



P2P 网络视频监控技术机制解析

房新彦, 张艳霞, 崔瑞琳, 罗思维
(天翼物联科技有限公司, 上海 200122)

摘要: 当前, 民用市场中中小企业和家庭视频监控规模呈爆发式增长, 针对上千万摄像机的监控需求, 产业界普遍采用点对点 (peer to peer, P2P) 网络视频监控技术, 综合阐述了 P2P 网络视频监控技术原理, 分析了主流的 P2P 网络视频监控所采用的流媒体控制技术、传输技术以及私网穿越技术, 最后提出了大规模部署的 P2P 视频监控解决方案建议。

关键词: 网络视频监控; P2P; 信令

中图分类号: TP393

文献标志码: A

doi: 10.11959/j.issn.1000-0801.2022295

Research on technology mechanism used in P2P network video surveillance system

FANG Xinyan, ZHANG Yanxia, CUI Ruilin, LUO Siwei
E-Surfing Internet of Things Technology Co., Ltd., Shanghai 200122, China

Abstract: At present, the scale of video monitoring of small and medium-sized enterprises and families in the civil market is growing explosively. In view of the monitoring demand of tens of millions of cameras, peer to peer (P2P) network video monitoring technology was widely used in the industry. The principle of P2P network video monitoring technology was expounded comprehensively, and the streaming media control technology, transmission technology and private network crossing technology adopted by the mainstream P2P network video monitoring were analyzed. Finally, a large-scale deployment of P2P video surveillance solution was proposed.

Key words: network video surveillance, P2P, signaling

0 引言

网络视频监控市场持续火爆升温, 除了公共安全市场持续高速增长, 民用市场中中小企业和家庭视频监控也在爆发式增长, 其需求和传统的公共安全监控需求有明显的不同, 一般来说规模很小, 通常是 1 台或者几台, 而且不会多人同时

查看一路视频, 最多几人同时看, 且几人同时观看的概率较小; 多采用移动侦测或者其他告警触发录像和拍照, 同时通过邮件、短信提醒。

为满足这一类用户需求, 一些安防企业以及运营商普遍采用对等网络 (peer to peer, P2P) 视频监控技术, 这是一种轻量级平台架构, 平台只负责设备的注册认证、远程管理升级及参数查询

等功能,不再承担视频的存储、转发、分发、转码等功能,视频流为点对点的直连传输,不再经平台转发,视频存储采用摄像机直存云存储,平台也不再提供中心存储,此种架构无疑大大减少了平台的软/硬件投资,有效地节约了平台成本,同时点对点直连的流媒体方案缓解了平台压力,使平台具有十万级甚至百万路的用户接入能力,降低了端到端时延,满足中小企业和家庭用户的监控需求。

P2P网络视频监控技术已成为一种发展趋势,下面针对业界关于P2P网络视频监控方案和技术机制进行分析。

1 P2P网络视频监控技术原理

目前,P2P网络视频监控比较有代表性的产品有海康萤石、大华乐橙、中国电信天翼看家和中国移动千里眼等。其中,安防企业的P2P网络监控系统一般采用同类设备或同品牌设备,而中国电信等运营商的P2P网络监控系统可支持多家厂商设备。

P2P网络视频监控通常具备以下特性。

- 标准化:在标准化方面,将多家产品集成在一个系统里面,对标准化和互通性提出的要求非常高,平台提供标准协议接口、标准网元结构,架构上支持多域互联。
- 大容量平台:支持大容量的前端设备接入、流媒体私网穿越转发、客户接入等。
- 大容量存储:支持大容量录像存储任务,且容量具有高扩展性,满足长时间大容量视频图像存储的需求。
- 接口开放:监控系统与其他相关系统的整合更加灵活和统一,提供可开放、可共享的接口,有利于与多种新技术的融合,如5G、智能识别的应用等。

在功能方面,P2P网络视频监控普遍支持视频监控、视频直播、云存储、音/视频通话等服务能力。

- 视频监控:支持摄像机、猫眼等智能终端接入,此外,有的平台还支持模组接入、嵌入式软件开发工具包(sdk)接入,不同接入方式的设备也可以实现互联互通等。
- 视频直播:支持全球广域网(world wideweb, Web)、第5代HTML(HTML5, H5)直播,可提供RTMP/HLS标准流地址,提供高清、标清、流畅等多种码率视频流,支持快速对接实现直播功能,支持云台机的远程超控、实时更新视频、直播时长控制等。
- 云存储:支持监控摄像机将视频直接上传云存储,支持云端录像下载和在线播放。
- 音/视频通话:有的平台还支持一对一、多对多的语音或视频通话,覆盖监控摄像机、儿童手表、安全帽、电视大屏等设备进行远程互动等。

某P2P监控系统工作流程如图1所示,展示了某P2P网络视频监控系统模块组成和P2P建立连接工作流程,主要包括前端IP摄像机、客户端和中心服务平台。其中,中心服务平台通常由中心信令服务器、私网穿越服务器以及云存储服务器组成,各部分均接入IP承载网实现通信。

