(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110401818 A
(43)申请公布日 2019.11.01

(21)申请号 201910731370.5

(22)申请日 2019.08.08

(71)申请人 北京珞安科技有限责任公司
地址 100083 北京市海淀区中关村东路18号1号楼13层A-1603

(72)发明人 关勇 孔令武 郭浩波 张晓东

(74)专利代理机构 北京慕达星云知识产权代理事务所(特殊普通合伙) 11465
代理人 曹鹏飞

(51)Int.Cl.
H04N 7/18(2006.01)
H04N 21/2347(2011.01)
H04N 21/258(2011.01)
H04N 21/266(2011.01)
H04N 21/4405(2011.01)

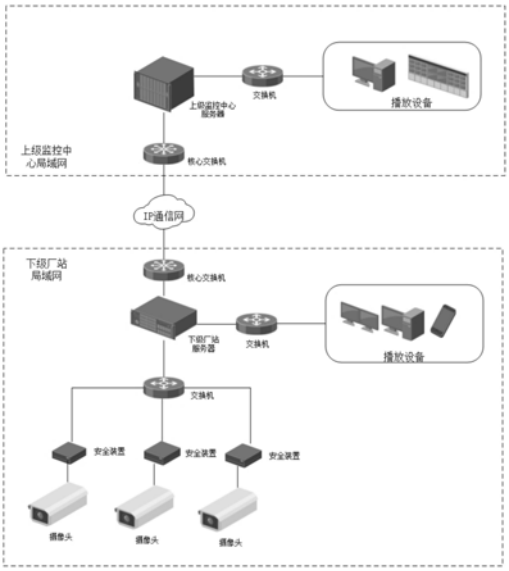
权利要求书2页 说明书8页 附图3页

(54)发明名称

一种电力视频传输的安全通信系统及方法

(57)摘要

本发明公开一种电力视频传输的安全通信系统及方法,通过在监控设备后接入安全设备对监控设备发送的视频数据进行深度解析,对解析出视频中的I帧数据进行加密,将I帧数据进行签名,最后将签名嵌入视频码流中发送到下级厂站服务器。下级厂站局域网内带解密插件的播放设备向下级厂站服务器发送身份认证请求,获取视频数据和密钥进行解密播放,并且保证现场监控的实时性要求。对于上级监控中心和厂站之间远距离的视频数据传输,使用混沌序列生成秘钥对视频数据进行两次置乱和两次扩散加密,对视频数据进行了重加密,提供了视频数据在长距离的远程传输中的安全性保障。



CN 110401818 A

1.一种电力视频传输的安全通信系统,其特征在于,包括通过IP通信网连接的上级监控中心局域网和下级厂站局域网;

其中,所述上级监控中心局域网包括与上级监控中心服务器连接通信的播放设备一;

所述下级厂站局域网包括通过安全装置与下级厂站服务器连接通信的监控设备,以及与所述下级厂站服务器连接通信的播放设备二;所述下级厂站服务器与所述上级监控中心服务器通过IP通信网连接通信。

2.根据权利要求1所述的一种电力视频传输的安全通信方法,其特征在于,所述监控设备设置有N个,包括但不限于摄像头。

3.根据权利要求1所述的一种电力视频传输的安全通信方法,其特征在于,所述安全装置由上级监控中心统一发放并部署在下级厂站的监控设备后端,所述安全装置的数量与所述监控设备的数量相同;每一个安全装置都配置有唯一的身份标识和两个公私钥对,还包括双向认证模块、加密模块和防篡改模块;

其中,所述双向认证模块提供上级监控中心服务器远程查看下级厂站的监控视频时对前端监控设备的安全认证;

所述加密模块用于在所述播放设备二查看监控设备输出的视频数据以及所述播放设备一监控设备录制的视频数据时,对视频数据进行加密,并对密文数据进行防止竞争处理;

所述防篡改模块用于计算得到视频数据的密文摘要,并嵌入至监控设备输出的视频码流中。

4.一种电力视频传输的安全通信方法,其特征在于,包括如下步骤:

安全信道的建立:建立上级监控中心局域网与下级厂站局域网相互通信的安全信道;

视频码流的加密:安全装置对监控设备输出的视频码流中的I帧数据进行安全加密操作;

视频码流的解密:对于发给下级厂站局域网播放设备的加密视频码流,下级厂站局域网的播放设备进行解密操作;对于发给远程的上级监控中心局域网播放设备的加密视频码流,下级厂站服务器对加密视频码流进行视频重加密,并发送至上级监控中心服务器,上级监控中心服务器进行解密操作。

5.根据权利要求4所述的一种电力视频传输的安全通信方法,其特征在于,所述安全信道的建立包括上级监控中心服务器与安全装置进行双向认证,包括如下步骤:

S11、上级监控中心服务器与下级厂站服务器之间通过数字证书完成基于PKI的认证,建立安全的密钥协商信道;

S12、下级厂站服务器使用基于IBC的加密认证方案对调用请求进行加密封装转发给安全装置;

S13、安全装置解密调用请求,发回确认信息至上级监控中心服务器,从而完成安全装置与上级监控中心服务器双向认证,并且建立起上级监控中心服务器-下级厂站服务器、下级厂站服务器-安全装置两条安全信道。

6.根据权利要求4所述的一种电力视频传输的安全通信方法,其特征在于,所述视频码流的加密包括如下步骤:

