短板,这与早期的"电视大学"局限十分相似。想要从教学质量和教学管理上保证线上直播教学与线下实体课堂教学实质等效,就需要线上直播教学能支持分学科分班级分课程等分组方式基础之上的成员动态管理,例如创建学习群、群组成员加入与退出等,从而有效支撑在线直播教学过程中线上发布作业、分组讨论、答疑辅导等教学活动。

1.3　资源跨域共享安全控制

疫情期间,按照政府主导、高校主体、社会参与的方式,线上优质教育教学资源共享除了通过由国家、省市各级政府主导的国家中小学网络云平台、国家精品在线开放课程以及 27 个省级网络学习平台等直接输出型供给之外,以高校为主体、社会广泛参与的校际合作,跨校课程和校地协同等各主体间交互型资源共享与直接输出型供给实现了优势互补,成为新的亮点。例如,清华大学先后与华中科技大学、武汉大学、华中农业大学、新疆大学、太原理工大学等 5 所高校通过校

际合作对接、跨校域及地域共享资源，实现了 5 校学生云端同上清华[11]。主体之间跨校域及地域的资源共享，对于构建更大范围的开放学习体系具有广阔的应用前景，但在资源跨域共享过程中也存在安全隐患。由于各主体的安全控制策略不尽相同，主体间的资源跨域共享过程中必然面临域间的安全协商与安全准入、资源跨域安全传输以及信息安全保密等安全性挑战，尤其对于面向未成年人的基础教育资源跨域共享的安全控制更值得高度关注，为此《指导意见》在工作保障部分将“确保在线教学安全平稳运行”单列为一条予以特别强调。

2 基于“VPN+组播”的组网技术

疫情期间在线教学实践表明，一是，线上直播深得一线师生认可，但同时带来持续大规模高密度同步传输需求给底层数据承载网络造成巨大压力；二是，基于电视的“空中课堂”通过一对多的传输方式能够有效保障远程直播教学，但又存在不支持分组式成员动态管理的技术性短板；再者，主体间的资源跨域共享安全控制的需求愈发强烈。该文以实践经验为基础、以问题为导向，探索将 VPN 的安全性与组播数据传输的高效性相结合的“VPN+组播”组网技术，既可为当前大规模线上直播教学提供关键性基础网络技术支撑，又能为面向未来线上教育发展开拓切实可行的技术途径。

2.1 方案设计

（1）方案一：域内组播。

在虚拟专用网（virtual private network，VPN）的隧道技术中，大部分隧道协议支持数据单播，这使得利用 VPN 单播成为跨公网传输数据的优先选择。针对直播教学课堂中的视频数据可先通过单播的方式从 VPN 隧道源端口点对点传送到目的端口，进而使目的端口处的路由器在接收到视频数据后通过域内组播的方式发送给目的域中需要该视频数据的接收者，形成一种 VPN 跨公网单播、局部域内网组播的组网方式，详见图 1 学校 A 与对接学校 B 或对接学校 C 之间的数据传输方式。

（2）方案二：全域组播。

随着 VPN 业务的深入，不同的实际应用对 VPN 组播业务提出了新的需求。利用传统的 VPN 技术与组播技术相结合，使得 VPN 能支持组播数据流跨公网安全传输，且无需进行单播到组播的数据转换，直接将组播数据送达至组播接收方所在的目标网络，既可以提高组播数据的传输效率，也能够增强 VPN 隧道对不同数据的兼容性，详见图 1 学校 A 与对接学校 D 之间的数据传输方式。