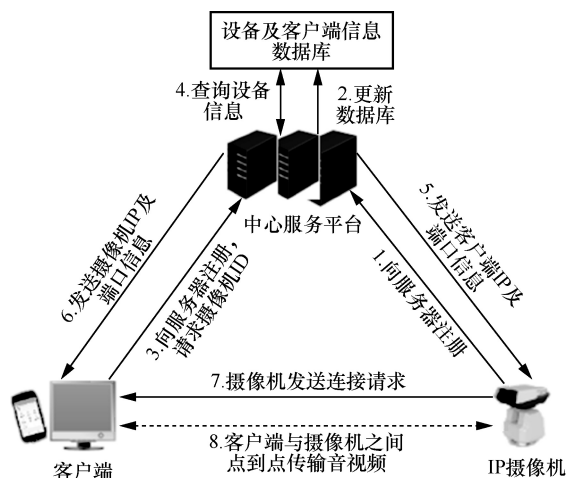


图1 某P2P监控系统工作流程



中心服务平台负责用户和设备的接入管理,提供视频访问和控制服务以及录像处理服务等。其中,中心信令服务器功能模块作为管理中心提供客户/用户管理、前端/平台设备管理、数据库存储业务参数配置数据以及作为门户提供内容发布等功能;云存储服务器作为存储中心存储用户录像视频或抓拍图片;私网穿越服务器为用户访问通过网关接入互联网的 IP 摄像机提供私网穿越解决方案。

前端 IP 摄像机是系统的信息采集端,可实现视频信息、音频信息、数据信息及告警信息的采集功能,可具有语音信息和数据信息的双向传送功能,也可实现音/视频录像的存储功能。

客户端是系统的客户应用端,可完成业务请求/认证等发起、监控列表页面等解析、视频流的解码和播放、发送云镜控制消息等功能。类型可包括 PC 客户端、手机客户端、Web 客户端等。

P2P 网络视频监控技术的主要工作原理是:用户通过电脑终端上的客户端或者手机客户端登录视频监控中心服务平台访问摄像机,初始化信息包含描述会话发起客户端媒体流的配置与特征,信息发送至视频监控中心服务平台信令服务器,信令服务器接收客户端请求后查询信息并通知双方 IP 地址和端口号,假设摄像机同意通信,即接收信息并反馈至客户端,从而在客户端和摄像机之间点到点建立连接传输音/视频。此外,信令服务器还可以为媒体流参数修改以及会话终止消息等提供支持。

2 P2P 网络视频监控主流技术概况

2.1 流媒体传输控制技术

流媒体控制协议是视频监控系统(监控平台、视频服务器、摄像机等设备)间的控制指令集,是建立视频监控图像连接的基本指令集;P2P 视频监控系统使用流媒体传输协议时需要自行定义信令协议,以通知摄像机主动向客户端推送音/视频流。

流媒体控制协议包括以下主流协议。

(1) WebRTC

网页即时通信(Web real-time communication, WebRTC)是一个支持网页浏览器进行实时语音对话或视频对话的应用程序接口(application programming interface, API),它提供了视频的核心技术,包括音/视频的采集、编/解码、网络传输、显示等功能,并且还支持跨平台。WebRTC 协议栈如图 2 所示,WebRTC 使用会话起始协议(session initiation protocol, SIP)进行视频的呼叫及会话管理机制,使用数据报传输层安全与实时传输协议相结合的 DTLS-SRTP(datagram transport layer security-secure real-time transport protocol)在点对点连接中实现了流媒体数据端到端的加密,使用 STUN-TURN-ICE(session traversal utilities for NAT-traversal using relays around NAT-interactive connectivity establishment)实现私网穿越。

数据					信令	
私网穿越			A/V	Data	SIP	
			SRTP	SCTP	HTTP	WebSocket
STUN	TURN	ICE	DTLS	DTLS	TLS	
UDP					TCP	
IP						

图 2 WebRTC 协议栈

此外,一般 P2P 方案中,各浏览器厂商不支持插件,导致 P2P 不能实现网页播放,并且一般的 P2P 方案不支持双向语音,针对门铃场景存在短板,所以采用 WebRTC 可以支持双向语音、支持浏览器且免费,非常适合 IP 摄像机(IP camera, IPC)直播场景,构建支持超低时延直播流式传输和双向实时通信的应用程序。

- 优点: WebRTC 客户端开发简单,可借用成熟 WebRTC 库;使用用户数据报协议(user datagram protocol, UDP)作为流媒体传输层协议,实时通信时延低,一般时延为 200 ms~1 s;该技术不使用第三方插件或软件,可以在不损失质量和不增加时延

的情况下通过防火墙。

- 缺点：在非 Web/Android 平台上开发难度较大，需要自行从 WebRTC 开源框架中剥离自己需要的代码；默认不支持 H.265 编码。

(2) RTSP

实时流协议 (real-time streaming protocol, RTSP) 是一种传统的流媒体控制协议，属于应用层协议，RTSP 传输一般需要 2~3 个通道，其中命令和数据通道分离。RTSP 在服务器和客户端之间建立连接之后，服务器开始持续不断地发送媒体数据包，媒体数据包采用 RTP 进行封装，客户端通过 RTSP 向服务器传达控制命令，如播放、暂停或中断等客户端控制信息通过 RTSP 信息包以 UDP 或传输控制协议 (transmission control protocol, TCP) 的方式传送。