S21:安全装置对监控设备输出的视频码流进行解析,解析出I帧数据;

S22:安全装置同时对解析出的I帧数据使用密钥key_1进行加密,并运算得到密文摘要,

将密文摘要写回至视频码流中；

S23：安全装置将S22得到的视频码流通过有线/无线传输发送至下级厂站服务器。

7.根据权利要求4所述的一种电力视频传输的安全通信方法，其特征在于，对于发给下级厂站局域网播放设备的加密视频码流，播放设备进行解密操作具体包括如下步骤：

S31：下级厂站局域网的播放设备通过安全身份认证后向下级厂站服务器申请查看监控视频；

S32：下级厂站服务器将密钥key_1通过安全信道发给播放设备，并发送加密后的视频码流给播放设备；

S33：下级厂站局域网的播放设备解析出安全装置构造的类型为SEI的NAL单元和加密的I帧数据，使用公钥Q'_{CID}解密出摘要值B，使用密钥key_1解密出I帧明文，并对I帧明文使用SM3算法进行散列运算后得到摘要B′，对比B和B′，若一致则I帧数据没有被篡改；

S34：完成解密和篡改检验后，将经S33还原后的视频码流进行解码，从而在播放设备显示出监控视频。

8.根据权利要求4所述的一种电力视频传输的安全通信方法，其特征在于，对于发给远程的上级监控中心局域网播放设备的加密视频码流，下级厂站服务器对加密视频码流进行视频重加密的具体过程包括：

在下级厂站服务器上使用混沌序列生成密钥序列对视频码流进行两次置乱和两次扩散加密，对视频数据进行重加密。

9.根据权利要求8所述的一种电力视频传输的安全通信方法，其特征在于，所述置乱和扩散加密方法包括，以NAL单元为处理单元，以3个字节为一组将NAL单元分为若干组，对组内数据通过左移进行比特位置置乱，通过混沌序列的大小排序序列将NAL单元中的分组进行第二次置乱；对置乱后的序列进行正向扩散和反向扩散两次扩散，扩散加密中的同或操作和异或操作的选择由混沌密钥序列形成的参数序列决定。

10.根据权利要求8所述的一种电力视频传输的安全通信方法，其特征在于，上级监控中心服务器进行解密操作包括：

上级主站服务器采用与加密时同样的混沌序列发生器生成解密密钥序列和参数，对接收到的重加密视频码流以同样的方式完成反扩散和反置乱的解密，得到仅加密I帧数据的视频码流；

上级监控中心局域网的播放设备对加密I帧数据的视频码流进行解密，包括，与上级监控中心服务器进行身份认证、获取密钥key_1并解密。

一种电力视频传输的安全通信系统及方法

技术领域

[0001] 本发明涉及视频监控技术领域，特别涉及一种电力视频传输的安全通信系统及方法。

背景技术

[0002] 随着对电力系统安防要求的深入推进，视频监控的需求越来越大，这些视频监控设备对发电厂、变电站等关键场所的实时运行情况进行监视和记录，维护了电力系统的稳定运行。视频监控系统应用包括以下几个层次，第一层次是现场视频监控，由前端摄像机、视频刻录器，视频显示器等组成，支持现场监控和监控视频存储等；第二层次是远程视频监控，由监控前端、控制台以及传输网络组成，支持适应无人值班的变电站、地市级监控中心等远程监控体系。第三层次融入应急指挥系统，实现各级监控视频与相应的应急指挥中心互联，供应急指挥中心直接调用现场视频的图像。

[0003] 然而，作为安防体系的重要构成，视频监控系统本身的安全问题也不容忽视。一方面，高清摄像头等视频采集前端难以管理，设备容易被接入替换，同时存在弱口令等问题；另一方面，监控中心对下级电厂或变电站的远程监控过程中，传输的视频数据采用标准化编码仅采用明文传输，视频数据易被窃取、篡改甚至替换，使得上级不能得到安全可靠的监控视频数据，电网安全受到威胁。甚至，黑客利用视频监控系统的安全隐患，注入恶意代码，以监控系统的后端作为跳板攻击内网内其他系统，带来更大的安全威胁。

[0004] 因此，如何针对视频监控系统的特征和安全威胁设计安全防护机制，提供一种确保视频监控系统的安全性和可靠性的电力视频传输的安全通信系统及方法是本领域技术人员亟待解决的技术问题。

发明内容

[0005] 本发明针对现有电力监控网络安全性低的问题，提供一种电力视频监控安全传输的系统和方法，能够提高视频监控系统的安全性和可靠性。具体方案如下：

[0006] 一种电力视频传输的安全通信系统，包括通过IP通信网连接的上级监控中心局域网和下级厂站局域网；

[0007] 其中，所述上级监控中心局域网包括与上级监控中心服务器连接通信的播放设备一；

[0008] 所述下级厂站局域网包括通过安全装置与下级厂站服务器连接通信的监控设备，以及与所述下级厂站服务器连接通信的播放设备二；所述下级厂站服务器与所述上级监控中心服务器通过IP通信网连接通信。

[0009] 优选的，所述监控设备设置有N个，包括但不限于摄像头。

[0010] 优选的，所述安全装置由上级监控中心统一发放并部署在下级厂站的监控设备后端，所述安全装置的数量与所述监控设备的数量相同；每一个安全装置都配置有唯一的身份标识和两个公私钥对，还包括双向认证模块、加密模块和防篡改模块；