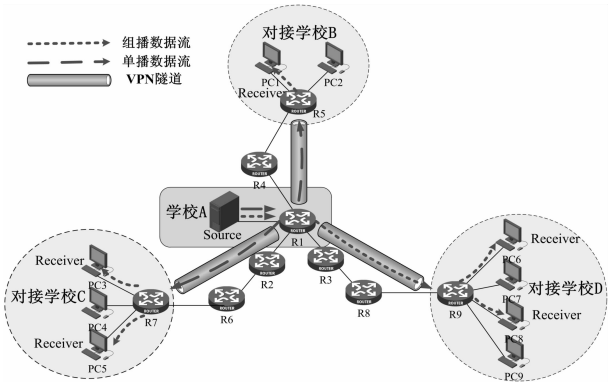

图 1 方案设计拓扑

（3）方案三：域间混合组播。

针对不同网段的多元化需要，可将 VPN 中单播和 VPN 中组播的方式相结合，形成一种混合式组网方案，即部分 VPN 采用的是仅支持单播的隧道协议，数据到达目标网络后再进行组播；其他采用的是支持组播的 VPN，组播数据直接通过 VPN 隧道到达目标网络及其组播接收方，具体如图 1 学校 A 与各对接学校间的数据传输所示。这种混合式的组网方案与前两种方案相比灵活性和可扩展性更强，适合不同网络传输视频数据。

2.2 工作机制

如图 2 所示，基于“VPN+组播”的组网方案的工作过程分为三个阶段：

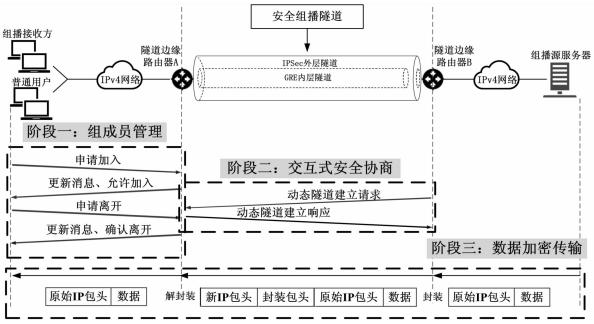

图 2 组网方案工作过程

（1）阶段一：组成员管理。

组播接收方需要向组播组注册成为该组的成员，以告知组播源自身所需的数据及所处的目标网络。通常由连接组播接收方的最后一跳路由器完成 Internet 组管理协议（internet group management protocol，IGMP）的管理，即对组播组成员进行加入、离开、查询等行为的组播组注册信息管理[12-13]，如图 2 阶段一所示，其中隧道边缘路由器 A 将同时充当组播接收方的最后一跳路由器。IGMP 管理能够提高数据分发的准确性和针对性，提出分组分级的概念，协助完成组播数据一对多高效传输的任务。

（2）阶段二：交互式安全协商。

VPN 隧道技术可以有效缓解数据在组播网络传

输中每段单播网络内的安全漏洞所带来的影响。在明确组播组成员所处的目标网络后,通过在组播源服务器和目标网络之间搭建 VPN 网络,能够进一步实现跨区域的数据传播和资源共享。而交互式的协商是搭建 VPN 隧道过程中必不可少的一步。如图 2 阶段二所示,安全组播隧道双方需要动态建立安全连接,该过程由 IPSec 安全协议中的 Internet 密钥交换(internet key exchange,IKE)协议完成[14],作为后续数据加密、认证、完整性校验等安全服务的前提。

(3)阶段三:数据加密传输。

为保障组播数据传输的可靠性与安全性,安全组播隧道综合了 GRE VPN 和 IPSec VPN 两种技术的优势[15-17]。利用 GRE 技术对用户数据和路由协议报文进行隧道封装,使得 VPN 支持组播;然后使用 IPSec 技术来保护 GRE 隧道的安全[18],由此构成可运用到组播应用中的 GRE over IPSec VPN 技术,加密数据报文在隧道传输中的封装过程如图 2 阶段三所示。

3　仿真实现

在上述给出的设计方案的基础上,该文采用由华为提供的图形化网络设备仿真平台 eNSP,主要对网络路由器、服务器等设备进行软件仿真,模拟大型网络。该平台引用了 VLC(video LAN client)跨平台多媒体播放器工具,允许组播源服务器播放多媒体文件模拟发送组播数据;同时利用 Wireshark 网络封包分析软件进行报文撷取和数据测量,为后续性能分析提供数据基础。