RTSP 协议栈如图 3 所示，RTSP 位于 TCP 之上，RTSP 负责建立和控制会话，使用 TCP 完成数据传输；RTP 数据协议负责对流媒体数据进行封包并实现媒体流的实时传输，RTCP 配合 RTP 做控制和流量统计，RTP/RTCP 使用 TCP 或 UDP 完成数据传输。

会话通道	媒体通道
RTSP	RTP/RTCP
TCP	TCP/UDP
IP	

图 3 RTSP 协议栈

- 优点：传输媒体数据可以使用 UDP，在网络环境比较稳定的情况下，传输效率比较高；RTSP 协议族可以控制到视频帧，因此可以承载实时性很高的应用，一般时延为 500 ms~1 s；倍速播放功能是 RTSP 独有的，其他视频协议都无法支持。
- 缺点：服务器端的复杂度比较高，实现起来也比较复杂；RTSP 没有自适应视频播放

的技术。

(3) SRT

安全可靠传输 (secure reliable transport, SRT) 协议是新一代低时延视频传输协议，是能够在复杂网络环境下实时、准确地传输数据流的开源网络传输技术，它在传输层使用 UDP，实现了安全、稳定、快速的传输效果。

SRT 协议发送支持多个并发流、多个不同的媒体流 (如多个摄像机角度或可选音频轨道)，可以通过在一个点对点链接上共享相同 UDP 端口和地址并行 SRT 流发送。安全方面，SRT 支持高级加密标准 (advanced encryption standard, AES) 加密，保障端到端的视频传输安全。可靠性方面，SRT 通过前向纠正技术保证传输的稳定性。

- 优点：SRT 相关开源库比较成熟，VLC/OBS/FFmpeg 客户端均已支持；实时通信时延低，使用可靠的 UDP 作为传输层协议，一般时延为 500 ms~1 s。
- 缺点：在浏览器上不支持直接播放使用，需要开发专业的 C/S 客户端。

(4) RTMP

实时消息传输协议 (real time messaging protocol, RTMP) 是基于 TCP 的应用层协议，RTMP 主要用来在 Flash/AIR 平台和支持 RTMP 的流媒体/交互服务器之间进行音/视频和数据通信，一般在一个 TCP 通道上传输命令和数据。RTMP 是一个协议族，包括 RTMP 基本协议及 RTMPT/RTMPS/RTMPE 等多种变种。协议中的基本数据单元成为消息，传输的过程中消息会被拆分为更小的消息块单元。最后将分割后的消息块通过 TCP 传输，接收端再反解接收的消息块并将其恢复成流媒体数据。RTMP 一般时延为 1~3 s。

- 优点：RTMP 是专为流媒体开发的协议，对底层的优化比其他协议更加优秀，基本上所有的编码器 (摄像机之类) 都支持



RTMP 输出;稳定性好,因为使用的是 TCP 传输,在互联网环境相对较差的情况下,采用 RTMP 保证了视频的传输质量,适合长时间播放。

- 缺点: RTMP 不使用标准的 HTTP 接口传输数据,所以在一些特殊的网络环境下可能被防火墙屏蔽; RTMP 是一种有状态协议,需要为每一个播放视频流的客户端维护状态,很难对视频服务器进行平滑扩展。

(5) HLS

HLS (HTTP live streaming) 是 Apple 公司开放的基于 HTTP 的流媒体网络传输协议,它的工作原理是把整个流分成一个个小的基于 HTTP 的文件下载,每次只下载一些。HLS 可以在任何浏览器或移动应用程序上直播和点播从设备提取的视频,还可持久地存储视频流并对其进行加密和编制索引。

- 优点: HLS 可以穿过任何允许 HTTP 数据通过的防火墙或者代理服务器; HLS 基于无状态协议 (HTTP), 客户端只是按照顺序使用下载存储在服务器的普通 TS 文件,做负载均衡如同普通的 HTTP 文件服务器的负载均衡一样简单。HLS 协议本身实现了码率自适应,不同带宽的设备可以自动切换到最适合自己码率的视频播放。
- 缺点: 采用 HLS 协议直播的视频时延无法降低到 10 s 以下,所以对直播时延比较敏感的服务不太适用。

(6) DASH

基于 HTTP 的动态自适应多媒体流 (dynamic adaptive streaming over HTTP, DASH) 是国际标准组动态图像专家组 (Moving Picture Experts Group, MPEG) 2014 年推出的技术标准,是基于 HTTP 的动态自适应的比特率流技术,使用的传输协议是 TCP。DASH 和 HLS 技术类似,都是把视频分割成一小段一小段后,通过 HTTP 进

行传输,客户端得到之后进行播放;不同的是 MPEG-DASH 支持 MPEG-2 TS、MP4 等多种格式,可以将视频按照多种编码切割,下载下来的媒体格式既可以是 TS 文件也可以是 MP4 文件,所以当客户端加载视频时,按照当前的网速和支持的编码加载相应的视频片段进行播放。