[0011] 其中,所述双向认证模块提供上级监控中心服务器远程查看下级厂站的监控视频时对前端监控设备的安全认证;

[0012] 所述加密模块用于在所述播放设备二查看监控设备输出的视频数据以及所述播放设备一监控设备录制的视频数据时,对视频数据进行加密,并对密文数据进行防止竞争处理;

[0013] 所述防篡改模块用于计算得到视频数据的密文摘要,并嵌入至监控设备输出的视频码流中。

[0014] 本发明还公开了一种电力视频传输的安全通信方法,包括如下步骤:

[0015] 安全信道的建立:建立上级监控中心局域网与下级厂站局域网相互通信的安全信道;

[0016] 视频码流的加密:安全装置对监控设备输出的视频码流中的I帧数据进行安全加密操作;

[0017] 视频码流的解密:对于发给下级厂站局域网播放设备的加密视频码流,下级厂站局域网的播放设备进行解密操作;对于发给远程的上级监控中心局域网播放设备的加密视频码流,下级厂站服务器对加密视频码流进行视频重加密,并发送至上级监控中心服务器,上级监控中心服务器进行解密操作。

[0018] 优选的,所述安全信道的建立包括上级监控中心服务器与安全装置进行双向认证,包括如下步骤:

[0019] S11、上级监控中心服务器与下级厂站服务器之间通过数字证书完成基于PKI的认证,建立安全的密钥协商信道;

[0020] S12、下级厂站服务器使用基于IBC的加密认证方案对调用请求进行加密封装转发给安全装置;

[0021] S13、安全装置解密调用请求,发回确认信息至上级监控中心服务器,从而完成安全装置与上级监控中心服务器双向认证,并且建立起上级监控中心服务器-下级厂站服务器、下级厂站服务器-安全装置两条安全信道。

[0022] 优选的,所述视频码流的加密包括如下步骤:

[0023] S21:安全装置对监控设备输出的视频码流进行解析,解析出I帧数据;

[0024] S22:安全装置同时对解析出的I帧数据使用密钥key_1进行加密,并运算得到密文摘要,将密文摘要写回至视频码流中;

[0025] S23:安全装置将S22得到的视频码流通过有线/无线传输发送至下级厂站服务器。

[0026] 优选的,对于发给下级厂站局域网播放设备的加密视频码流,播放设备进行解密操作具体包括如下步骤:

[0027] S31:下级厂站局域网的播放设备通过安全身份认证后向下级厂站服务器申请查看监控视频;

[0028] S32:下级厂站服务器将密钥key_1通过安全信道发给播放设备,并发送加密后的视频码流给播放设备;

[0029] S33:下级厂站局域网的播放设备解析出安全装置构造的类型为SEI的NAL单元和加密的I帧数据,使用公钥Q'_{CID}解密出摘要值B,使用密钥key_1解密出I帧明文,并对I帧明文使用SM3算法进行散列运算后得到摘要B',对比B和B',若一致则I帧数据没有被篡改;

[0030] S34:完成解密和篡改检验后,将经S33还原后的视频码流进行解码,从而在播放设备显示出监控视频。

[0031] 优选的,对于发给远程的上级监控中心局域网播放设备的加密视频码流,下级厂站服务器对加密视频码流进行视频重加密的具体过程包括:

[0032] 在下级厂站服务器上使用混沌序列生成密钥序列对视频码流进行两次置乱和两次扩散加密,对视频数据进行重加密。

[0033] 优选的,所述置乱和扩散加密方法包括,以NAL单元为处理单元,以3个字节为一组将NAL单元分为若干组,对组内数据通过左移进行比特位置置乱,通过混沌序列的大小排序序列将NAL单元中的分组进行第二次置乱;对置乱后的序列进行正向扩散和反向扩散两次扩散,扩散加密中的同或操作和异或操作的选择由混沌密钥序列形成的参数序列决定。

[0034] 优选的,上级监控中心服务器进行解密操作包括:

[0035] 上级主站服务器采用与加密时同样的混沌序列发生器生成解密密钥序列和参数,对接收到的重加密视频码流以同样的方式完成反扩散和反置乱的解密,得到仅加密I帧数据的视频码流;

[0036] 上级监控中心局域网的播放设备对加密I帧数据的视频码流进行解密,包括,与上级监控中心服务器进行身份认证、获取密钥key_1并解密。

[0037] 本发明相较现有技术具有以下有益效果:

[0038] 1、在不改变现有已部署好的摄像设备的情况下,在摄像头后端部署安全装置,并通过服务器与上级调度中心完成加密认证等任务,不但能满足安全监控的需求,而且能降低成本。

[0039] 2、通过在摄像头后端安装具有认证功能的安全装置,使得上级监控中心在调用监控视频时首先需要完成双向安全认证,从而防止摄像头被替换或者恶意用户访问摄像头,有效的防止了窃取视频或篡改视频的发生。

[0040] 3、根据电力视频监控系统的特点设计不同的加密方案,对于局域网内的视频传输,使用仅加密I帧数据的加密方案,在提供视频数据加密传输的同时保证了现场监控的实时性要求。对于上级监控中心和厂站之间的远距离视频数据传输,使用了混沌序列生成密钥,对视频数据进行两次置乱和两次扩散的加密方案,对视频数据进行了重加密,提供了视频数据在长距离的远程传输中的安全性保障。

