(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107911362 B
(45)授权公告日 2020.09.29

(21)申请号 201711124608.5

(22)申请日 2017.11.14

(65)同一申请的已公布的文献号
申请公布号 CN 107911362 A

(43)申请公布日 2018.04.13

(73)专利权人 杭州万为科技有限责任公司
地址 310052 浙江省杭州市滨江区六和路368号一幢(北)三楼D3113室

(72)发明人 何圣斌 张海君

(74)专利代理机构 杭州中成专利事务所有限公司 33212
代理人 金祺

(51)Int.Cl.
*H04L 29/06*(2006.01)
*H04N 7/18*(2006.01)

(56)对比文件
CN 104219500 A,2014.12.17
CN 201789587 U,2011.04.06
CN 104284165 A,2015.01.14
CN 102547251 A,2012.07.04
CN 104270618 A,2015.01.07
KR 101773768 B1,2017.09.13

审查员 刘叶

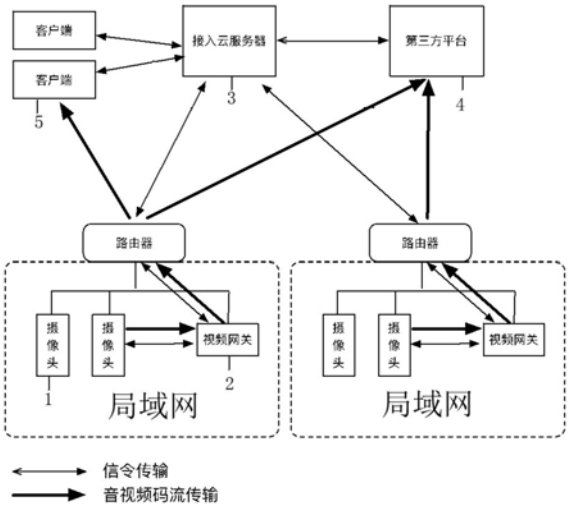
权利要求书3页 说明书10页 附图1页

(54)发明名称

轻量级的互联网视频网关安全接入的系统及方法

(57)摘要

本发明提出一种轻量级的互联网视频网关安全接入的系统,包括摄像头、视频网关、接入云服务器、第三方平台和客户端;视频网关通过局域网与该局域网内所有摄像头相连;视频网关、接入云服务器和第三方平台两两信号相连,且视频网关和接入云服务器均与客户端信号相连。本发明还提出一种轻量级的互联网视频网关安全接入的方法,当用户通过第三方平台或客户端对向接入云服务器下发拉流指令,接入云服务器接收并转发给视频网关,视频网关根据指令控制摄像头,并将该摄像头采集的音视频码流直接发送至对应的第三方平台或客户端,从而使信令与音视频码流分离传输,实现轻量级低成本的社会面监控视频接入,降低了接入云服务器的带宽需求。




CN 107911362 B

1.利用轻量级的互联网视频网关安全接入的系统进行的轻量级的互联网视频网关安全接入的方法,其特征在于:

系统包括第三方平台(4);

所述系统包括至少一个与第三方平台(4)信号相连的接入云服务器(3);

每个接入云服务器(3)分别与至少一个客户端(5)和至少一个视频网关(2)信号相连,每个视频网关(2)与至少一个摄像头(1)信号相连,每个客户端(5)通过视频网关(2)和与其相对应的摄像头(1)信号相连;

所述视频网关(2)均与第三方平台(4)信号相连;

所述摄像头(1)用于对监控视频的采集、保存和上传;所述摄像头(1)将监控视频信息以及采集到的监控视频发送到视频网关(2);所述监控视频信息至少包括摄像头(1)的ID;

所述视频网关(2)用于集中管理其所在局域网里的摄像头(1),视频网关(2)收集和更新摄像头(1)发送的监控视频信息,并将监控视频信息和视频网关信息同步至接入云服务器(3);所述视频网关信息至少包括视频网关(2)的ID;所述视频网关(2)还用于接收摄像头(1)发送的监控视频,并将其进行封装和加密后转发至第三方平台(4)或客户端(5);

所述客户端(5)和第三方平台(4)均用于向接入云服务器(3)发送控制、查询或拉流指令;所述客户端(5)和第三方平台(4)均用于接收和播放视频网关(2)发送的监控视频;

所述接入云服务器(3)用于汇总视频网关(2)上报的视频网关信息和监控视频信息,并为客户端(5)和第三方平台(4)提供访问上述两种信息的服务;所述接入云服务器(3)接收客户端(5)或第三方平台(4)发送的控制、查询或拉流指令,并根据指令将该指令转发至对应的视频网关(2);

所述视频网关(2)还用于接收和响应接入云服务器(3)发送的控制、查询或拉流指令;

所述接入云服务器(3)还用于收集和汇总用户信息及权限,并将每个用户的用户信息与对应的监控视频信息相绑定;

所述客户端(5)根据用户的用户信息及权限相绑定的监控视频信息,管理相对应摄像头(1)的监控视频;

所述第三方平台(4)对所有摄像头(1)采集的监控视频进行集中管理;

方法包括以下步骤:

S1、所述视频网关(2)收集并及时更新其所在局域网里的监控视频信息,视频网关(2)将所有的视频网关信息和监控视频信息通过信令通道上报到接入云服务器(3);

S2、所述接入云服务器(3)接收、保存并更新步骤S1中视频网关(2)上报的视频网关信息和监控视频信息,并将所有视频网关信息和监控视频信息进行汇总;所述接入云服务器(3)、客户端(5)和第三方平台(4)提供访问视频网关信息和监控视频信息的服务;

S3、所述客户端(5)或者第三方平台(4)向接入云服务器(3)发送控制、查询以及拉流指令,接入云服务器(3)接收该指令,并将其转发到视频网关(2);