- 优点: 媒体服务器摄取单个视频源,并将其转码为十几种不同的格式,可以在各种设备和连接速度上实现无缓冲播放,解决多制式传输方案并存格局下的存储与服务能力浪费、运营成本与复杂度高、系统间互操作弱等问题。
- 缺点: iOS 或 Apple TV 不支持;在传递速度方面滞后,时延为 6~30 s,只有通过分块传输编码进行调整或传递时,才有可能降低时延。

2.2 安全传输技术

为保证 P2P 视频监控通信中指令集不包含网络攻击指令、其他非法字符集嵌入或机密数据向外泄露,系统应具备视频协议安全控制功能,对所有视频监控交互指令进行严格安全保护,阻断非法数据传输和网络攻击的入侵。

(1) SSL/TLS

安全套接层 (secure socketslayer, SSL) 和传输层安全 (transport layer security, TLS) 简单理解就是同一件东西的两个演进阶段,同样都是在应用层和传输层之间加入的安全层,最早的时候这个安全层叫做 SSL,由 Netscape 公司推出,后来被 IETF 组织标准化并称为 TLS。

SSL/TLS 体系结构中包含两个协议子层,即记录协议层和握手协议层。记录协议建立在可靠的传输 (如 TCP) 之上,为高层协议提供数据封装、压缩、加密等基本功能;握手协议建立在记录协议之上,用于在实际的数据传输开始之前,通信双方进行身份认证、协商加密算法、交换加密密钥等。

- 优点: SSL/TLS 实施起来比较简单, 对现有网络系统的修改不大, 并且它具有速度快、成本低等优点, 目前已得到广泛的应用; 运用密钥技术保证了数据的完整性和机密性。
- 缺点: SSL/TLS 要求对每个数据进行加密和解密操作, 因而在带来高性能的同时, 也要求系统高资源开销; SSL/TLS 协议不能保证信息的不可抵赖性。

(2) DTLS

由于 SSL/TLS 不能用来保证 UDP 上传输的数据的安全, 因此数据包传输层安全性 (datagram transport layer security, DTLS) 协议在现存的 TLS 协议架构上提出扩展使之支持 UDP, 成为 TLS 的一个支持数据包传输的版本。SSL/TLS 基于 TCP, 因此不需要担心重放、乱序、丢包的问题, 可靠传输由 TCP 做保证; 而 DTLS 基于 UDP, UDP 是一种尽力而为的协议, 因此 DTLS 需要自己处理重放、乱序、丢包的问题。

- 优点: DTLS 可以保证 UDP 上传输的数据的安全。
- 缺点: DTLS 是基于 UDP 的, 不可避免地会出现丢包需要重传的情况, 如果处理不当, 会导致通信双方无法建立会话, 通话失败。

(3) HTTPS

安全套接层超文本传输协议 (Hyper Text Transfer Protocol over Secure Socket Layer, HTTPS) 在 HTTP 的基础上通过传输加密和身份认证保证了传输过程的安全性, HTTPS 主要由两部分组成: HTTP + SSL/TLS, 也就是在 HTTP 上又加了一层处理加密信息的模块。服务端和客户端的信息传输都会通过 TLS 进行加密。

- 优点: HTTPS 可以提供更加优质、保密的信息, 保证了用户数据的安全性, 此外也在一定程度上保护了服务端, 使用恶意攻

击和伪装数据的成本大大提高。

- 缺点: HTTPS 加重了服务端的负担, 与 HTTP 相比, 其需要更多的资源支撑, 同时也降低了用户的访问速度。

2.3 P2P 监控中私网穿越技术

在现实 Internet 环境中, 大多数计算机主机位于防火墙或 NAT 之后, 只有少部分主机能够直接接入 Internet。很多时候, 希望网络中的两台主机能够直接进行通信 (即所谓的 P2P 通信), 而不需要其他公共服务器的中转。由于主机可能位于防火墙或 NAT 之后, 在进行 P2P 通信之前, 需要进行检测以确认它们之间能否进行 P2P 通信以及如何通信, 这种技术通常被称为 NAT 穿越 (NAT traversal)。目前采用的私网穿越技术主要有通用即插即用 (universal plug and play, UPNP)、NAT 的 UDP 简单穿越 (simple traversal of UDP through NATs, STUN)、使用中继穿越 NAT (traversal using relays around NAT, TURN) 和交互式连通建立方式 (interactive connectivity establishment, ICE)。

(1) UPNP

UPNP 网关自动配置端口映射, 将来自 NAT 外部端口的数据包转发到网络摄像机使用的内部端口上, 用户无须手动映射端口或者进行其他工作。UPNP 私网穿越的前提是要求所有网关必须要开启 UPNP 服务。

(2) STUN

STUN 是一种处理 NAT 传输的协议, 它允许位于 NAT (或双重 NAT) 后的客户端找出自己绑定的公网地址以及端口, 即私网中的终端通过某种机制预先得到公网上的服务地址, 然后在报文净载中所要求的地址信息就直接填写该公网地址。STUN 的缺点是不适用于双方都位于同一个 NAT 之后的场景, 不适合支持 TCP 连接的穿越, 需要终端支持 STUN CLIENT 的功能以及不支持对防火墙的穿越等。