附图说明

[0041] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据提供的附图获得其他的附图。

[0042] 图1为本发明电力视频传输安全通信系统的场景结构图;

[0043] 图2为本发明中安全装置对视频码流进行安全处理的实现框图;

[0044] 图3为本发明具体实施方式中涉及的SEI自定义数据字段示意图;

[0045] 图4为本发明在服务器上进行监控视频重加密的实现框图。

具体实施方式

[0046] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0047] 图1展示了本发明所实施的电力视频传输安全通信系统的场景结构图，所包含的实体从视频发送端至接收端分别为监控设备、安全装置、下级厂站服务器、下级厂站播放设备、上级监控中心服务器和上级监控中心播放设备等。其中监控设备、安全装置、下级厂站服务器、下级厂站播放设备同处在下级厂站的局域网内，上级主站服务器和上级厂站播放设备同处在在上级主站局域网内，下级厂站局域网与上级监控中心局域网之间通过IP通信网进行连接。

[0048] 考虑到下级厂站中大量的监控设备(如摄像机)早已部署好，在不改动监控设备硬件情况下，本发明提供一种安全装置，在监控设备后端接入该装置，对外网的监控设备调用请求进行安全认证，对监控设备录制的视频数据进行加密。该安全装置分为双向认证模块，加密模块和防篡改模块。

[0049] 上级监控中心远程查看下级厂站的监控视频时，首先需要与监控设备(如摄像机)进行双向安全认证，双向认证由安全装置和两级服务器共同完成。安全装置由上级监控中心统一发放并部署在下级厂站的监控设备后端，每一个安全装置都拥有唯一的身份标识CID、加密私钥S_{CID}和签名私钥S'_{CID}，上级厂站记录安全装置所连接的摄像设备的编号以及部署位置。上级监控中心的密钥服务器生成系统主密钥MSK和系统公钥PK，对外公开PK，秘密保存MSK，并根据CID秘密生成安全装置的加密私钥S_{CID}和签名私钥S'_{CID}，置入安全装置CID中，加密公钥Q_{CID}和签名公钥Q'_{CID}可由公开的公钥计算函数得到，则安全装置拥有两个公私钥对$\{Q_{CID},S_{CID}\}$和$\{Q'_{CID},S'_{CID}\}$。

[0050] 所述双向安全认证方法包括以下步骤：

[0051] S11：上级监控中心服务器和下级厂站服务器均安装有数字证书，上下级服务器之间通过数字证书完成基于PKI的认证，确认双方身份，建立起安全的密钥协商信道，使得接下来可以在这条安全信道上完成密钥交换、参数协商等方案。

[0052] S12：上级监控中心发送视频调用请求，请求内容包括摄像头对应的安全装置编号CID、时间戳TS和随机数r，通过安全信道发送给下级厂站服务器。下级厂站服务器使用基于IBC的加密认证方案，计算CID的公钥Q_{CID}来封装请求命令，并发送给对应的安全装置。

[0053] S13：安全装置使用私钥S_{CID}对下级厂站服务器发来的请求命令进行解密，解密得到来自上级监控中心的请求命令，并使用私钥S'_{CID}加密随机数r得到E(r)发回给下级厂站服务器，下级厂站服务器通过安全信道将E(r)发回给上级主站服务器，服务器使用公钥Q_{CID}解密E(r)验证是否一致，若一致，则完成安全装置与上级监控中心双向认证，并且建立起了上级监控中心-下级厂站、下级厂站-安全装置两条安全信道。

[0054] 安全信道建立完成后，上级监控中心通过安全信道将加密密钥key_1发送至下级厂站服务器和安全装置中，安全装置使用key_1完成对于监控视频的加密，使用安全装置的私钥S'_{CID}完成签名，特别的，若上级监控中心不参与视频的调用，则密钥key_1和key_2由下级厂站服务器生成。

[0055] 现在市面上的摄像头大多采用H.264或者H.265编码技术，其中H.264占大部分，本发明以H.264编码标准为实施例对发明内容做进一步说明。H.264码流是由一系列网络提取层(NAL)单元组成，通过起始码0x000001或0x00000001进行标识，每个网络提取层单元又由网络提取层头信息(1个字节)和原始字节序列负荷(RBPS)构成，在网络提取层头信息中的第3～7比特的nal_unit_type用于标识RBPS的类型，其中nal_unit_type＝5时标识NALU类型为IDR图像的片，nal_unit_type＝6时标识NALU类型为补充增强信息单元(SEI)。视频码流一般分为I、P、B三种帧，I帧是全帧压缩编码帧，描述了图像背景和运动主体的详情，P、B帧的编码通过I帧进行，我们通过对I帧数据加密以达到监控视频加密的实现。

[0056] 如图2所示，安全装置对摄像头输出的H.264码流中的I帧数据进行安全加密操作，具体为:

[0057] S21:安全装置对摄像头输出的H.264码流进行解析，解析出I帧数据，具体的，安全装置读取H.264码据流至缓冲区1，通过起始标识符0x000001或0x00000001从码流中定位到NAL单元的开始位置，接下来读取nal_unit_type＝5是否成立，成立则这个NAL单元就属于IDR帧(一种特殊的I帧)，如果不是，还要进一步通过哥伦布编码方法计算first_mb_in_slice和slice_type，当slice_type为2、4或7时该NAL单元就属于I帧。确定该NAL单元为I帧后，依次读取接下来的RBPS数据直到检测到下一个NAL单元的起始码，则该NAL单元结束，将RBPS数据放入缓存区2。由于一个GOP的I帧可能被分配在几个连续的NAL单元中，所以需要继续检测下一个NAL单元，直至检测到NAL单元所负载的是其他类型数据后截止。

[0058] S22:安全装置同时对缓存区2中的I帧数据进行加密和摘要，具体为：

[0059] S22-1:安全装置将缓存区2中的I帧数据按字节编号，选择奇数号的字节组成奇队列，选择偶数号的字节组成偶队列，安全装置内嵌国密算法SM4加密芯片，将缓存区2内的I帧数据的奇队列作为输入，通过SM4加密芯片进行加密，其中密钥为通过安全信道接收到的密钥key_1，将加密输出的奇队列密文与偶队列进行异或得到偶队列密文。由此，I帧数据完成加密，对于加密后的I帧数据，还需要检查是否存在以下的四个字节序列，如果存在，则在最后一个字节的前插入防止竞争的字节0x03，具体为：

[0060] 0x000000→0x00000300

[0061] 0x000001→0x00000301

[0062] 0x000002→0x00000302

[0063] 0x000003→0x00000303

[0064] 将最后消除竞争的I帧密文替代I帧明文，写回缓冲区1中的H.264码流中。

[0065] S22-2:安全装置对缓冲区2中的I帧数据进行散列运算得到摘要并使用安全装置的私钥进行签名，通过构造SEI将签名嵌入H.264码流中。具体的，SEI是增强补充信息，是H.264标准的特性之一，它提供了视频码流中加入额外信息的方法，并且它的数据表示区域与视频编码数据独立，在SEI域中填入自定义的数据，从而实现将安全验证信息插入视频码流中而不会影响基于H.264视频通信系统的兼容性，SEI消息的结构如图3所示。

[0066] 构造SEI自定义数据，首先设置SEI payload type＝0x05，标识SEI为用户数据未注册类型。接下来构造uuid部分，uuid长度为16个字节，其中包括填入的CID、TS、随机序列seq和保留字段。对于这些字段，若遇到S22-1中所述的竞争冲突，则填充03防止冲突，剩下的字节则补齐0xff。然后，使用安全装置内置的SM3芯片对缓冲区2中的I帧数据进行散列运

算后得到32个字节的摘要B,并将摘要使用安全装置的私钥S'_{CID}加密得到签名,若签名中遇到S21-1中所述的竞争冲突,则填充0x03防止冲突,并计算签名的长度m字节,将签名填入SEI payload content部分。最后将m-16字节作为SEI负载的长度填入SEI payload size中并补齐RBSP。自此,SEI已经构造好,在SEI前加入NAL的头部信息,其中设置nal_unit_type=6表示构造好的NAL为自定义数据的SEI类型,最后将NAL单元插入缓冲区1中H.246码替换的I帧之前。

[0067] S23:安全装置将缓冲区1中的H.264码流通过有线或者无线传输发送至局域网内的下级厂站服务器。

[0068] 下级厂站服务器对收集到的监控视频进行管理,包括监控视频的本地播放管理、监控视频的本地存储和上级监控中心对监控视频的调用等。

[0069] 对于厂站本地的监控视频查看,本发明提供一种解密插件,安装在监控视频播放设备上。播放设备包括手机、电脑、带解码器的电视墙等。带解密插件的播放设备播放监控视频的具体步骤如下:

[0070] S31:播放设备通过安全身份认证后向服务器申请查看监控视频。

[0071] S32:服务器将密钥key_1通过安全信道发给播放设备,并发送加密后的视频数据给播放设备。

[0072] S33:解密插件解析出安全装置构造的类型为SEI的NAL单元,将该NAL单元提取出来,去掉防止冲突的字节0x03,根据uuid中的CID获取签名公钥Q'_{CID},使用公钥Q'_{CID}对SEI的载荷部分进行解密得到摘要值B。则下一个NAL单元是I帧密文,解密插件根据密钥key_1对I帧密文进行解密得到I帧明文,并对I帧明文使用SM3算法进行散列运算后得到32个字节的摘要B',对比B和B',若一致则I帧数据没有被篡改。

[0073] S34:完成解密和篡改检验后,将还原后的H.264码流进行解码,从而显示出监控视频。

[0074] 虽然安全装置对码流中的I帧数据进行了加密,在保证实时性的前提下保证了视频数据的安全性与完整性,但是由于P帧和B帧中会有帧内预测的宏块,仍存在安全隐患,所以对于发给远程的上级监控中心的视频,下级厂站服务器对H.264码流进行了视频重加密,确保在复杂的网络环境内视频数据的安全传输。

[0075] 在下级厂站服务器上,采用三线程的运行方式,将每个线程分配到不同的CPU上进行并行操作,使得加密速度得到提升。线程1为混沌序列发生器,混沌序列发生器产生的伪随机序列作为重加密的密钥,对监控视频数据进行再次加密,有效的防止不法分子对视频数据的明文和密文暴力破解,增加了视频数据的安全性。混沌序列发生方程为:

[0076]
$$\begin{cases} \dfrac{dx}{dt} = a(y-x) \\ \dfrac{dy}{dt} = (c-a)x - zx - cy \\ \dfrac{dz}{dt} = xy - bz \end{cases}$$

[0077] 下级厂站和上级监控中心服务器之间混沌参数的协商在上文所述的安全信道中进行,并且当通信超过一定时间后,自动进行混沌参数的协商,参数的取值由内部代码自动

实现，不能人为操作。每次参数更新后，方程需要迭代2000次后开始取用，生成的序列X、Y和Z存入共享内存供线程2和线程3的加密取用。

[0078] 下级厂站服务器循环读取出安全装置发来的经过加密的H.264流码，以NAL单元为单位，使用线程1生成的密钥和参数在线程2上执行置乱加密，在线程3上执行扩散加密，加密视频的码流通过网络发送和IP通信网传输。具体的，如图4所示，加密过程如下：

[0079] S41：线程1的混沌序列生成器使用经过协商的混沌参数进行迭代，首先迭代2000次消除初值影响，继续迭代生成三个混沌序列X、Y和Z存入共享内存1中等待线程2和线程3中的加密程序取用。

[0080] S42：线程2循环读取出安全装置发来的经过加密的H.264流码，根据起始标识符0x000001或0x00000001识别出NAL单元，设NAL单元的长度为m字节，如果m不是3的倍数则采用补0的方式扩展字节数，以3个字节为一组将NAL单元分为n组，得到序列$P=\{p_1,p_2,p_3,...,p_n\}$。对NAL单元分组序列P进行比特置乱和分组置乱两次置乱操作，具体为：

[0081] S42-1：从共享内存1中取出长度为n的三组混沌序列，分别为$X=\{x_1,x_2,...,x_n\}$，$Y=\{y_1,y_2,...,y_n\}$和$Z=\{z_1,z_2,...,z_n\}$，其中$X=\{x_1,x_2,...,x_n\}$中的x_i对应NAL单元序列$P=\{p_1,p_2,p_3,...,p_n\}$中的$p_i$。

[0082] S42-2：将序列$X=\{x_1,x_2,...,x_n\}$中的实数值的x_i根据规则转换成整数值a_i，规则如下：

[0083] 取实数值x_i的小数点后8位构成$L_i=0.l_0l_1l_2l_3l_4l_5l_6l_7$，计算$a_i=\left(\left(\bar{L}_i\times10^8\right)\bmod23+1\right)$，使得$1\leqslant a_i\leqslant23$，将$L_i$对应的$p_i$左移$a_i$位进行比特位置置乱得到$p'_i$，置乱后NAL单元为$P'=\{p'_1,p'_2,p'_3,...,p'_n\}$。

[0084] S42-3：将序列X按照从大到小的顺序排序，得到有序序列$X'=\{x'_1,x'_2,...,x'_n\}$，并生成用于记录X'中各元素在原始序列X中位置的新序列$D=\{d_1,d_2,...,d_n\}$，利用序列D对NAL单元序列$P'=\{p'_1,p'_2,p'_3,...,p'_n\}$按分组进行置乱得到$P''=\{p''_1,p''_2,p''_3,...,p''_n\}$，其中$p''_i=p'_{d_i}\left(i=1,2,3,...,n\right)$，将P''存入共享内存2中。

[0085] S43：对共享内存2中经过置乱加密后的NAL单元进行扩散加密，扩散加密包括正向扩散和反向扩散。具体为：

[0086] S43-1：首先对S42-1中的序列Y和序列Z进行预处理。对于序列Y，将实数值y_i表示成浮点数形式，设其有效位为24位，进而生成了24比特的二进制数，进而表示成：$|y_i|=b_1(y_i)b_2(y_i)\cdots b_j(y_i)\cdots b_{24}(y_i)$，其中$b_j(x_i)$是$|y_i|$的第j(1≤j≤24)位，由此得到扩散所需的密钥$K=\{k_1,k_2,...,k_n\}$。求出Y的均值$\bar{Y}$，根据阈值函数$\begin{cases}q_i=0,x_i\leq\bar{Y}\\q_i=1,x_i>\bar{Y}\end{cases}$生成参数控制序列$Q=\{q_1,q_2,q_3,...,q_n\}$。对于序列Z也采用同样的方法构造出24比特的密钥序列$K'=\{k'_1,k'_2,...,k'_n\}$和参数控制序列$Q'=\{q'_1,q'_2,q'_3,...,q'_n\}$。

[0087] S43-2：利用序列$K=\{k_1,k_2,...,k_n\}$对NAL单元置乱序列$P''=\{p''_1,p''_2,p''_3,...,p''_n\}$进行正向扩散，具体为：

[0088] $$p_1^*=\begin{cases}k_1\oplus p''_1,q_1=0\\k_1\odot p''_1,q_1=1\end{cases}$$

[0089] $$p_i^* = \begin{cases} ((p''_{i-1} + k_i) \bmod 256) \oplus p''_i, q_i = 0 \\ ((p''_{i-1} + k_i) \bmod 256) \odot p''_i, q_i = 1 \end{cases}, \quad i = 2,...,n$$

[0090] S43-3：利用序列K′＝{k′1,k′2,...,k′n}对NAL单元的中间密文 $P^* = \{p_1^*, p_2^*, p_3^*, ..., p_n^*\}$ 进行反向扩散，具体为：

