复杂涉密网络高清视频会议系统的设计与实现

马绍良[1] 李凤保[2] 路 海[1]
(中国工程物理研究院计算机应用研究所 绵阳 621900)[1]
(中国工程物理研究院电子工程研究所 绵阳 621900)[2]

摘 要 通过对国内外涉密视频会议系统发展现状的调查分析以及对相关音视频编解码技术、边界防护、QoS服务保障、安全策略部署等关键技术的研究,设计了一种基于涉密复杂网络的高清视频会议系统。结合摄像自动跟踪控制和高清视频编解码等技术,完成了在窄带宽、安全管控严格的涉密网环境中的高清视频会议系统的设计与实施,其满足国家涉密网络应用系统的相关接入要求。实践表明,该设计在涉密网络环境视频会议系统建设中具有一定的指导意义。

关键词 高清视频会议,H.264,H.323,涉密网络,安全策略
中图法分类号 TP393,TP309 **文献标识码** A

Design and Implementation of High-definition Video Conference System in Complex and Confidential Network

MA Shao-liang[1] LI Feng-bao[2] LU Hai[1]
(Institute of Computer Application, China Academy of Engineering Physics, Mianyang 621900, China)[1]
(Institute of Electronics Engineering, China Academy of Engineering Physics, Mianyang 621900, China)[2]

Abstract This paper surveyed recent development of classified video conference system, introduced a design method of high-definition video conference in complex and confidential network. Combining typical confidential and secure network infrastructure, described in detail a high-definition video conference's structure, automatic video track and control technology and deployment. Through research on key technologies such as related audio and video encoding, boundary defense, service quality guarantee and security policy configuration, proposed a practical and feasible design method which is successfully applied in projects.

Keywords High-definition video conference, H.264, H.323, Confidential network, Security policy

1 引言

计算机网络与多媒体技术的迅猛发展,特别是H.264视频编解码技术的出现使得图像效果进一步提高,语音技术向高保真、传输向低带宽方向很好地发展,基于IP网络构建高清视频会议系统的技术日臻成熟。高清视频会议可以为用户提供更优的音视频体验,可以被广泛应用于协调指挥、突发事件应急处理、跨域远程会议、培训、教育、医疗、电子商务和协同办公等,极大地提高了工作效率,节约了办公成本,目前已经渗透到各行各业。据统计,目前我国在政府、金融、能源、通信、交通、医疗、教育等重点行业机构中使用视频会议的用户比例达到了65%以上,其中也包括在政府、科研、军工等单位涉密网络环境中的部署应用。

2 涉密视频会议系统国内外现状

在国外,以Esnet(美国能源部能源科学网)为例,它连接美国能源部总部和属下机构,包括SNL(Sandia)、LANL(Los Alamos)、LLNL(Lawrence Livermore)三大核武器实验室。1997年在Esnet限制区网络基础上建成了基于虚拟链路的涉密网SecureNet,它与Esnet开发区、限制区通过防火器、PKI等防护措辞采用逻辑隔离。2000年起在SecureNet上建成连接加州、新墨西哥州、能源部总部的涉密视频会议系统(SecureNet Video Conferencing),并在随后几年再次升级扩充,实现了与国家战争避难所(War Reserve)、三大实验室、各实验场及国内外多家合作机构多达数百个节点的互联互通。

在国内,随着政府机关、军工及科研院所等单位信息化工程的推进,为保障融合通信、多业务交互信息安全,相关单位一般采用自建网络或租用运营商的专用链路,并部署必要的网络安全防护、网络加速等设备组建涉密网络。碍于投资和运营成本,建设的广域网络专线带宽资源一般都很有限(多数小于10M),并需要承载多种业务,因此,基于涉密网络的视频会议系统需重点解决以下需求:提供何种音频/视频协作工具及流媒体传输协议来保证高清视频会议流畅召开;QoS保障各业务带宽合理分配;实施相应的安全分级管理及部署相

