第32卷 第14期 计 算 机 工 程 2006年7月
Vol.32 № 14 Computer Engineering July 2006
·安全技术· 文章编号：1000—3428(2006)14—0138—03 文献标识码：A 中图分类号：TP309+.7

基于H.323协议的视频加密网关的设计

张 镭[1]，张 川[2]，徐正全[3]
(1. 武汉大学计算机学院，武汉 430079；2. 武汉供电公司电力调度中心，武汉 430013；
3. 武汉大学多媒体网络通信工程中心，武汉 430079)

摘 要：提出了一种在视频会议系统中增设视频加密网关（VEG）的保密通信解决方案。视频加密网关能对视频数据进行加密处理，并提供了H.323协议的代理服务功能，使得各H.323终端可通过不可信网络进行安全通信。视频加密网关具有系统独立性，能方便地对现有视频会议系统进行升级。

关键词：视频会议；视频加密；H.323代理服务；PER 编码

Design of Video Encryption Gateway Based on H.323 Protocol

ZHANG Lei[1], ZHANG Chuan[2], XU Zhengquan[3]
(1. Computer School, Wuhan University, Wuhan 430079; 2. Electric Power Dispatch Center, Wuhan Electric Power Supply Company, Wuhan 430013; 3. Multimedia Communication Engineering Center, Wuhan University, Wuhan 430079)

【Abstract】 This paper presents a new security solution for video conference by implementing video encryption gateway(VEG). Video encryption gateway can encrypt video data and provide H.323 protocol proxy function, which make H.323 endpoints communicate securely through untrusted network. Video encryption gateway has system-independent characteristics, so it can update current video conference systems conveniently.

【Key words】 Video conference; Video encryption; H.323 proxy; PER coding

1 概述

随着IP网络的迅速发展，基于分组交换的多媒体通信协议H.323广泛应用于视频会议。由于会议中的视频信息可能涉及到商业机密和国防安全，当视频信息在不可信网络上传输时容易被窃取分析，因此如何实现视频信息在不可信网络(如Internet)上的保密传输是人们十分关心的热点问题。目前市场上的视频会议产品的保密通信方案有以下几种：

(1)使用网络层的IPSec协议对视频会议数据进行加密；

(2)加密用户数据包，如加密视频数据RTP包中，除包头外的所有视频信息；

(3)使用信道加密机，外接于视频会议终端，实现数据流的加密；

(4)设立VPN(虚拟专用网)虚拟通道。

但目前这些保密通信方案存在一些不足：视频会议的视频数据量大，使用IPSec协议、加密用户数据包等方案加密视频信息，运算量较大，容易造成网络延时；视频数据流中的某些标志位被加密，无法识别，影响视频会议的服务质量(QoS)；视频加密功能一般需要终端支持，只能在特定的视频会议系统中实现安全服务；使用信道加密机的成本则较高，不利于广泛应用。

本文提出了一种在视频会议系统中增设视频加密网关(VEG)的保密解决方案。VEG工作在网络的应用层，属于应用级网关。其主要功能为(1)对视频信息数据进行加解密处理。(2)对H.323系列协议信令内容进行解析和修改，使视频会议系统在增设视频加密网关后，各终端间仍能保持正常通信。VEG采用了一种新式的视频加密算法，仅加密视频流中的关键数据，运算量小，对网络延迟少，保密性高，并且不改变视频流中的控制信息；VEG独立于终端设备，可以方便地对现有视频会议系统进行升级，提高其安全性能；制造VEG的成本较低，易于推广应用。

2 视频加密网关的设计方案

VEG在视频会议系统中的工作原理如图1所示。

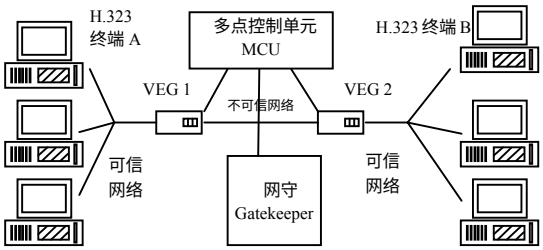

图 1 视频加密网关工作原理

H.323终端均在可信网络中；VEG1和VEG2各有2块网卡分别与可信网络和不可信网络相连。下面以H.323终端的点对点通信方式为例，说明VEG实现视频会议保密通信的工作流程：当H.323终端A希望与H.323终端B进行保密通信时，其首先呼叫VEG1；通过VEG1转接呼叫VEG2；再由它把呼叫消息传递给终端B。同理，终端B的应答消息也通过VEG2和VEG1传递给终端A。按照上述过程，终端A和B在完成呼叫建立(H.225.0/Q.931)和控制消息交互(H.245)后，开始分别向对方发送媒体信息流。终端A的视频数据在VEG1上进行加密后传递给VEG2，再由其解密传递给终端