所述视频网关(2)接收由接入云服务器(3)所发送的控制、查询或拉流指令,并根据指令控制摄像头(1)进行相应的操作;

所述步骤S3中客户端(5)或者第三方平台(4)向接入云服务器(3)发送拉流指令时,包括以下步骤:

1.1、所述客户端(5)或者第三方平台(4)向接入云服务器(3)发送拉流指令;

1.2、所述接入云服务器(3)接收步骤1.1中的拉流指令，接入云服务器(3)将该拉流指令转换为私有协议对应功能的指令，并通过信令通道发送给相应的视频网关(2)；

1.3、所述视频网关(2)接收步骤1.2中由接入云服务器(3)所转发的拉流指令，根据拉流指令向对应的摄像头(1)发送拉流请求，并准备接收摄像头(1)的码流；摄像头(1)接收并响应拉流请求；

1.4、所述视频网关(2)将步骤1.3中对摄像头(1)发送拉流请求的结果通过信令通道发送给接入云服务器(3)；

1.5、所述接入云服务器(3)接收步骤1.4中由视频网关(2)发送的拉流结果，并将其发送给发出拉流指令的客户端(5)或第三方平台(4)；

1.6、所述摄像头(1)接收步骤1.3中由视频网关(2)发送的拉流指令后，不停地将码流发送给视频网关(2)，视频网关(2)根据拉流指令中码流格式封装码流，根据音视频码流是否加密的信息将码流按照要求加密，之后通过音视频码流接收者地址发送给码流接收者。

2.根据权利要求1所述的轻量级的互联网视频网关安全接入的方法，其特征在于：

所述用户通过客户端(5)或者第三方平台(4)接收并观看步骤1.6中发送的视频码流后，进行关闭码流操作，包括依次进行的以下步骤：

2.1、所述客户端(5)或第三方平台(4)向接入云服务器(3)发送关闭码流指令；所述关闭拉流指令至少包括：目标信息和会话ID；

2.2、所述接入云服务器(3)通过信令通道向视频网关(2)发送码流关闭指令，接入云服务器(3)向客户端(5)或第三方平台(4)返回关闭结果；

2.3、所述视频网关(2)接收到码流关闭指令，关闭摄像头(1)的码流，并通过信令通道向接入云服务器(3)发送确认信息。

3.根据权利要求2所述的轻量级的互联网视频网关安全接入的方法，其特征在于：

所述步骤S3中客户端(5)或者第三方平台(4)向接入云服务器(3)发送查询或控制指令时，包括依次进行的以下步骤：

3.1、所述客户端(5)或者第三方平台(4)向接入云服务器(3)发送查询或控制指令；

3.2、所述接入云服务器(3)接收步骤3.1中的查询或控制指令，接入云服务器(3)将该查询或控制指令转换为私有协议对应功能的指令，并通过信令通道发送给相应的视频网关(2)；

3.3、所述视频网关(2)接收步骤3.2中由接入云服务器(3)所转发的查询或控制指令，根据查询或控制指令向对应的摄像头(1)发送查询或控制请求，摄像头(1)接收并响应该查询或控制请求；

3.4、所述视频网关(2)将步骤3.3中对摄像头(1)控制/查询请求的结果通过信令通道发送给接入云服务器(3)；

3.5、所述接入云服务器(3)接收步骤3.4中由视频网关(2)发送的控制/查询结果，并将其发送给发出控制/查询指令的客户端(5)或第三方平台(4)。

4.根据权利要求1~3任一所述的轻量级的互联网视频网关安全接入的方法，其特征在于：

所述视频网关信息还至少包括视频网关(2)的名称、厂家、型号、系统平台、区域和备注信息；

所述监控视频信息还至少包括摄像头(1)的名称、厂家、型号、备注、状态、是否支持云台、录像状态、通道数目及通道号；

所述用户信息至少包括用户名和密码；

所述控制指令至少包括：目标信息、会话ID和控制类型及参数；

所述查询指令至少包括：目标信息、会话ID和查询类型及参数；

所述拉流指令至少包括：目标信息、会话ID、拉流类型及参数、音视频码流接收者地址、码流格式和加密类型；

所述控制指令、查询指令、拉流指令中的目标信息为具体的视频网关(2)的ID、摄像头(1)的ID以及通道号，或者为能够被接入云服务器(3)翻译为具体的视频网关(2)的ID、摄像头(1)的ID以及通道号的编码。

# 轻量级的互联网视频网关安全接入的系统及方法

## 技术领域

[0001] 本发明涉及视频监控领域，具体涉及一种轻量级的互联网视频网关安全接入的系统及方法。

## 背景技术

[0002] 现今很多地方都存在将社会面大量的分散的摄像头接入到互联网平台，进行集中统一管理以及远程访问的需求。由于音视频数据量一般比较大，比较占用带宽，如25路4mbps的码流就可以占满百兆带宽，250路就可以占满千兆带宽，且社会面接入的监控视频量是非常大，可以达到几千甚至几万个摄像头，因此对服务器网络带宽的需求较高。

[0003] 现如今安防需求扩大到了社会面和互联网，大量的安防系统和设备是遵循GB28181标准，而该标准是为安防专网网络制定的，由于国标接入需要两端的IP地址和端口都是固定的，而局域网中的IP和端口无法固定，比如端口是随机的，IP地址是运营商分配，并没有考虑NAT(网络地址转换)的情况，从而使互联网上的服务器(GB28181上级)无法接入NAT(网络地址转换)后面的局域网中的摄像头(GB28181下级)；现今众多前端摄像头存在于NAT后的局域网中，修改现有的安防系统软件和设备的工程较大，因此现有技术中将大量摄像头接入互联网平台进行统一管理以及远程访问的接入方案存在对服务器和相关设备要求太高以及对现有的设备兼容性差的缺点。