[0091] $$p_n^{**} = \begin{cases} k'_n \oplus p_n^*, q'_n = 0 \\ k'_n \odot p_n^*, q'_n = 1 \end{cases}$$

[0092] $$p_i^{**} = \begin{cases} ((p_{i+1}^* + k'_i) \bmod 256) \oplus p_i^*, q'_i = 0 \\ ((p_{i+1}^* + k'_i) \bmod 256) \odot p_i^*, q'_i = 1 \end{cases}, \quad i = 1,...,n-1$$

[0093] S44：在完成置换和扩散加密操作后，对序列 $P^{**} = \{p_1^{**}, p_2^{**}, p_3^{**}, ..., p_n^{**}\}$ 进行扫描，检查是否存在以下的四个字节序列，如果存在，则在最后一个字节的前插入防止竞争的字节0x03，具体为：

[0094] 0x000000→0x00000300

[0095] 0x000001→0x00000301

[0096] 0x000002→0x00000302

[0097] 0x000003→0x00000303

[0098] S4：将NAL单元经过两次置换两次扩散操作后得到的最终密文写回H.264码流中，发送到上级监控中心服务器。

[0099] 在上级主站服务器接端，采用同样的混沌序列发生器生成解密密钥，对接收到的H.264密文以同样的方式完成反扩散和反置乱的解密，解密过程不再详述。解密后的结果就是下级厂站服务器从安全装置接收到的只加密了I帧数据的H.264码流，只不过此时密文数据是在上级监控中心的服务器上，相同的，上级监控中心的播放设备采用上文S31到S34所述的相同方法，通过向服务器进行身份认证、获取密钥key1、解密插件进行解密、播放器解码播放完成监控视频的播放，具体过程不再详述。

[0100] 以上对本发明所提供的一种电力视频传输的安全通信方法进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

[0101] 在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

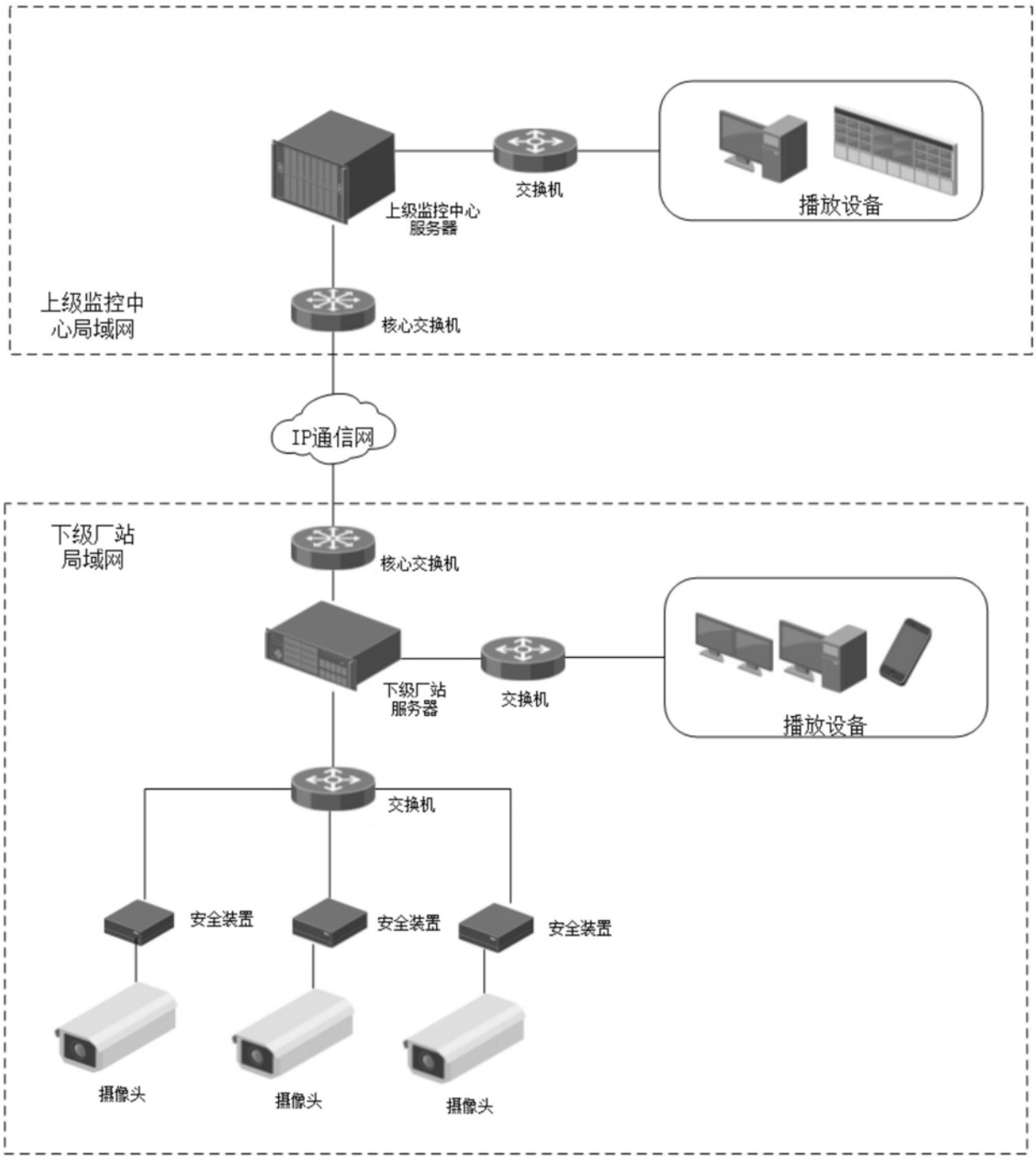

上级监控中心局域网
上级监控中心服务器
交换机
播放设备
核心交换机
IP通信网
下级厂站局域网
核心交换机
下级厂站服务器
交换机
播放设备
交换机
安全装置
安全装置
安全装置
摄像头
摄像头
摄像头