(3) TURN

TURN 是 STUN 的一个拓展, 主要添加了 Relay 功能, 即在该模式中私网终端发出的报文都要经过 TURN Server 进行 Relay 转发。TURN Server 控制分配地址和端口, 能分配 RTP/RTCP 地址对 (RTCP 端口号为 RTP 端口号加 1) 作为私网终端用户的接收地址, 避免了 STUN 方式中出口 NAT 对 RTP/RTCP 地址端口号的任意分配, 使得客户端无法收到对端发来的 RTCP 报文 (对端发 RTCP 报文时, 目的端口号缺省按 RTP 端口号加 1 发送)。TURN 与 STUN 的共同点都是通过修改应用层中的私网地址达到 NAT 穿透的效果。与 STUN 的不同点包括: STUN 得到的地址为出口 NAT 上的外部地址; TURN 得到的地址为 TURN Server 上的公网地址, 且支持基于 TCP 的应用等。TURN 的主要缺点是需要终端支持 TURN CLIENT 的功能、所有报文都必须经过 TURN Server 转发, 增大了包的时延和丢包的可能性等。

(4) ICE

ICE 并非一种新的协议, 它综合运用 STUN、TURN 或 RSIP (realm specific IP), 使之在最适合的情况下工作, 以弥补单独使用其中任何一种所带来的固有缺陷, 它不需要对 STUN、TURN 或 RSIP 进行扩展就可适用于各种 NAT。ICE 原理是通过通信双方互相发探测包, 首先探测内网地址, 再探测 STUN 提供的反射地址, 最后探测 TURN 协议的中继地址, 从而找出一种可行路径。ICE 私网穿越技术使用前提是需要每一个客户端和摄像机支持 traversal 方。

3 大规模部署的 P2P 视频监控技术分析

3.1 大规模部署 P2P 监控架构

大规模部署 P2P 监控架构可采用“中心+区域/边缘节点”二级部署方案架构, 如图 4 所示, 管理节点部署中心信令服务器 (包括设备管理、

数据库服务、接口服务、调度服务及节点管理等), 区域/边缘节点部署区域信令服务器 (包括设备接入服务、级联服务等) 和区域私网穿越服务器 (TURN 和 STUN), 摄像机视频存储一般直接上联分布式云存储系统或第三方云存储系统。

针对二级架构, 摄像机设备注册时涉及中心平台和区域/边缘节点, 需要处理好设备注册和管理信息, 流程如下。

步骤 1 设备向中心平台发起请求, 主要上报设备编号以及设备验证码。

步骤 2 中心平台检查其数据库是否已经保存该设备, 如果没有则进行保存入库; 如果已经入库, 则检查该设备是否已经被某区域平台确认使用。

步骤 3 如果设备确认没有被区域平台使用, 则返回给设备错误, 后续设备继续向中心平台发送重定向请求, 直到返回 200OK。

步骤 4 用户使用客户端添加设备, 向区域平台发起注册请求。

步骤 5 区域平台首先在其自身数据库进行检查, 如果已被绑定则提示错误, 如果未被绑定则进行合法性验证并绑定。

步骤 6 如果区域平台数据库没有该设备记录, 则区域平台向中心平台进行查询请求, 如果查询到该编号的设备已经向中心平台申请重定向, 则区域平台在其数据库添加该设备记录, 并允许用户保存。