[0004] 在申请号为201610954750.1的发明专利《一种基于HTML5浏览器的音视频直播方法》中提出了用户端和主播端通过WebRTC建立通信通道进行视频流和音频流的传输以及消息传输，用户端和主播端建立通信后由用户端浏览器接收和处理数据；该方法直接将主播端的视频流和音频流传输至用户端不需要再完全依赖服务器推流，极大减轻了网络服务器的压力，但是该视频直播与视频监控的技术领域不同，且该直播视频的传输方法无法直接套用在监控视频的传输中。

[0005] 因此，需要对现有技术进行改进。

## 发明内容

[0006] 本发明要解决的技术问题是提出一种轻量级的互联网视频网关安全接入的系统，及通过该系统实现的轻量级的互联网视频网关安全接入的方法。

[0007] 为了解决上述技术问题，本发明提出一种轻量级的互联网视频网关安全接入的系统，包括第三方平台；

[0008] 所述系统包括至少一个与第三方平台信号相连的接入云服务器；

[0009] 每个接入云服务器分别与至少一个客户端和至少一个视频网关信号相连，每个视频网关与至少一个摄像头信号相连(同一局域网下的所有摄像头)，每个客户端通过视频网关和与其相对应的摄像头信号相连；

[0010] 所述视频网关均与第三方平台信号相连；

[0011] 所述摄像头用于对监控视频的采集、保存和上传；所述摄像头将监控视频信息以

及采集到的监控视频(即,监控视频的码流)发送到视频网关;所述监控视频信息至少包括摄像头的ID;

[0012] 所述视频网关用于集中管理其所在局域网里的摄像头,视频网关收集和更新摄像头发送的监控视频信息,并将监控视频信息和视频网关信息同步至接入云服务器;所述视频网关信息至少包括视频网关的ID;所述视频网关还用于接收摄像头发送的监控视频,并将其进行封装和加密后转发至第三方平台或客户端;

[0013] 所述客户端和第三方平台均用于向接入云服务器发送控制、查询或拉流指令;所述客户端和第三方平台均用于接收和播放视频网关发送的监控视频;

[0014] 所述接入云服务器用于汇总视频网关上报的视频网关信息和监控视频信息,并为客户端和第三方平台提供访问上述两种信息的服务;所述接入云服务器接收客户端或第三方平台发送的控制、查询或拉流指令,并根据指令将该指令转发至对应的视频网关;

[0015] 所述视频网关还用于接收和响应接入云服务器发送的控制、查询或拉流指令(即视频网关根据指令内容控制摄像头进行相应操作)。

[0016] 作为本发明轻量级的互联网视频网关安全接入的系统的改进:

[0017] 所述接入云服务器还用于收集和汇总用户信息及权限,并将每个用户的用户信息与对应的监控视频信息相绑定;

[0018] 所述客户端根据用户的用户信息及权限相绑定的监控视频信息,管理相对应摄像头的监控视频;

[0019] 所述第三方平台对所有摄像头采集的监控视频进行集中管理。

[0020] 作为本发明轻量级的互联网视频网关安全接入的系统的进一步改进:

[0021] 所述视频网关信息还至少包括视频网关的名称、厂家、型号、系统平台、区域(即视频网关所在区域)和备注信息;

[0022] 所述监控视频信息还至少包括摄像头的名称、厂家、型号、备注和状态(是否在线等)、是否支持云台、录像状态、通道数目及通道号;

[0023] 所述用户信息至少包括用户名和密码。

[0024] 作为本发明轻量级的互联网视频网关安全接入的系统的进一步改进:

[0025] 所述控制指令至少包括:目标信息、会话ID和控制类型(即,云台控制、启用录像、禁用录像或固件升级)及参数(如,上下左右旋转方向或步进控制,以及开或关);

[0026] 所述查询指令至少包括:目标信息、会话ID和查询类型(即,录像列表,其他均为主动上报)及参数(如,录像列表参数);

[0027] 所述拉流指令至少包括:目标信息、会话ID、拉流类型(即,实时视频或录像视频)及参数(如,实时视频包含清晰度参数,录像包含录像时间段参数)、音视频码流接收者地址、码流格式和加密类型(即,加密或不加密)。

[0028] 作为本发明轻量级的互联网视频网关安全接入的系统的进一步改进:

[0029] 所述控制、查询拉流指令中的目标信息为具体的视频网关的ID、摄像头的ID以及通道号,或者为能够被接入云服务器翻译为具体的视频网关的ID、摄像头的ID以及通道号的编码。

[0030] 本发明还提出一种轻量级的互联网视频网关安全接入的方法,包括以下步骤:

[0031] S1、所述视频网关收集并及时更新其所在局域网里的监控视频信息,视频网关将

所有的视频网关信息和监控视频信息通过信令通道上报到接入云服务器；

[0032] S2、所述接入云服务器接收、保存并更新步骤S1中视频网关上报的视频网关信息和监控视频信息，并将所有视频网关信息和监控视频信息进行汇总；所述接入云服务器、客户端和第三方平台提供访问视频网关信息和监控视频信息的服务；