3.1　组网拓扑

在上述分析需求的基础上,由于域内组播和域间混合组播均是全域组播的变形与拓展,故该文选取具有代表性的 GRE over IPSec VPN 及全域组播方案进行仿真模拟。对于三个对接学校而言,GRE over IPSec VPN 的功能实现是相同的,所以仿真实现以其中一个分支的网络配置为例做具体描述。仿真拓扑如图 3 所示,路由器 R1 代表学校 A,路由器 R9 代表对接学校 D,其余路由器模拟 Internet 网络,由 OSPF 协议实现网络互联互通,其中对接学校网络 D 内存在组播接收者和普通用户。

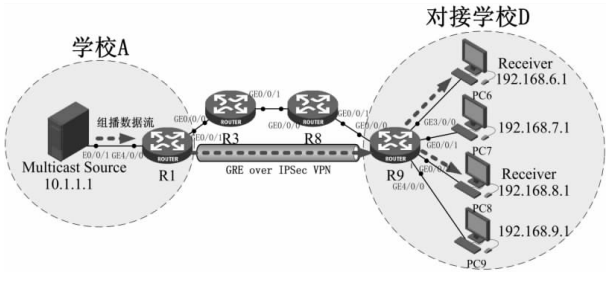

图 3　“VPN+组播”全域组播方案的仿真拓扑

3.2　技术实现

3.2.1　实现步骤

仿真实现的内容包括配置组播信息、配置 GRE 隧道和配置 GRE over IPSec VPN,具体步骤如图 4 所示。

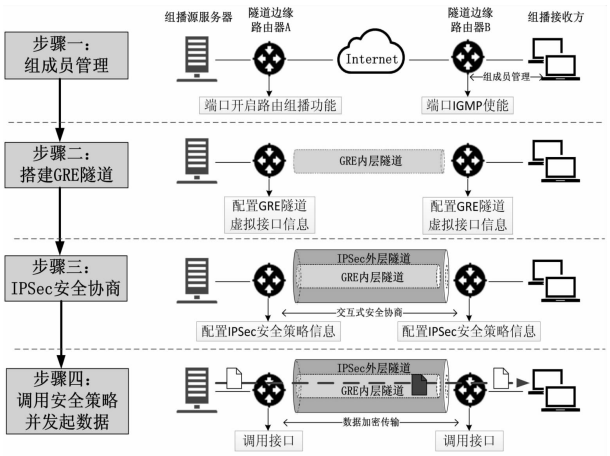

图 4　实现步骤

(1)配置组播信息。

结合图 3 分析,与组播相关的配置包括给组播网络设备,如学校 A 中的组播源服务器和对接学校 D 中的 PC6、PC8 设置组播组地址、开启路由器,如路由器 R1、R9 的组播功能以及 IGMP 使能。

(2)配置 GRE 隧道。

分别对路由器 R1 和 R9 配置 GRE 隧道虚拟源接口和虚拟目的接口的信息,并在组播源所在的学校 A 网络中配置静态路由,令其下一跳指向隧道口,将组播报文流量引入 GRE 隧道,使得数据流只通过隧道到达组播接收方所在的网络。

(3)配置 GRE over IPSec VPN。

在 GRE VPN 实现的基础上继续对路由器 R1 和 R9 进行 IPSec 配置,采用 IKE 动态协商方式建立 IPSec 隧道。在 IPSec 安全提议的配置中,将封装模式定义为传输模式,与隧道模式相比,传输模式下的封装可以避免因新增 IP 包头导致报文长度增加而造成的分片问题;同时采用算法安全性高的对称加密算法和验证算法进一步保障隧道的安全。最后,在隧道接口处调用安全策略并发起数据。

3.2.2　实现过程

GRE over IPSec VPN 对组播数据的处理如图 5 所示。

经检测判断隧道连通性良好后,由组播源服务器向隧道发送组播数据,从而触发 GRE 隧道感兴趣流。组播数据进入隧道后先由 GRE 封装原始报文的 IP 包头信息,产生的新 IP 包头的源 IP 和目的 IP 均变为隧道物理接口地址。经过 IPSec 安全协商后,由 ESP 对新 IP 包头后的数据部分进行加密再封装,并在加密数