本文受中国工程物理研究院级信息化建设项目子项课题资助。
马绍良(1975-),男,高级工程师,主要研究方向为信息规划设计、信息系统集成、网络工程、软件设计、数理统计分析,E-mail:masl@caep.ac.cn;**李凤保**(1970-),男,博士,高级工程师,主要研究方向为网络测试、网络工程、自动化测控等;**路 海**(1971-),男,高级工程师,主要研究方向为信息规划设计、信息系统集成、网络工程等。

关安全策略等来解决涉密高清视频会议的安全及业务保障。

3 涉密网络的基础设施构成

涉密网络基础设施主要由路由器、交换机、加密机、防火墙、网络加速器及防入侵检测系统(IDS)等组成。典型的大集团组织下跨域多分支机构星型涉密网络组网模型结构如图1所示。

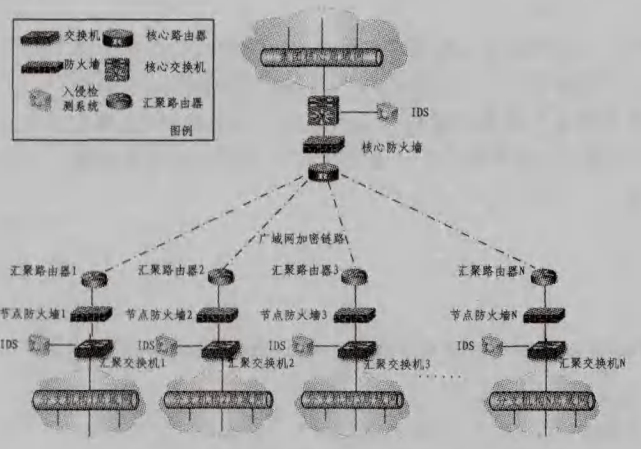

图1 跨域涉密网络组网模型拓扑结构

涉密网络在组网设计时重点考虑对数据的私密性、完整性保护,在保证网络的高可靠性及高可用性的同时,需要有针对性地增强网络的安全性。如图1所示,主干网络采用两台具备高可靠性、高端口密度、高安全性、可管理性的核心路由器实现与各分支机构汇聚路由器的双路链接,全网络实际采用全物理隔离;部署防火墙对业务系统进行安全保护,跨域间的信息访问通过防火墙边界防护,相关数据只能访问指定的TCP/UDP端口,以有效防止来自非授权用户对各种业务系统的DDOS攻击;同时在核心交换设备区部署IDS设备监控黑客攻击;跨域链路主干接入端部署机密机设备,实现重要组播、实时传输数据传输加密。以上手段可以有效实现网络链路层面多重信息的安全保护。

4 高清视频会议系统设计

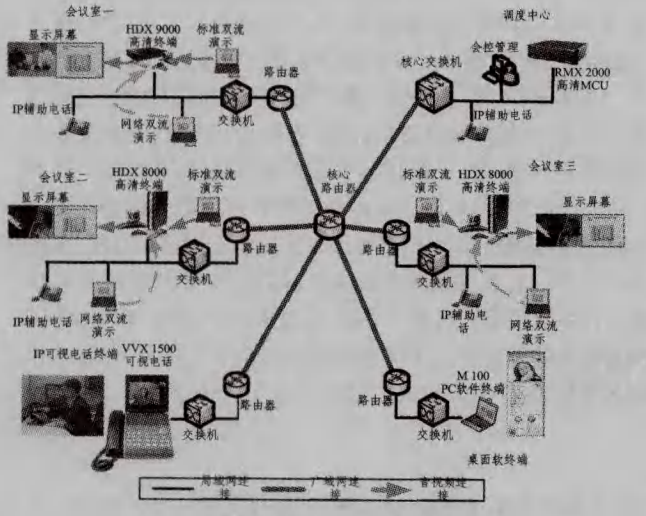

图2 视频会议系统结构示意图

高质量的涉密高清视频会议系统建设需结合业务需求主导、用户便捷式体验以及高安全性"三位一体"的架构开展相关设计。从规划阶段起始就应开展网络现状下最低带宽利用视频设备选型评估测试、便捷式音视频联动的摄像全会场覆盖跟踪、多会议模式保障及多安全域信息保护设计工作。该涉密高清视频会议系统由高清视频总控单元、高清视频会议终端系统、高清辅助显示系统、音控及摄像自动跟踪、传输网络、会议辅助保障等部分组成,如图2所示。