步骤 7 中心平台在接收到区域平台的查询请求后, 首先确认该设备在数据库内, 并且未被其他区域平台使用, 则设备划归该区域平台; 否则返回错误。

步骤 8 当中心平台已将设备划归某区域平台, 则设备注册请求返回 200OK, 并携带划归区域平台的接入地址。

步骤 9 设备向区域平台注册。

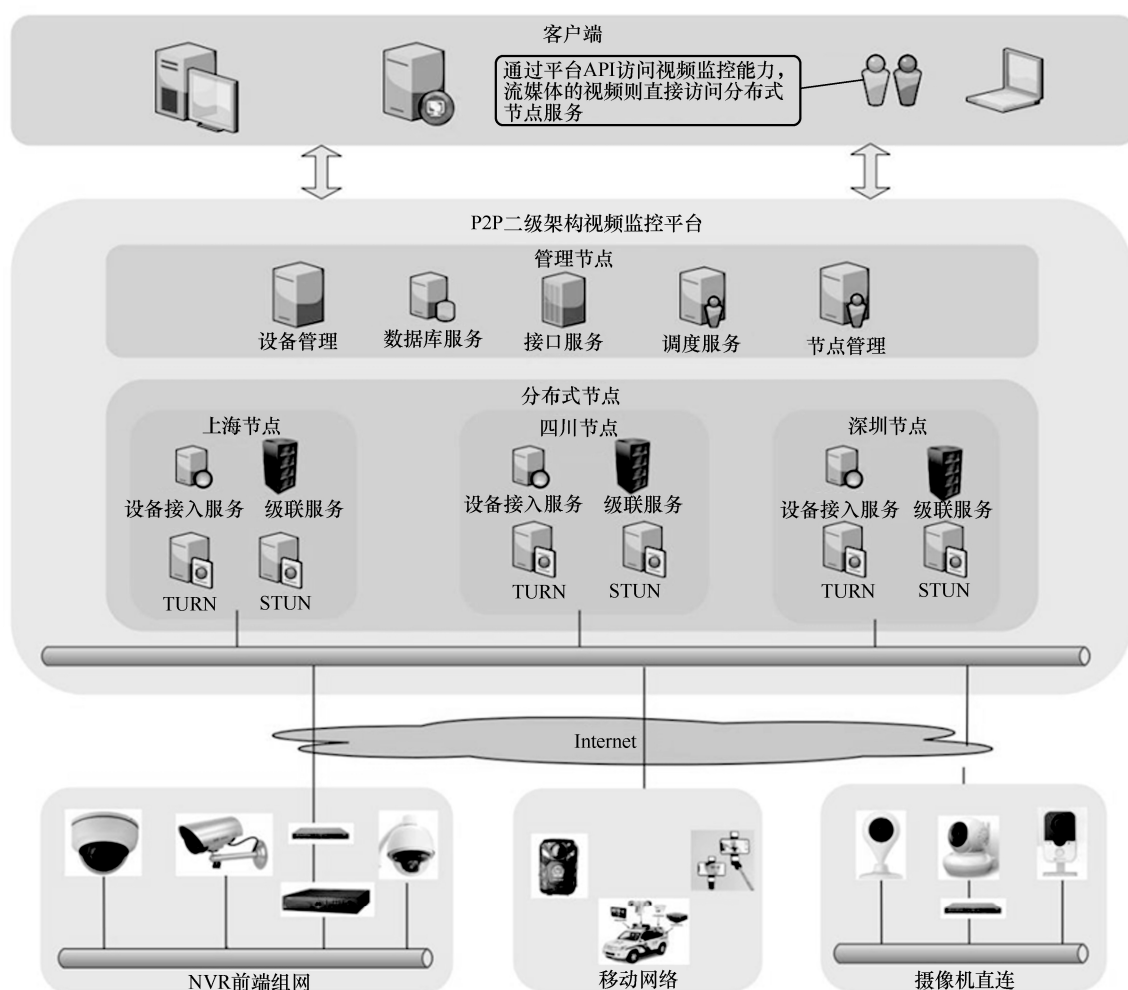


图4 “中心+区域/边缘节点”二级部署方案架构

步骤 10 区域平台检查该设备是否已经入库，如果是从中心平台验证则已经入库并绑定给用户；否则如果没有入库则进行入库，返回平台终端接入服务器地址（支持设备直接配置接入区域平台，无须首先接入中心平台）。

3.2 大规模部署 P2P 监控协议分析

视频监控系统业务数据和媒体数据通常采用分离的通道进行操作，其传输通道类型可分为信令流和媒体流。由于摄像机是被动接受视频呼叫请求，故摄像机需要与服务器之间设计一套信令通信协议，用于进行视频的呼叫及会话管理机制；而媒体流是指传输的视频、音频和数据流。

P2P 网络视频监控主流协议见表 1，涉及多种控制、传输、视频编码、私网穿越等协议。

表 1 P2P 网络视频监控主流协议

主流协议类型	协议种类
流媒体传输控制协议	WebRTC、RTSP、SRT、RTMP、HLS、RTP、HTTP、DASH 等
安全传输协议	TSL、SSL、DTSL、HTTPS 等
音/视频封装格式	MP4、MOV、MKV、AVI、PS 等
视频编码协议	H.264、H.265、H.266、AV1 等
私网穿越协议	TURN、STUN、ICE 等

以亚马逊为例，其视频监控系统支持的多媒体协议包括 HLS、WebRtc、RTSP、DASH，其中采用 WebRtc 协议对接摄像机、Web 端和移动端，终端和用户可以利用 WebRTC 功能进行双向实时媒体流式传输与交互；采用 HLS 对接 Web 端和移动端，DASH 是动态适应网络的媒体协议，用



户采用基于 HLS/DASH 主流的协议播放观看；采用 RTSP 支持多种媒体播放器；在私网穿越方面，包含用于 TURN 的托管终端节点，以便在应用程序无法流式传输对等媒体时通过云启用媒体中继；还包含用于 STUN 的托管终端节点，以便应用程序在位于 NAT 或防火墙之后时能够发现其公有 IP 地址。

3.3 基于多技术集成的私网穿透方案分析

在 P2P 点到点视频监控应用中，IP 摄像机连接到网关后使用的是私网地址，NAT 会将客户机私网地址和端口 {X:y} 转换成公网地址和端口 {A:b} 并绑定，当处于公网的用户访问位于私网的摄像机时会出现私网穿越的问题。

针对采用 SIP/RTSP 信令协议的 P2P 点到点视频监控，SIP/RTSP 协议无法穿过 NAT 回送信令，因为 SIP/RTSP 信令中的 From 和 Contact 头域记录的是私网地址和端口 {X:y}，NAT 无法识别和转换，所以针对 UPNP 私网穿越技术，平台侧信令服务器通过与摄像机的 Socket 连接获取其公网接入地址，从协议中获取其网关映射端口和终端