据尾部提供校验认证数据,这使得被 GRE 封装后的原始报文再次被封装形成加密报文,最终穿越隧道传输到达隧道目的接口并被解封装成原始报文发送给下游的组播接收方。

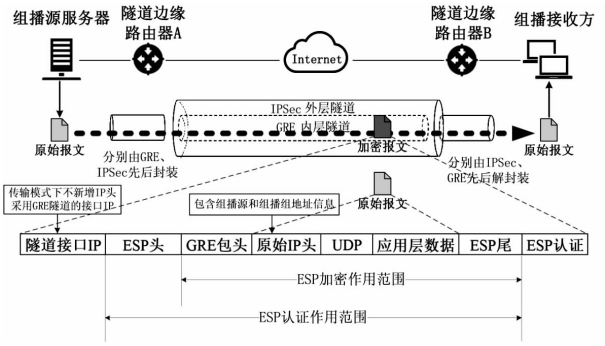

图 5 组播数据穿越隧道传输过程及加密报文格式

3.3 数据测量与性能分析

3.3.1 组成员管理

IGMP 组管理主要针对最后一跳路由器对组成员的查询和管理,具体体现为组成员通过发送成员关系报告报文和成员离开报文实现申请加入和离开操作。在 GRE 隧道实现的基础上,组播源服务器在发起组播数据后由组播接收方依次执行成员的加入和离开操作。

此时捕捉 GRE 隧道中的报文,观察到组播组成员的加入和离开操作分别引起 PIM 协议对上游组播网络发起的加入和剪枝操作,具体如图 6 所示。

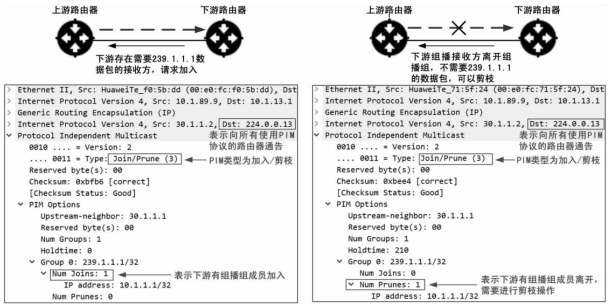

图 6 PIM 协议加入与剪枝实现组成员管理

由此可知,IGMP 能够对组播组成员进行有效的动态成员信息管理,与 PIM 协议相辅相成,及时将组成员信息反馈给上游网络中的路由器完成组播网络的加入和剪枝操作。

3.3.2 交互式安全协商

当 GRE 隧道接口应用 IPSec 安全策略后,抓包发现,IKE 协商过程分为主模式和快速模式两个阶段,如图 7 所示。其中主模式由六个数据包完成策略交换、密钥信息交换和身份和认证信息交换;快速模式由三个数据包建立双方的 IPSec 安全连接,进一步保障了交互的安全,完成安全协商。IKE 协商过程及部分抓包结果如图 8 所示。

No.	Source	Destination	Protocol	Length	Info
6413	10.1.13.1	224.0.0.5	OSPF	82	Hello Packet
6414	10.1.13.1	10.1.89.9	ISAKMP	206	Identity Protection (Main Mode)
6415	10.1.89.9	10.1.13.1	ISAKMP	166	Identity Protection (Main Mode)
6416	10.1.13.1	10.1.89.9	ISAKMP 主模式	190	Identity Protection (Main Mode)
6417	10.1.89.9	10.1.13.1	ISAKMP	190	Identity Protection (Main Mode)
6418	10.1.13.1	10.1.89.9	ISAKMP	110	Identity Protection (Main Mode)
6419	10.1.89.9	10.1.13.1	ISAKMP	110	Identity Protection (Main Mode)
6420	10.1.13.1	10.1.89.9	ISAKMP	206	Quick Mode
6421	10.1.89.9	10.1.13.1	ISAKMP 快速模式	206	Quick Mode
6422	10.1.13.1	10.1.89.9	ISAKMP	94	Quick Mode
6423	10.1.13.3	224.0.0.5	OSPF	82	Hello Packet
6424	10.1.13.1	224.0.0.5	OSPF	82	Hello Packet