4.1 高清视频总控单元

视频会议总控单元包括会议集中管理工作平台、实时媒体多点会议管控平台MCU(Multi- Control Unit),主要实现视频会议系统配置管理、全网视频设备运行状态的实时监测及会议集中管控调度。通过MCU管控平台,可以灵活实现双方/多方、分屏/全屏、分组、混速等多会议模式下视频会议的召开及集中管控。

4.2 高清视频会议终端系统

各分会场部署的高清视频会议终端系统主要是采集本地视频信号(1080P/720P、XGA、4CIF以及CIF等高、标清视频格式)、音频信号(G.722,G.722.1协议标准下的7kHz,14kHz及G.719协议下22kHz)及PC数据信息流,同时支持将单向或双向的双流(PC+音视频)信号远程传输和本地化还原。

4.3 高清辅助显示系统

在各个会场中提供支持高清1080P的显示设备,分辨率1920(水平)×1080P(垂直),并配置HDMI、DVI等高清数字图像接口实现与会议终端设备的链接及本地化双流信息的显示。

4.4 会议音控及摄像自动跟踪

各会场音控主要包括会议话筒、会议音控主机、调音台、会议音响、功放、回声抑制器等设备;为实现会议话筒与多个高清摄像机的自动跟踪联动控制,配置支持控制协议PELCO-D的摄像控制主机和音控主机连接,当会议发言人发言时,通过会议话筒的预设机位实现摄像头自动跟踪定位,进而实现特写跟踪及双向声音的高保真还原;另外,结合"语音自动定位"和"面部智能识别"的突破性创新技术,设计采用双高清摄像机,辅助声像定位,实现与会者发言摄像机自动跟踪的智能快速响应。

4.5 会议辅助保障

在各个分会场及调度中心内采用IP会议辅助电话提供专业辅助会议保障系统,与视频会议系统实现无缝融合,帮助MCU管控中心与各节点用户之间完成会议预约、调度、运维指导与应急保障等任务。

5 关键技术研究

带宽不足、网络拥塞、网络及音视频设备故障、安全访问控制等因素会导致实时传输的图像出现花屏、马赛克、模糊等现象,传输的声音则会出现断续、失真以及声音与图像不同步等。在一般的网络环境中提供高质量、高安全的音视频图像,需重点研究音视频压缩编码、信息传送安全性、高品质传输保障等关键技术。

5.1 音视频编解码技术

高清视频会议系统传输的是大量数字化视音频信号,需要通过"窄带技术"选择优秀编码性能的编解码协议来降低对

传输信道带宽的占用。国际电信联盟 ITU 制定的编解码协议标准历经十几年由 H. 261/262/263 到最新的 H. 264 几代的发展，目前已经能够在低带宽下获得满意的声音图像质量，为视频会议系统的应用提供了可靠的技术基础。目前主流高清视频终端均支持实时流媒体传输的 H. 264 视频编解码协议及 H. 239 双流协议，但对于双流信息传输和带宽最低利用率方面，各厂商设备还是存在支持带内双流或带外双流传输的差距。本系统设计采用目前最新的 H. 264 High Profile 视频编码技术，因具备极优的网络适应性和抗丢包能力、抗误码机制，结合基于标准双流、远程网络双流以及图像合成演播"叠加双流"的 H. 239 双流数据协议，实现在 H. 323 和 SIP 传输协议下 512kbps 超低带宽 25 帧/秒(NTSC 制下为 30 帧/秒)、1280×720P 动态双流高清远程会议的召开；音频技术方面，G. 719 音频协议标准下支持 22kHz 高保真原声传送，结合回音消除和声音同步技术，使得视频会议能在更低成本网络带宽下提供更高质量的音视频效果。