本地网络端口并保存。但如果仅采用 UPNP 或者 DDNS 技术，至多可解决 20% 左右的视频 P2P 传输（而且上门安装配置复杂，无法实现即插即用）。此外，中小企业的适用场景比家庭复杂，如会涉及网络设备的级联，且其网关设备往往不是定制的，因此要网关都配置支持 UPNP 也不现实，而如果采用 STUN 技术又不适用于对称型 NAT，采用 TURN 又增大了包的时延和丢包的可能性，因此，适用于各种类型的 NAT 的集成多种私网穿越技术的方案是较好的技术选择。

由于媒体流穿透 NAT 的过程是独立于具体的信令协议的，所以平台侧需要部署 STUN 和 TURN 服务器提供媒体流转发服务。

私网穿越方案流程如图 5 所示，集成了多种私网穿越技术。

步骤 1 网络摄像机与客户端在同一局域网内，客户端直接访问网络摄像机本地地址，该种情况不需用采用私网穿越技术。该情况在现实应用中仅占 1% 的情况。

步骤 2 当网络摄像机在一层路由器下，

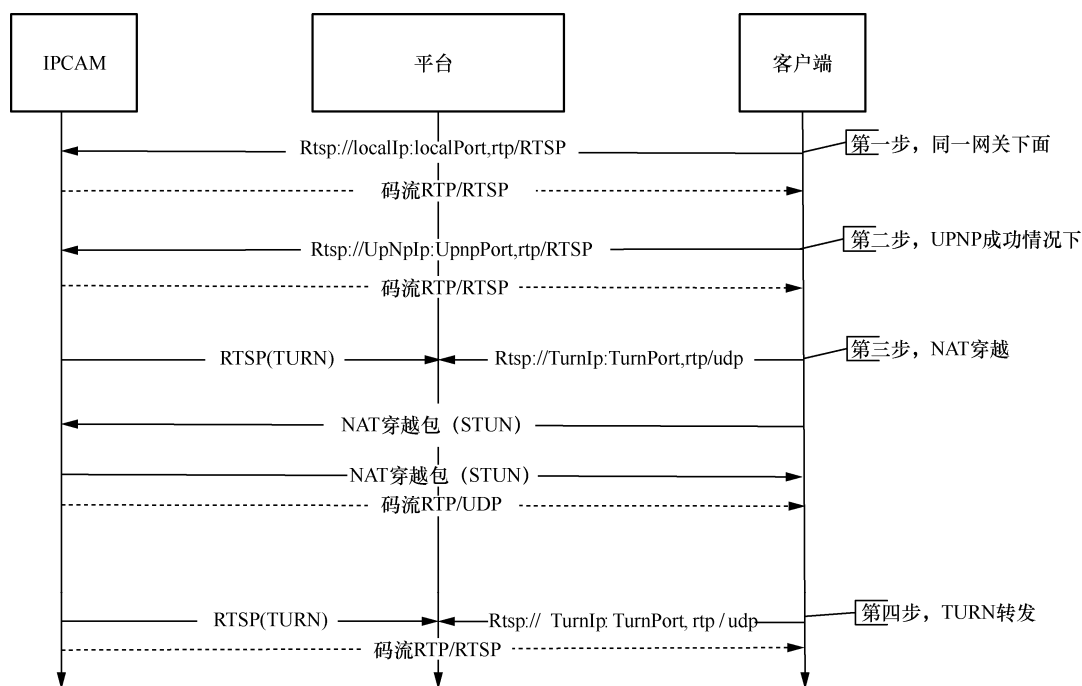


图 5 私网穿越方案流程

并且 UPNP 自动端口映射成功, 则客户端在非局域网情况下优先使用该协议进行 P2P 视频流请求。该情况在实际使用时, 可覆盖 20% 左右的用户。

步骤 3 当网络摄像机处于多层路由器之后或者 UPNP 不通的情况下, 客户端与网络摄像机分别使用 STUN 协议到平台进行 NAT 端口映射, 然后分别向对方映射端口发送 UDP 穿网包进行 P2P 打洞。在该情况下, 可解决现实情况中 90% 以上用户进行 P2P 视频传输。

步骤 4 以上 3 种情况结合使用, 可对现实环境的 98% 以上用户进行 P2P 视频传输。其余 2% 无法进行 P2P 传输视频的情况, 采用 TURN 国际标准协议进行视频转发。

4 结束语

本文综合阐述了 P2P 网络视频监控技术原理, 分析了主流的 P2P 网络视频监控所采用的流媒体控制技术、传输技术以及私网穿越技术。此外, 随着 P2P 视频监控涵盖越来越多的业务场景, 相应的技术也在向标准化、智能化、开放化和规模化等方向发展。例如, 在实际应用中平台侧往往支持多种标准协议, 以支持多种终端厂商产品的统一接入和全协议播放能力。平台既能针对标准化的应用场景提供即插即用的标准化产品, 也可通过能力开放支持定制化场景需求。在规模化方面, 通常采用云存储技术保障大规模视频存储的需求。智能算法部署在云 AI 算力服务上, 可与云存储节点、区域节点同址部署, 以减少 AI 能力获取视频/图片时的机房公网/专线带宽资源等, 多种技术的发展和融合应用保障了 P2P 视频监控支持上千万个视频监控终端, 支撑跨用户群融合场景和应用。