图 7 IKE 协商报文

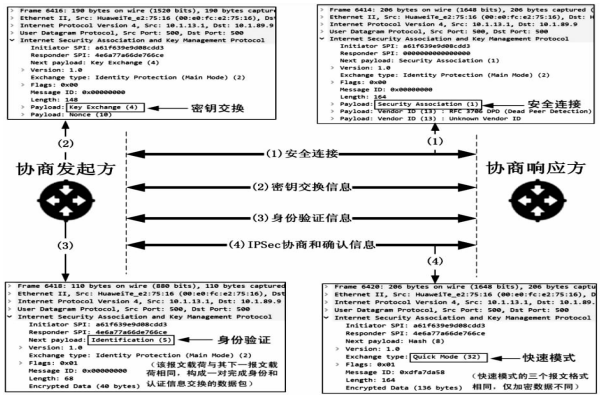

图 8 IKE 交互协商过程

3.3.3 数据加密传输

当网络中仅搭建 GRE 隧道时,此时发起组播流量,在隧道端口处抓包发现 UDP 数据包,说明组播报文能够通过 GRE 隧道穿越公网更高效地传输,其抓包结果如图 9 中上侧报文所示。

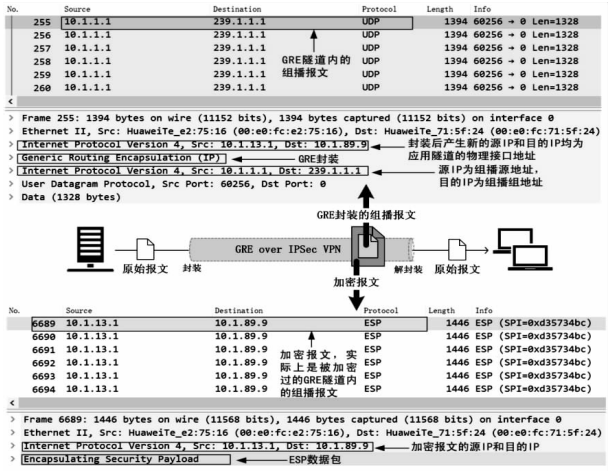

图 9 组播加密报文

分析捕获的数据报文可知,GRE 隧道为原始报文添加了新的 IP 包头,允许组播流量通过隧道传输,但同时数据被暴露,说明此时隧道并不安全,容易造成信

息泄露,故需要在传输中对数据进行加密操作以保障隧道安全。

当完成 GRE over IPSec VPN 的搭建及进行过安全协商后再次发起组播流量,抓包得到 ESP 数据包,如图 9 中下侧报文所示,其源地址和目的地址均是隧道的物理接口地址,无组播源地址和组播组地址。仿真结果说明 GRE over IPSec VPN 对组播数据进行了加密,增强了数据传输的保密性和安全性。

4　结束语

疫情防控期间,全国范围的大中小学校普遍开设线上直播课堂,如此大规模持续性的线上直播业务给数据承载网络带来海量数据同步传输的巨大压力并由此导致网络大面积拥塞。该文充分认识此次大规模、成建制开展在线教育教学实践对底层信息网络提出的持续大规模高密度同步传输、分组式成员动态管理和资源跨域共享安全控制等组网性能需求,基于将 VPN 的安全性与组播数据传输的高效性相结合的设计思路给出了域内组播、全域组播和域间混合组播等三种“VPN+组播”组网技术设计方案,并通过仿真实现了 GRE over IPSec VPN 上的全域组播。仿真结果表明,“VPN+组播”组网技术能够实现组成员管理、交互式安全协商和数据加密传输,既可有效支持疫情防控期间大规模线上直播教学业务,又可为建设适应未来教学资源共享常态化发展的基础网络提供关键技术支撑。

参考文献:

[1] 湖北省教育厅. 关于全省中小学在疫情防控期间开展网络教学的指导意见[EB/OL]. 2020-01-29. http://www.hubei.gov.cn/zhuanti/2020/xgfyyqfkzszq/fwzq/zclxx/msbz/202003/t20200305_2173063.shtml.