5.2 H. 323 传输协议下防火墙边界防护技术

ITU-T H. 323 网络传输协议是为现有的分组网络(PBN)提供多媒体通信标准。整体上来说，H. 323 是一个框架性协议，它涉及终端设备、视频、音频和数据传输、通信控制、网络接口方面的内容。在涉密网络视频会议系统建设中，防火墙的边界防护策略的部署是需要重点考虑的内容之一，H. 323 网络协议下流畅传输音视频流通过防火墙需要经过测试来解决网络安全及端口开放的最小化问题。防火墙对特定 IP 地址设备采用 H. 323 协议传输视频流时，需要开放的端口为 1718 或 1719(发向网守的 RAS 消息所用端口)、1720(呼叫信令消息所用端口)，但这些设定并不能完整地解决 H. 323 应用穿越防火墙的问题，主要原因是媒体流需要通过 RTP 协议来传输，传输所需要的源端口和目的端口是动态跳跃的。因此，通过在涉密网络环境下的音视频流分析、H. 323 动态端口检测、修复检测或深度包检测来跟踪端口，切实解决基于 UPD 实时多媒体流组播传输的端口跳跃跟踪并实现防火墙穿越问题，保障端到端最小端口开放，使信息不备截取，满足涉密环境应用。

5.3 QoS 保障技术

涉密广域网链路往往需承载多种信息业务传输，在 IP 组播技术下，通过具有服务质量(QoS)的多媒体组通信保障技术来解决网络中大量多媒体、交互式实时信息流传输的延时、抖动和丢包等问题是十分必要的。

高复杂涉密网络下延时敏感业务包括实施视频服务质量 QoS 保障及相关安全策略部署。通过建立视频网络感知量化评估模型和指标体系，在 QoS 保障性中，采用在窄带宽下建立多业务高负荷环境的动态带宽保障策略，保证涉密视频会议流畅性召开。主要采用的技术包含设置 ToS(服务类型)中 IP 优先顺序和 DiffServ(区分服务)，当视频会议召开时实现相关联的主干接入网络加密机、交换机设备按照内容类别(视频流、文件流)来进行优先级传输转发；采用 PVEC(视频错误隐藏)技术实现智能纠错和视音频丢包补偿，保障数据丢包率减少到 3%或更低；采用前向纠错(FEC)的差错恢复技术，使得接收方可系统地侦测并纠正错误，保障在 5%的丢包率下图像不受影响，在 50%的丢包率下声音可持续；视频会议各个终端节点启用 RSVP(资源预约安装协议)请求路由器或防火墙沿着 IP 连接路径对特定 IP 地址发出的信息流实施动态带宽保障；结合 PacketShaping(信息包整形)、MTU(最大传输单元)自适应、NAT(网络地址转换)等技术手段，充分适应并高效利用网络资源，有效解决网络拥塞和数据丢包，为涉密视频会议召开提供稳定的服务保障。

5.4 安全防护技术

按照信息系统保密标准 BMB22-2007(国家保密标准)中相关的规范，相关涉密视频会议系统安全保护框架应从物理安全、运行安全、信息安全保密、安全保密管理和产品选型与安全服务等方面进行顶层设计，如图 3 所示。