参考文献:

- [1] 梁笃国, 张艳霞, 曹宁, 等. 网络视频监控技术与智能应用[M]. 北京: 人民邮电出版社, 2013.
LIANG D G, ZHANG Y X, CAO N, et al. Network video surveillance technology and intelligent application[M]. Beijing: Posts and Telecommunications Press, 2013.
- [2] 杨磊, 张艳霞, 梁笃国, 等. 网络视频监控技术[M]. 北京: 中国传媒大学出版社, 2017.
YANG L, ZHANG Y X, LIANG D G, et al. Network video surveillance technology[M]. Beijing: Communication University of China Press, 2017.
- [3] 蔡彦. 基于 P2P 架构下的移动“全球眼”系统实现及性能分析[D]. 上海: 上海交通大学, 2011.
CAI Y. Video surveillance system called mobiling “global eyes” over P2P[D]. Shanghai: Shanghai Jiao Tong University, 2011.
- [4] 李永明. 利用 UDP 穿越 P2P 网络中 NAT 的技术研究[J]. 软件导刊, 2012, 11(9): 126-128.
LI Y M. Research on traversing NAT in P2P network using UDP[J]. Software Guide, 2012, 11(9): 126-128.
- [5] 黄辉, 张涛, 孙菲. “全球眼”系统云化演进思路分析[J]. 电信技术, 2012(3): 9-11.
HUANG H, ZHANG T, SUN F. Analysis on cloud evolution of “global eye” system[J]. Telecommunications Technology, 2012(3): 9-11.
- [6] 季一木, 袁永阁, 张苏锐. 一种新型 P2P 流媒体协议及其流量模型研究[J]. 计算机工程与科学, 2014, 36(11): 2100-2105.
JI Y M, YUAN Y G, ZHANG S R. A novel P2P streaming protocol and its traffic model[J]. Computer Engineering & Science, 2014, 36(11): 2100-2105.
- [7] 刘沛钊. P2P 流媒体关键技术的研究进展[J]. 电子技术与软件工程, 2014(3): 21.
LIU P Z. Research progress on key technologies of P2P streaming media[J]. Electronic Technology & Software Engineering, 2014(3): 21.
- [8] 霍龙社, 甘震. 移动流媒体协议综述[J]. 信息通信技术, 2010, 4(4): 6-13.
HUO L S, GAN Z. Review on streaming media protocols over the mobile Internet[J]. Information and Communications Technologies, 2010, 4(4): 6-13.
- [9] 赵宇. WebRTC 技术在语音平台中的应用研究[J]. 通信技术, 2018, 51(2): 506-510.
ZHAO Y. Exploration on IVR solutions of WebRTC technology[J]. Communications Technology, 2018, 51(2): 506-510.
- [10] 李波, 李雪梦, 王彦本. 基于 RTP 的 WebRTC 音视频传输优化方法[J]. 西安邮电大学学报, 2019, 24(1): 26-30.
LI B, LI X M, WANG Y B. WebRTC audio and video transmission optimization method based on RTP[J]. Journal of Xi'an University of Posts and Telecommunications, 2019, 24(1): 26-30.
- [11] 孙建伟, 陈立, 王卫. 基于 SIP 协议的 WebRTC 信令研究与应用[J]. 计算机系统应用, 2018, 27(9): 273-277.
SUN J W, CHEN L, WANG W. Research and application of WebRTC signaling based on SIP protocol[J]. Computer Systems & Applications, 2018, 27(9): 273-277.



- [12] LO W T, CHANG Y S, SHEU R K, et al. Implementation and evaluation of large-scale video surveillance system based on P2P architecture and cloud computing[J]. International Journal of Distributed Sensor Networks, 2014, 10(4): 375871.
- [13] KIM S, JEONG J. Design and performance analysis of a novel P2P-SIP architecture for network-based mobility support in intelligent home networks[C]//Proceedings of 2013 IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks. Piscataway: IEEE Press, 2013: 310-317.
- [14] HOUNGUE P, DAMIANI E, GLITHO R. Overcoming NAT traversal issue for SIP-based communication in P2P networks[C]//Proceedings of 2011 4th Joint IFIP Wireless and Mobile Networking Conference (WMNC 2011). Piscataway: IEEE Press, 2011: 1-8.



张艳霞（1974—），女，天翼物联科技有限公司正高级工程师，主要从事视频监控系统产品开发、技术标准制定等工作。



崔瑞琳（1973—），女，天翼物联科技有限公司工程师，主要从事视频监控系统产品开发、技术标准制定等工作。

[作者简介]



房新彦（1982—），男，天翼物联科技有限公司工程师，主要从事视频监控系统产品开发、技术标准制定等工作。



罗思维（1990—），男，天翼物联科技有限公司工程师，主要从事视频监控系统产品开发、技术标准制定等工作。