[0033] S3、所述客户端或者第三方平台向接入云服务器发送控制、查询以及拉流指令，接入云服务器接收该指令，并将其转发到视频网关；

[0034] 所述视频网关接收由接入云服务器所发送的控制、查询或拉流指令，并根据指令控制摄像头进行相应的操作。

[0035] 作为轻量级的互联网视频网关安全接入的方法的改进：

[0036] 所述步骤S3中客户端或者第三方平台向接入云服务器发送拉流指令时，包括以下步骤：

[0037] 1.1、所述客户端或者第三方平台向接入云服务器发送拉流指令；

[0038] 1.2、所述接入云服务器接收步骤1.1中的拉流指令，接入云服务器将该拉流指令转换为私有协议对应功能的指令，并通过信令通道发送给相应的视频网关；

[0039] 1.3、所述视频网关接收步骤1.2中由接入云服务器所转发的拉流指令，根据拉流指令向对应的摄像头发送拉流请求，并准备接收摄像头的码流；摄像头接收并响应拉流请求；

[0040] 1.4、所述视频网关将步骤1.3中对摄像头发送拉流请求的结果通过信令通道发送给接入云服务器；

[0041] 1.5、所述接入云服务器接收步骤1.4中由视频网关发送的拉流结果，并将其发送给发出拉流指令的客户端或第三方平台；

[0042] 1.6、所述摄像头接收步骤1.3中由视频网关发送的拉流指令后，不停地将码流发送给视频网关，视频网关根据拉流指令中码流格式封装码流，根据音视频码流是否加密的信息将码流按照要求加密(或不加密)，之后通过音视频码流接收者地址发送给码流接收者。

[0043] 作为轻量级的互联网视频网关安全接入的方法的进一步改进：

[0044] 所述用户通过客户端或者第三方平台接收并观看步骤1.6中发送的视频码流后，进行关闭码流操作，包括依次进行的以下步骤：

[0045] 2.1、所述客户端或第三方平台向接入云服务器发送关闭码流指令；所述关闭拉流指令至少包括：目标信息和会话ID(该会话ID为将关闭的拉流指令的会话ID)；

[0046] 2.2、所述接入云服务器通过信令通道向视频网关发送码流关闭指令，接入云服务器向客户端或第三方平台返回关闭结果；

[0047] 2.3、所述视频网关接收到码流关闭指令，关闭摄像头的码流，并通过信令通道向接入云服务器发送确认信息。

[0048] 作为轻量级的互联网视频网关安全接入的方法的进一步改进：

[0049] 所述步骤S3中客户端或者第三方平台向接入云服务器发送查询或控制指令时，包括依次进行的以下步骤：

[0050] 3.1、所述客户端或者第三方平台向接入云服务器发送查询或控制指令；

[0051] 3.2、所述接入云服务器接收步骤3.1中的查询或控制指令，接入云服务器将该拉

流指令转换为私有协议对应功能的指令，并通过信令通道发送给相应的视频网关；

[0052] 3.3、所述视频网关接收步骤3.2中由接入云服务器所转发的查询或控制指令，根据控制指令向对应的摄像头发送查询或控制请求，摄像头接收并响应该查询或控制请求；

[0053] 3.4、所述视频网关将步骤3.3中对摄像头控制/查询请求的结果通过信令通道发送给接入云服务器；

[0054] 3.5、所述接入云服务器接收步骤3.4中由视频网关发送的控制/查询结果，并将其发送给发出控制/查询指令的客户端或第三方平台。

[0055] 与现有技术相比，本发明的技术优势在于：

[0056] 1、本发明通过将视频网关与接入云服务器的组合，并将信令与音视频码流分离传输，音视频码流直接传输至第三方平台或客户端，从而实现轻量级低成本的社会面监控视频接入，降低了接入云服务器的带宽需求；

[0057] 2、本发明通过与局域网中的摄像头直接对接的视频网关，从而不必推翻现有网络结构或重新设计部署新的网络，只需在现有网络基础上进行简单改造；视频网关还根据实际情况对所传输的信令进行转化，从而简化接入云服务器的信令，并降低接入云服务器的复杂度和资源消耗；

[0058] 3、本发明接入云服务器可以在不修改现有的安防系统软件和设备的情况下，与视频网关配合工作，令摄像头无缝对接到现有的视频管理平台(如GB28181上级平台)，即，第三方平台。

## 附图说明

[0059] 下面结合附图对本发明的具体实施方式作进一步详细说明。

[0060] 图1为本发明一种轻量级的互联网视频网关安全接入的系统的组成框架示意图；本图还体现了本发明一种轻量级的互联网视频网关安全接入的方法的数据流。

## 具体实施方式

[0061] 下面结合具体实施例对本发明进行进一步描述，但本发明的保护范围并不仅限于此。

[0062] 实施例1、一种轻量级的互联网视频网关安全接入的系统，如图1所示，包括摄像头1、视频网关2、接入云服务器3、第三方平台4和客户端5；其中视频网关2位于局域网中，并通过局域网与该局域网内所有摄像头1相连；接入云服务器3、第三方平台4和客户端5位于互联网中，视频网关2、接入云服务器3和第三方平台4两两信号相连，且视频网关2和接入云服务器3均与客户端5信号相连。

[0063] 注：图1中的路由器为现有技术中进行保障通讯的稳定性的常用技术，因此在本说明书对路由器与其他模块的连接关系，及其工作内容进行省略。图1中双箭头表示两个模块之间信令传输，单箭头表示音视频码流沿着该箭头方向在各模块中进行传输。

[0064] 第三方平台4为现有的视频管理平台，本实施例中第三方平台4采用现有的GB28181上级平台；本实施例设有至少一个与第三方平台4信号相连的接入云服务器3，每个接入云服务器3与至少一个客户端5和至少一个视频网关2信号相连；每个视频网关2与至少一个摄像头1信号相连(同一局域网下的所有摄像头1)；每个客户端5通过视频网关2和与其

相对应的摄像头1信号相连;视频网关2均与第三方平台4信号相连。

[0065] 上述每个摄像头1、视频网关2、接入云服务器3和客户端5的工作内容均相同,故本说明书中仅针对依次信号相连的单个摄像头1、视频网关2和接入云服务器3,以及用于控制上述摄像头1的客户端5(该客户端5分别与上述视频网关2和接入云服务器3信号相连)进行详细描述。