基金项目：湖北省科技攻关计划基金资助项目(2004AA101C18)；武汉市重点科技攻关计划基金资助项目(20031003021)

作者简介：张 镭(1980—)，男，硕士生，主研方向：多媒体网络通信，图像处理；张 川，硕士、工程师；徐正全，博士、教授、博导

收稿日期：2005-10-15 **E-mail：**leizhang@public.wh.hb.cn

B。反之亦然。由于视频数据是经过加密后在不可信网络上传输的，因此其保密性得到了保证。通过 VEG1 和 VEG2，2 个 H.323 终端在不可信网络上实现了安全通信。当多个 H.323 终端进行视频会议时，其保密通信方式与上述类似，只不过通信的一方由 H.323 终端变成了多点控制单元 MCU；各个 H.323 终端通过 VEG 与 MCU 进行安全通信。

3 视频加密算法的原理和特点

针对视频数据具有层次结构性强、数据量大以及实时传输要求高的特点，VEG 采用了一种新式的视频加密算法。

主要思想为：仅对视频码流中的少部分重要数据进行高强度的加密。因为视频码流中各部分数据的重要性是不同的，某些关键数据(如视频宏块中的直流分量值 DC，交流分量值 AC 和位移矢量 MV 等)虽然数据量比较小，但是对视频码流的解码和视频图像的重建起着至关重要的作用；因此仅对这些少量数据运用 AES、IDEA 等加密算法进行加密，就可以取得对整个视频码流安全加密的效果。本视频加密算法的原理如图 2 所示。

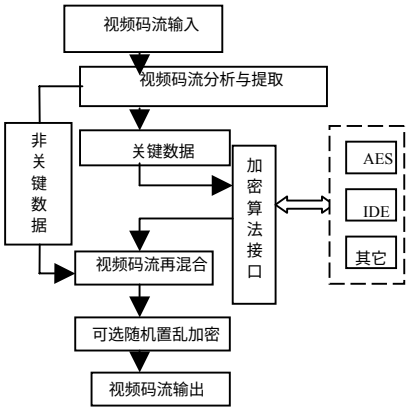

图 2 视频加密算法原理

本视频加密算法具有如下特点：

(1)独立于视频编解码器。

(2)独立于密码学算法，用户可以根据自己的要求选择不同的加密算法，如 DES、AES 或 IDEA 等。

(3)对不同关键数据的选取和组合，可以提供高、中、低 3 个不同的加密级别；用户可根据不同的保密要求和网络带宽进行选择。

(4)计算量小，加密速度快，附加带宽少。

4 视频加密网关的 H.323 协议代理服务

视频会议系统在增设 VEG 后，各终端必须通过其进行通信，即提供了 H.323 协议的代理服务。为了说明本代理服务的原理和实现方法，下面简要介绍一下 H.323 协议的通信过程。

4.1 H.323 协议通信过程

H.323 协议是在基于分组交换的网络上进行多媒体通信的一个框架协议。本标准定义了呼叫信令(Q.931)、逻辑通道控制(H.245)、媒体复用/解复用(H.225.0)、音视频编解码等相关协议。

图 3 为 H.323 终端的点对点方式通信过程，其中 Caller 为呼叫发起方，Callee 为呼叫接收方。通信过程主要分为 3 个阶段：Q.931 呼叫建立过程，H.245 控制信息交互的过程，媒体数据的传输过程。

在整个通信过程中，Callee 的呼叫监听端口号 1 720 是固定的。而其他端口号，如终端的 H.245 监听端口号和 RTP/RTCP 端口号都是在 H.225.0 和 H.245 信令交互过程中动态协商的。由于这些信息包含在 H.225.0 和 H.245 信令中且位置不固定，因此视频加密网关要获取它们，必须解析 H.225.0/Q.931 和 H.245 信令。这些信令是用 ASN.1 的 PER 方式进行编码的。

4.2 PER 编码原理

ISO 组织为解决不同类型终端开放系统之间应用数据信息的交换，推出了抽象语法表符号 1(ASN.1)。H.323 协议中的信令原语(例如 MasterSlaveDetermination/Ack，OpenLogicalChannel/Ack 等)都是用 ASN.1 表示的。国际标准 8825 定义了把 ASN.1 表示的数据结构值编码为适合传输的字节序列的转换语法。分组编码规则(PER)不对数据类型进行编码，只对数据值进行编码，而且采用的是精简编码，效率很高；其前提是通信双方已知传输的数据结构。H.225.0/Q.931 和 H..245 均采用 PER 编码规则，且采用其中的对齐方式(aligned)，即在要求对齐的数据前插“0”，以达到字节边界对齐的目的。与实现 VEG 代理服务密切相关的数据类型编码方法如下：(注：在以下举例中，为对齐需要插入 0 的地方，以(pad)表示。)