图1

图2

SEI payload type	SEI payload size	uuid	SEI payload content	Rbsp trailing bits

图3

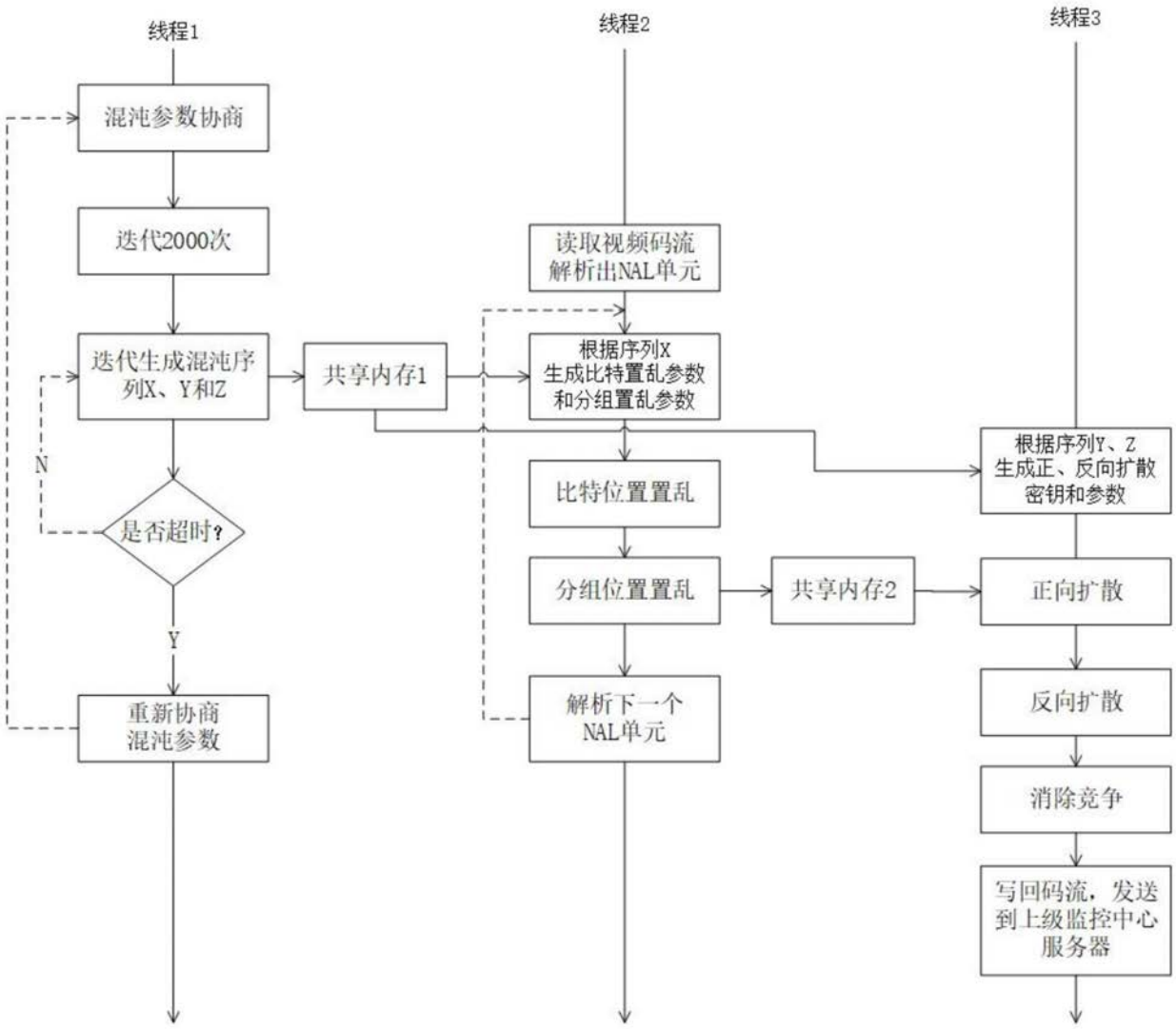

线程1
混沌参数协商
迭代2000次
迭代生成混沌序列X、Y和Z
N
是否超时?
Y
重新协商混沌参数
共享内存1
线程2
读取视频码流解析出NAL单元
根据序列X生成比特置乱参数和分组置乱参数
比特位置置乱
分组位置置乱
解析下一个NAL单元
共享内存2
线程3
根据序列Y、Z生成正、反向扩散密钥和参数
正向扩散
反向扩散
消除竞争
写回码流，发送到上级监控中心服务器

图4