[0066] 摄像头1用于实现对监控视频的采集、保存及上传,本实施例中摄像头1可采用IPC(IP Camera,网络摄像机)和NVR(Network Video Recorder,网络硬盘录像机)等多种摄像装置。摄像头1将监控视频信息和所采集的监控视频的码流(即,音视频码流)通过局域网发送至视频网关2。

[0067] 视频网关2集中管理其所在局域网里的摄像头1,视频网关2接收和更新所有摄像头1所发送的监控视频信息,并将视频网关信息和监控视频信息同步至接入云服务器3;视频网关还用于接收摄像头1发送的音视频码流,并将其直接转发至第三方平台4或客户端5。

[0068] 视频网关信息至少包括视频网关2的ID,还可以根据实际工作需要添加视频网关2的名称、厂家、型号、系统平台、区域(即视频网关2所在区域)和备注信息等信息。监控视频信息保存在相应的视频网关2的ID下,监控视频信息至少包含摄像头1的ID,还可根据实际工作需要添加摄像头1的名称、厂家、型号、备注、状态(是否在线等)、是否支持云台、录像状态、通道数目及通道号等信息;其中IPC有一个视频通道,NVR有多个视频通道,对应通道的通道号根据数字顺序编号(例如通道数目为4时,通道的通道号分别为0、1、2、和3)。本系统中每一个设备(包括摄像头1和视频网关2)或通道都具有唯一的标识信息,确保该设备或通道唯一可定位,如摄像头1的ID和通道号,以及视频网关2的ID,设备除了该唯一的标识信息外还可以根据业务需求添加辅助信息信息,比如该设备的名称、厂家、备注、是否启用、何时安装、安装位置和所属单位等信息。

[0069] 视频网关2还用于接收接入云服务器3下发的指令,并根据该指令对摄像头1进行相应的控制;本实施例中,视频网关2将上级接入云服务器3发过来的统一信令分别转换成不同厂家摄像头1可识别信令,同时将发自摄像头1的信令转换为统一指令给接入云服务器3,即,视频网关1将接入云服务器3下发的指令转换为实际所控制摄像头1可识别的信令,并将摄像头1上报的信令转换为统一指令给接入云服务器3,使接入云服务器3不需要考虑每个摄像头1厂家的差异,从而简化接入云服务器3信令,并降低接入云服务器3的复杂度和资源消耗。

[0070] 接入云服务器3收集和汇总视频网关2上报的视频网关信息和监控视频信息,并对外提供访问上述信息的服务,即,对客户端5和第三方平台4提供访问上述两种信息的服务;本实施例中第三方平台4对所有监控视频进行集中管理,因此接入云服务器3将上述两种信息对接到现有第三方平台4;工作方式为,接入云服务器3和第三方平台4之间采用国标GB28181协议或第三方平台现有其他协议进行对接,客户端5采用私有协议直接访问接入云服务器3,从而实现视频网关信息和监控视频信息的获取。接入云服务器3还收集和汇总用户信息及权限,并将每个用户的用户信息与相对应的监控视频信息进行绑定。

[0071] 接入云服务器3还用于接收客户端5和第三方平台4下发的指令,并根据指令内容将该指令转发至对应的视频网关2,从而使视频网关2接收接入云服务器3下发的指令,并根据该指令对摄像头1进行相应的控制。本实施例中客户端5、接入云服务器3和视频网关2均

通过上述私有协议进行通信。

[0072] 客户端5和第三方平台4均可以向接入云服务器3发送控制、查询以及拉流等指令，且客户端5和第三方平台4用于播放监控视频；其中控制包括对云台控制、启用和禁用录像，以及固件升级等控制，查询包括查询指定摄像头1的录像列表，拉流包括拉取摄像头1的实时音视频码流和录像的音视频码流。由于本发明中具有至少一个接入云服务器3，故在实际下发指令的过程中，客户端5会指定具体的接入云服务器3，第三方平台4能够通过配置下级信息指定具体的接入云服务器3的地址。

[0073] 客户端5由用户直接操作，用于获取用户信息及权限，并对指定摄像头1的监控视频进行管理；用户信息至少包括用户名和密码，本实施例中，用户通过用户名和密码在客户端5上进行登录操作，登录成功后客户端5根据其用户信息获取相对应的权限，即，用户可通过客户端5对指定的摄像头1进行查询、控制以及拉流等操作；用户通过客户端5对监控视频进行控制、查询以及拉流等操作时，客户端5将对应的指令发送至相应的接入云服务器3；客户端5还用于接收码流并将其显示给用户。

[0074] 第三方平台4用于对所有摄像头1采集的监控视频进行集中管理，由于第三方平台4可接入多个接入云服务器3，多个接入云服务器3均可通过第三方平台4已有的安防监控行业标准(国标GB28181)同时将监控视频信息上报给第三方平台4，并受第三方平台4控制(第三方平台4通过国标GB28181向接入云服务器3下发指令)，这样本系统可以构成多级级连架构，即，第三方平台4将多个下级区域的监控视频汇总在一起，在该第三方平台4上进行集中管理。