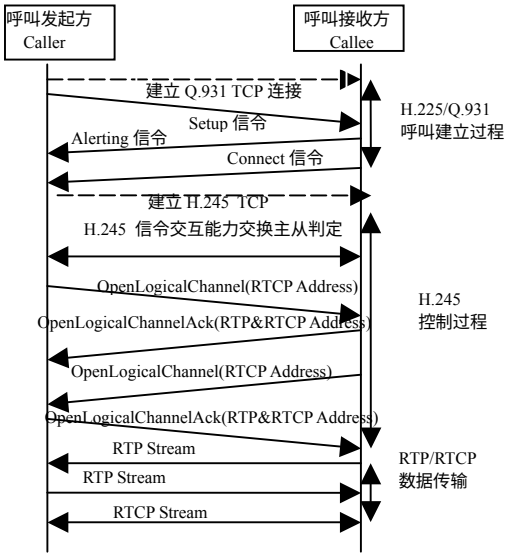

图 3 H.323 协议通信过程

(1)范围受限的整数类型 INTEGER(lb…ub)，其中，lb 为范围的下限，ub 为上限，范围 N=ub-lb+1。

PER 针对 N 的大小不同，采用不同的编码方法，且对整数 n 进行编码时，以(n-lb)的值进行编码。当 N≥255 时，整数编成不需对齐的 1bit～8bits；当 N＝256 时，编成需对齐的 8bits，当 256<N≤65 536 时，编成需对齐的 16bits。例如：当 ASN.1 描述的数据 maximumNestingDepth INTEGER(1…15)的值为 3 时，PER 编码为 0010；g711Alaw64k INTEGER(1…256)的值为 10 时，PER 编码为(pad)00001001；而当 statusDeterminationNumber INTEGER(0…16 777 215)的值为 1 000，PER 编码是 00000010(pad)0010011100010000。

(2)对象标识符类型 OBJECT IDENTIFER。OBJECT IDENTIFER 是一种用层次标识符来描述对象的方法；每一层为一标识符，用一个十进制整数表示。

例如：protocolIdentifier OBJECT IDENTIFIER 可被赋值为{ itu-t(0) recommendation(0) h(8) 245 version (0) 3}。

protocolIdentifier 是由 itu-t、recommendation、h245 和 version 这 4 层标识符来描述，用{0, 0, 8, 245, 0, 3}十进制整

数序列表示。

OBJECT IDENTIFER 编码方法为：length+各层标识符编码，其 length 值按半约束整数类型编码。PER 并不分别对第 1 层和第 2 层的标识符整数值进行编码，而是将 2 层的整数值合并成“40*第 1 层整数值+第 2 层整数值”一个值来进行编码。其他层次标识符整数值被对齐编码为 8bits 串；其中首位是标志位，“1”表示整数值在本比特串没有被编码完，后面接着 8bits 串还是原标识符整数值的编码；而“0”则表示整数值在本比特串编码完毕。

如上例：由于 0*40+0 =0，因此第 1 层，第 2 层的标识符被编码为：0000 0000 ；第 3 层标识符的编码是 0000 1000；245 无法只用一个 8bits 串表示，其编码为 10000001 01110101；剩下的标识符分别被编码为 00000000 和 00000011。因为各层标识符的编码长度总共为 6Bytes，因此 length=0x06。ProtocolIdentifier 最后的编码是 0x06、0x00、0x08、0x81、0x75、0x00 和 0x03。

4.3 VEG 的 H.323 代理服务功能的原理和实现

VEG 的 H.323 代理服务在不同的 H.323 终端通信间起中继的作用。其工作原理如图 4 所示。

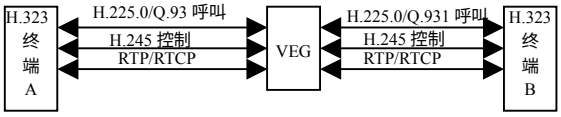

图 4 H.323 代理服务原理

在中继过程中，VEG 不能简单将双方的 H.225.0/Q.931 和 H.245 信令进行直接转发。这是因为 H.225.0/Q.931 和 H.245 在信令消息中含有地址信息和控制信息，如终端的 IP 地址，H.245 端口号以及音视频数据传输及控制(RTP/RTCP)端口号等；VEG 必须深入解析并修改双方信令消息中的相关内容，从而实现代理服务功能。需要解析和修改的 H.225.0/H245 信令数据结构值如表 1 所示。