[2] 山西省教育厅. 关于全省中小学校在疫情防控期间开展网络教学的指导意见[EB/OL]. 2020-02-05. http://www.shanxi.gov.cn/ztjj/fyyqfk/xgzc/202003/t20200309_768705.shtml.

[3] 浙江省教育厅. 关于防控疫情延迟开学期间在全省中小学全面实施线上教育教学工作的指导意见[EB/OL]. 2020-02-06. http://jyt.zj.gov.cn/art/2020/2/6/art_1532973_41883921.html.

[4] 战德臣. 一种确保高校教学质量的新模式——同步异步混合式教学[J]. 计算机教育,2020(7):1-10.

[5] 李春华,周海英. “停课不停学”在线教学效果提升研究—基于苏南地区高职院校的调查[J]. 职教论坛,2020(4):125-130.

[6] 邬大光,沈忠华. 我国高校开展在线教学的理性思考——基于 6 所本科高校的实证调查[J]. 教育科学,2020,36(2):1-8.

[7] 教育部. 2019 年全国教育事业发展统计公报[EB/OL]. 2020-05-20. http://www.gov.cn/xinwen/2020-05/20/content_5513250.htm.

[8] 江西省教育厅. 停课不停学 2 月 10 日起江西统一安排中小学生在线上课[EB/OL]. 2020-01-31. http://jyt.jiangxi.gov.cn/art/2020/1/31/art_35644_1650809.html.

[9] 西安市教育局. 西安市教育局同步课程直播课表完整发布[EB/OL]. 2020-02-08. http://jyt.shaanxi.gov.cn/jynews/rdjj/202002/08/96613.html.

[10] 钟端浪. 全省统一安排中小学线上教育教学[N]. 江西日报,2020-02-03(002).

[11] 国务院新闻办公室. 教育部举行疫情期间大中小学在线教育情况和下一步工作考虑发布会[EB/OL]. 2020-05-14. http://www.scio.gov.cn/xwfbh/gbwxwfbh/xwfbh/jyb/Document/1679176/1679176.htm.

[12] CONTRERAS L M, ASAEDA M H, BCRNARDOS C J, et al. Enabling new multicast distribution architectures through the introduction of IGMP/MLD proxy with multiple upstream interfaces[C]//2018 IEEE international symposium on broadband multimedia systems and broadcasting (BMSB). Valencia: IEEE, 2018: 1-5.

[13] JUN P, LIJUN B, RENMING Z. The project of multicast setting of campus network in China agricultural university[C]//2012 fourth international conference on computational and information sciences. Chongqing: [s. n.], 2012: 834-836.

[14] SCHULZ S, VARADHARAJAN V, SADEGHI A. The silence of the LANs: efficient leakage resilience for IPsec VPNs[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(2): 221-232.

[15] OGUDO K A. Analyzing generic routing encapsulation (GRE) and IP security (IPSec) tunneling protocols for secured communication over public networks[C]//2019 international conference on advances in big data, computing and data communication systems (icABCD). Winterton, South Africa: IEEE, 2019: 1-9.

[16] JAHAN S, RAHMAN M S, SAHA S. Application specific tunneling protocol selection for virtual private networks[C]//2017 international conference on networking, systems and security (NSysS). Dhaka: IEEE, 2017: 39-44.

[17] LIANG G, SHU X, XIAO H, et al. Evaluation of MVPN technologies for China's NGB backbone networks[C]//2014 IEEE international symposium on broadband multimedia systems and broadcasting. Beijing: IEEE, 2014: 1-5.

[18] 杨菲菲,孙　婧,王　彬. L2TP over IPSec 技术在私有桌面云中的应用[J]. 计算机技术与发展,2015,25(10):160-165.