[0075] 当用户通过客户端5登录时，客户端5将用户名发送至接入云服务器3获取对应的用户信息及权限，此时用户可通过客户端5在接入云服务器3中访问相绑定的监控视频信息，从而使用户通过客户端5对相绑定的摄像头1进行控制、查询以及拉流等操作。由于接入云服务器3将视频网关信息和监控视频信息与第三方平台4对接，即，第三方平台4具有所有视频网关信息和监控视频信息，在实际工作过程中，用户通过第三方平台4根据实际需要选择摄像头1进行控制、查询以及拉流等操作；第三方平台4和客户端5区别点仅在于客户端5仅能管理对应摄像头1(如，某一警察能通过其客户端5查看属于该派出所监管的摄像头1的列表，并从中选择摄像头1进行控制、查询以及拉流等操作)，第三方平台4能管理所有的摄像头1，而第三方平台4和客户端5对摄像头1进行控制、查询以及拉流等操作的工作方式完全相同，故在本说明书中不分别对其具体实现步骤进行详细描述。

[0076] 本发明通过上述系统进行互联网视频网关2安全接入的方法，包括以下步骤：

[0077] 用户通过客户端5或者第三方平台4对监控视频进行控制、查询以及拉流操作：

[0078] 客户端5或者第三方平台4向接入云服务器3发送控制、查询以及拉流等指令，接入云服务器3接收该指令，并将其转发到视频网关2；

[0079] 视频网关2接收由接入云服务器3所发送的指令，视频网关2将收到的上级指令转换为摄像头1通信协议中的对应功能的指令，并将该指令发送给摄像头1，从而依据指令控制摄像头1依据指令进行控制、查询或拉流等操作；最后并接收摄像头1的返回结果，将该操作结果(即，控制和查询指令的操作结果和拉流指令的反馈结果)原路发回；上述摄像头1通讯协议包括厂家SDK(软件开发工具包)、国标和ONVIF(全球性的开放接口标准)等协议。

[0080] 上述控制指令至少包括：目标信息、会话ID和控制类型(即，云台控制、启用录像、

禁用录像或固件升级)及参数,控制参数包括云台控制参数(即,上下左右旋转方向或步进控制等参数)和录像参数(即开或关);

[0081] 查询指令至少包括:目标信息、会话ID和查询类型(即,录像列表,其他均为主动上报)及参数,查询参数包括录像列表参数(即时间段,比如可查询今日01:00-06:00的录像);

[0082] 拉流指令至少包括:目标信息、会话ID和拉流类型(即,实时视频或录像视频)及参数(如,实时视频包含清晰度参数,录像包含录像时间段参数)、音视频码流接收者地址、码流格式和加密类型(即,加密或不加密);

[0083] 关闭拉流指令至少包括:目标信息、会话ID(该会话ID为拉流指令中的会话ID);

[0084] 目标信息为视频网关2的ID、摄像头1的ID以及通道号(即,具体的目标信息),或者目标信息为能够被接入云服务器3根据内部对应关系将其翻译为具体的目标信息的编码(即,等价的目标信息)。

[0085] 当用户通过客户端5或者第三方平台4对指定的摄像头1进行控制、查询和拉流等操作时,客户端5或者第三方平台4根据用户实际操作指定具体的接入云服务器3,并向该接入云服务器3发送控制、查询以及拉流等指令;接入云服务器3接收指令后,通过指令中目标信息的视频网关2的ID将该指令转发至对应的视频网关2;视频网关2接收到指令后,根据指令中目标信息的摄像头1的ID以及通道号将指令转发至指定的摄像头1,从而实现用户通过客户端5对指定的摄像头1进行控制、查询和拉流等操作。

[0086] 注:上述流程为信令交互,其中拉流等操作产生的音视频码流是独立传输的,拉流的信令中会指定音视频码流的接收者地址以及是否需加密,码流将从视频网关2直接发送到指定音视频码流的接收者地址,中间不经过接入云服务器3。

[0087] 上述方法中拉流的具体工作过程如下(仅拉流时摄像头1可采用普通摄像头):

[0088] 1.1、视频网关2收集并及时更新其所在局域网里的摄像头1的监控视频信息,视频网关2将所有的视频网关信息和监控视频信息通过信令通道上报到接入云服务器3。

[0089] 1.2、接入云服务器3接收、保存和更新步骤1.1中视频网关2上报的视频网关信息和监控视频信息,并将所有视频网关信息和监控视频信息进行汇总。接入云服务器3向客户端5和第三方平台4提供访问视频网关信息和监控视频信息的服务;

[0090] 1.3、客户端5或者第三方平台4向接入云服务器3发送拉流指令。

[0091] 用户通过操作客户端5或者第三方平台4获取并观看监控视频时,首先通过客户端5或者第三方平台4设置目标信息、拉流类型(即,实时视频或录像视频)和参数(如,实时视频包含清晰度参数,录像包含录像时间段参数)、码流格式和加密类型(即,加密或不加密)等信息,其中目标信息为客户端5或者第三方平台4通过接入云服务器3汇总的视频网关信息和监控视频信息获得所需监控视频所在的视频网关2的ID、摄像头1的ID以及通道号。客户端5或者第三方平台4根据上述信息生成拉流指令并发送至接入云服务器3;当系统具有多个接入云服务器3时,客户端5下发指令时会指定接入云服务器3,第三方平台4添加和配置下级信息时会指定下级地址(即指定接入云服务器3的地址)。

[0092] 1.4、接入云服务器3接收步骤1.3中的拉流指令,接入云服务器3将该拉流指令转化为私有协议对应功能的指令,并通过信令通道发送给视频网关2。

[0093] 由于每个环节之间的通信协议都不一样,其形式也不一样,但是功能是等价的。在接入云服务器3将拉流指令发送给对应视频网关2时需要对该指令进行转换,具体转换方式

如下：

[0094] 第三方平台4拉流指令采用GB28181协议，该拉流指令中的视频通道信息是通过号码的形式进行传输，接入云服务器3接收上述号码(即，由第三方平台4发送的拉流指令)翻译成具体的视频网关2的ID、摄像头1的ID以及通道信息(接入云服务器3内部维护了这些对应关系)；接入云服务器3将上述所翻译的具体信息转换为接入云服务器3与视频网关2之间定义的私有协议对应功能的指令，并将该指令发送至相对应的视频网关2。