表 1 需解析和修改的信令数据结构值(ASN.1 描述)

信令消息	数据结构	包含信息
Setup	sourceCallSignalAddress destCallSignalAddress	终端地址
Connect	H245Address	终端地址和 H.245 控制信息传输端口号
OpenLogical Channel	MediaControlChannel、networkAddress	终端地址和 RTCP 端口号
OpenLogical ChannelAck	MediaControlChannel、mediaChannel、networkAddress	终端地址、RTCP 和 RTP 端口号

VEG 的 H.323 代理服务的工作流程如图 5 所示。

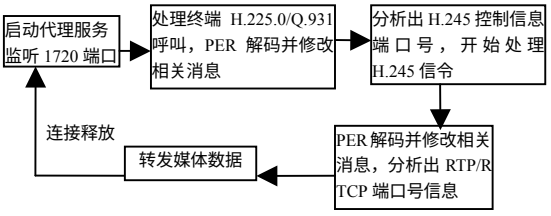

图 5 H.323 代理服务的工作流程

具体步骤如下：

(1)启动 H.323 代理服务，初始化套接字，开始监听 1720 端口。

(2)源端有信令到来，VEG 对其进行 PER 编码解析，判断是否为 Setup 信令；若是，代理服务器修改其中的 sourceCallSignalAddress 和 destCallSignalAddress 地址信息，再连接目的终端，将其转发出去。

(3)VEG 收到目的终端的应答信令后，进行 PER 编码解析，判断是否为 Connect 信令；若是，VEG 修改其中相关地址信息并分析 H.245 端口号，再转发给源端。

(4)初始化与 H.245 信令相关的套接字，开始准备处理。

(5)在处理 H.245 信令过程中，VEG 解析 OpenLogicalChannel/ OpenLogicalChannelAck 信令，修改其中相关的地址信息并转发，分析出 RTP/RTCP 端口号。

(6)初始化媒体数据传输及控制(RTP/RTCP)的套接字，并开始转发媒体数据流。

5 实验结果

本人以 2 块 Philips 公司的 PNX1300 多媒体数据处理器为主核，采用 pSOS 实时操作系统，并配置 16M 的可擦写存储器 FLASH、16M 的同步动态存储器 SDRAM 和两片 RTL8139C(L)网络接口芯片等元件制成了嵌入式视频加密网关。本 VEG 在由 4 台 H.323 终端和一台多点控制器(MCU)组成的多媒体视频会议系统中进行了实验。其测试数据如表 2 所示。(注：测试环境为内部 100M 局域网；图像格式为 CIF；DC、AC、MV 分别代表视频数据的直流分量值、交流分量值和位移矢量。)

表 2 嵌入式视频加密网关的测试数据

视频编码标准	加解密视频路数	算法	加密参数	附加网络延时	附加网络带宽
H.263	2	AES	DC+ AC+MV	<3ms	无
H.263	4	AES	DC+AC+MV	<5ms	无
H.263	2	AES	DC+MV	<3ms	无
MPEG4	2	AES	DC+AC+MV	<3ms	<1%
MPEG4	4	AES	DC+AC+MV	<5ms	<1%
MPEG4	2	AES	DC+MV	<3ms	<1%

6 结论

本文提出了在视频会议系统中增设视频加密网关的安全方案。视频加密网关采用具有自主知识产权的视频加密算法，仅加密视频流中的关键数据，运算量小，对网络延迟少，保密性高，对视频数据进行加解密处理后，能实现视频信息在不可信网络上的保密传输。加密过程中，其深入解析并修改 H.323 信令消息中的相关内容使终端间保持正常通信。由于视频加密网关独立于终端设备，因此能很方便地对现有视频会议系统进行升级。

参考文献

1 ITU-TH.323-2000. Packet-based Multimedia Communications Systems[S]. 2000-06.

2 ITU-TH.225.0-1998. Infrastructure of Audiovisual Services-transmission Multiplexing and Synchronization[S]. 1998-02.

3 ITU-TH.245-1998. Control Protocol for Multimedia Communications[S]. 1998-02.

4 廉士国, 孙金生, 王执铨. 几种典型视频加密算法的性能评价[J]. 中国图像图形学报 2004, 9(4): 483-490.

5 李 伟, 刘树波, 徐正全等. 基于 TM1300 的嵌入式网络视频编码器的设计[J]. 武汉大学学报, 2004, 37(3): 110-113.

6 任延珍, 胡瑞敏, 徐正全. H.323 通信穿越防火墙的问题和解决策略[J]. 计算机工程与应用, 2004, 40(16): 9-13.