[0095] 注：由于客户端5拉流指令也采用的私有协议，故接入云服务器3无需对客户端5所下发的指令进行翻译。

[0096] 1.5、视频网关2接收步骤1.4中由接入云服务器3所转发的拉流指令，根据拉流指令向对应的摄像头1发送拉流请求，并准备接收摄像头1的码流。摄像头1接收并响应拉流请求。

[0097] 视频网关2将所接收的拉流指令转换成目标摄像头1可识别的信令，发送至目标摄像头1；同理，当摄像头1向视频网关2发送信令时，视频网关2将接收的信令转化为统一信令发送至接入云服务器3。

[0098] 1.6、视频网关2将步骤1.5中摄像头1发送拉流请求的结果(成功或失败)通过信令通道发送给接入云服务器3。

[0099] 当摄像头1发生死机无响应、突然离线、拉流数量太多超出其自身限制等情况，将会导致拉流会失败。拉流失败后视频网关2直接将结果(即，错误信息)发送接入云服务器3，接入云服务器3根据实际情况将该信息进行原路返回，最终返回到对应客户端5或第三方平台4，由客户端5和第三方平台4进行处理(比如提示用户操作失败，显示错误信息等)。

[0100] 1.7、接入云服务器3接收步骤1.6中由视频网关2发送的拉流结果，并将其发送给客户端5或第三方平台4(发出拉流指令的客户端5或第三方平台4)。

[0101] 1.8、摄像头1接收步骤1.5中由视频网关2发送的拉流指令后，不停地将码流发送给视频网关2，视频网关2根据拉流指令中音视频码流的码流格式将码流进行封装，根据是否加密的信息将封装后的码流按照要求加密(或不加密)，之后通过音视频码流接收者地址发送给码流接收者(即，提出拉流指令的第三方平台4或客户端5)。

[0102] 关闭码流的具体工作过程包括依次进行的以下步骤：

[0103] 2.1、客户端5或第三方平台4向接入云服务器3发送关闭码流指令。

[0104] 2.2、接入云服务器3通过信令通道向视频网关2发送关闭码流指令，同时接入云服务器3向客户端5或第三方平台4返回关闭结果(即，成功关闭码流)：

[0105] 注：关闭码流的原则是让下级保证关闭成功，在实际工作过程中如发生关闭失败的情况，如摄像头1死机无响应，此时摄像头1会变成离线状态，离线后视频网关2会自动该摄像头1对应的所有码流关闭，从而实现关闭码流成功。因此在本实施例中接入云服务器3向视频网关2下发关闭码流指令，同时向接入云服务器3向客户端5或第三方平台4返回关闭结果：

[0106] 2.3、视频网关2接收到码流关闭指令，关闭摄像头1的码流，并通过信令通道向接入云服务器3发送确认信息。

[0107] 本发明中控制及查询的工作方式与步骤1.3-1.7拉流的工作方式均相同，可根据实际情况直接对摄像头1进行控制或查询，或在拉流过程中对摄像头1进行控制或查询。

[0108] 控制的具体工作流程：

[0109] 1.3.1、客户端5或者第三方平台4向接入云服务器3发送控制指令。

[0110] 用户通过操作客户端5或者第三方平台4对监控视频进行控制时，首先通过客户端5或者第三方平台4设置目标信息、上述控制指令至少包括：目标信息、会话ID和控制类型(即，云台控制、启用录像、禁用录像或固件升级)及参数(如云台控制参数和录像参数)，其中目标信息为客户端5或者第三方平台4通过接入云服务器3汇总的视频网关信息和监控视频信息获得所需监控视频所在的视频网关2的ID、摄像头1的ID以及通道号。客户端5或者第三方平台4根据上述信息生成控制指令并发送至接入云服务器3。

[0111] 1.4.1、接入云服务器3接收步骤1.3.1中的控制指令，接入云服务器3将该控制指令为私有协议对应功能的指令，并通过信令通道发送给视频网关2。

[0112] 1.5.1、视频网关2接收步骤1.4.1中由接入云服务器3所转发的控制指令，根据控制指令向对应的摄像头1发送控制请求，摄像头1接收并响应该控制请求。

[0113] 1.6.1、视频网关2将步骤1.5.1控制的结果(成功或失败)通过信令通道发送给接入云服务器3。

[0114] 1.7.1、接入云服务器3接收步骤1.6.1中由视频网关2发送的控制结果，接入云服务器3将该信息进行原路返回，最终返回到对应客户端5或第三方平台4，由客户端5和第三方平台4进行处理(比如提示用户启用/禁用成功、启用/禁用失败、升级成功/失败，以及显示错误信息等)。

[0115] 查询的具体工作流程：

[0116] 1.3.2、客户端5或者第三方平台4向接入云服务器3发送查询指令。

[0117] 用户通过操作客户端5或者第三方平台4对监控视频进行查询时，首先通过客户端5或者第三方平台4设置目标信息、上述查询指令至少包括：目标信息、会话ID和查询类型(即，录像列表)和参数(即，录像列表参数)，其中目标信息为客户端5或者第三方平台4通过接入云服务器3汇总的视频网关信息和监控视频信息获得所需监控视频所在的视频网关2的ID、摄像头1的ID以及通道号。客户端5或者第三方平台4根据上述信息生成查询指令并发送至接入云服务器3。

[0118] 1.4.2、接入云服务器3接收步骤1.3.2中的查询指令，接入云服务器3将该查询指令为私有协议对应功能的指令，并通过信令通道发送给视频网关2。

[0119] 1.5.2、视频网关2接收步骤1.4.2中由接入云服务器3所转发的查询指令，根据查询指令向对应的摄像头1发送查询请求，摄像头1接收并响应该查询请求。

[0120] 1.6.2、视频网关2将步骤1.5.2中查询的结果(录像列表信息或查询失败)通过信令通道发送给接入云服务器3。

[0121] 1.7.2、接入云服务器3接收步骤1.6.2中由视频网关2发送的查询结果，接入云服务器3根据将该信息进行原路返回，最终返回到对应客户端5或第三方平台4，由客户端5和第三方平台4进行处理。

[0122] 上述方法中，信令是轻量级的数据传输，不需要耗费很多资源(包括网络、CPU和内存等)；音视频码流是重量级数据传输，比较消耗资源。我们通过将信令与码流分离传输的方式，让接入云服务器3仅传输信令，让码流从视频网关2直接传输到拉流的客户端5或第三方平台4，不经过接入云服务器3，从而将接入云服务器3做到轻量化，实现以很低的成本将

社会面摄像头1接入到已有的视频管理系统(即,第三方平台4)中。另外,通过信令和码流的分离传输以及不同码流的分离传输,还可以根据实际需求,对他们进行不同级别的安全加密,即按需加密,以减少不必要的加密计算,从而降低计算资源需求。

[0123] 最后,还需要注意的是,以上列举的仅是本发明的若干个具体实施例。显然,本发明不限于以上实施例,还可以有许多变形。本领域的普通技术人员能从本发明公开的内容直接导出或联想到的所有变形,均应认为是本发明的保护范围。

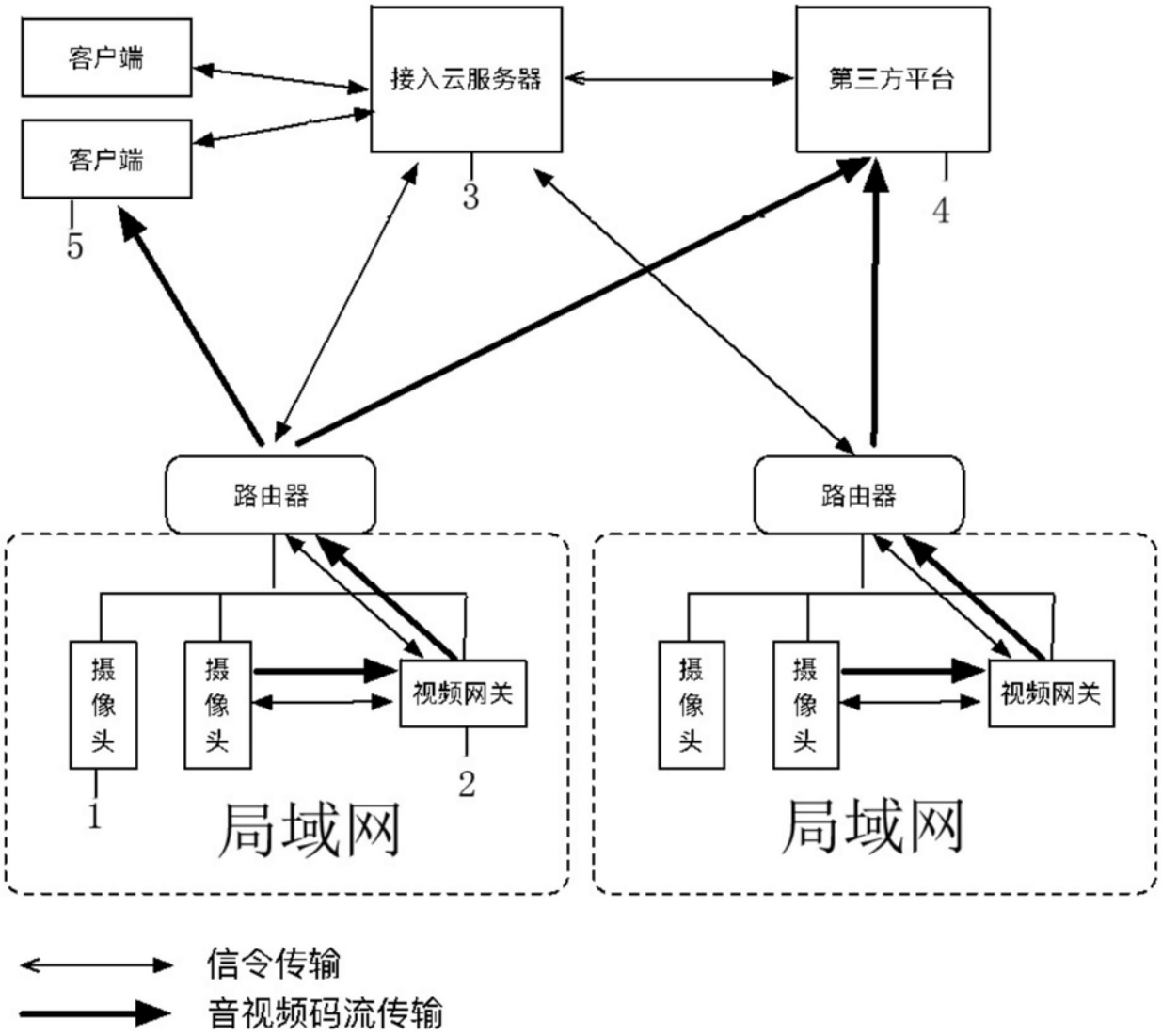

客户端
客户端
接入云服务器
第三方平台
3
4
5
路由器
路由器
摄像头
摄像头
视频网关
2
1
局域网
摄像头
摄像头
视频网关
局域网
信令传输
音视频码流传输

图1