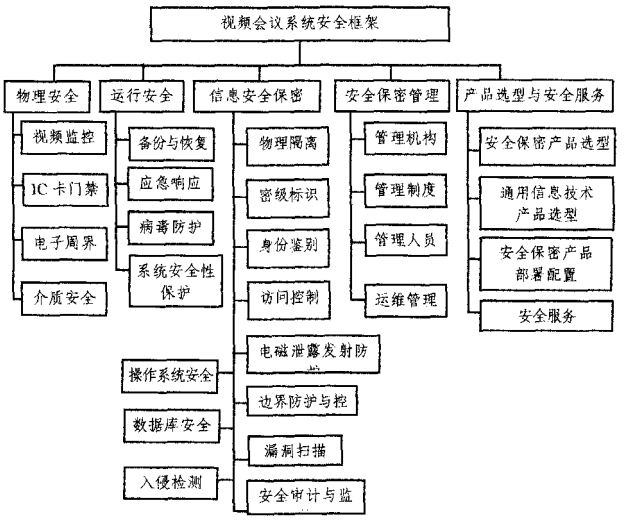

图 3 视频会议系统安全框架

与网络安全息息相关的主要体现在信息安全保密方面，特别是访问控制，它所需要解决的是视频会议系统在网络中不被非法访问和非法利用，是涉及到全网络访问层面的安全保护和防范的重要技术手段。访问控制主要包含入网访问控制、权限控制、目录级安全控制以及属性安全控制等多种手段。在视频会议系统中需要采用的访问控制技术安全防范手段主要包括实施视频联网设备 MAC 地址与 IP 地址绑定，关闭各视频信息接入点交换机空闲端口，防止非法 IP 地址接入及 IP 地址盗用；各节点局域网视频会议系统划分独立 VLAN，与局域网中其它应用系统分属于不同的安全域，不同安全域之间的数据不能直接交换，通过 ACL 访问控制列表实现安全访问控制，有效防止网内其它用户发起的 DDoS 攻击；各个视频会议节点间访问由 MCU 实现统一管控，相应的配置和访问采用一定复杂度的密码保护等。部署有效的访问控制后，配合边界防护与控制、入侵检测、漏洞扫描、安全设计及监控等其它手段一起实现健全的信息安全保密体系。

另外，在物理技防安全、运行安全、相关安全保密管理及产品选型与安全服务方面通过一系列常规性技术手段并制定相关接入规范、管理制度和操作流程实施严格管理，来保障全网视频会议系统的安全性。

结束语 目前，结合摄像跟踪影音控制技术、跨安全域信息防护的涉密网高清视频会议系统，通过建立涉密视频网络感知量化评估模型和指标体系，结合流量测量，提取网络带宽、时延、抖动、丢包率等，并从测量指标入手，提取网络的节点度与节点度分布、节点核数/图核数、聚集系数，建立健全 QoS 服务保障策略等，完成了一套完备的涉密网络视频会议

系统的分析评估体系和应用系统。相关研究成果已经成功应用到国内某大型科研研究机构，并通过了安全保密测评。实践证明，该系统具有了操作简便、运维方便、多模式下视频业务应用灵活及高安全防护等级等特点，对涉密等级和安全要求高的单位在建设高清视频会议系统及解决相关安全防护方面具有一定的借鉴意义。

参 考 文 献

[1] ITU-T Recommendation H. 323-1998, Packet-based multimedia communication systems[S]

[2] SNL. Sandia Lab Accomplishments 2001－2007 [EB/OL]. http://www.sandia.gov/LabNews/labs-accomplish/archive.html

[3] Masullo C. BNL. "Can you See me Now?"[R]. NLIT. 2010

[4] 王颖. H.264 在视频会议系统中的应用[J]. 硅谷，2010(08)

[5] 刘浩，胡栋. 基于 RTP/RTCP 协议的 IP 视频系统设计与实现[J]. 计算机应用研究，2002，19(10)

[6] 王枫博，贾世杰，郭宇明，等. 基于 H.323 网络视频会议系统的关键技术研究[J]. 科技情报开发与经济，2009(05)

[7] 丁久荣. 浅议网络安全与信息安全[J]. 新课程：教育学术，2010，(03)

[8] 陈丽英. 网络视频会议业务的现状与未来[J]. 电信技术，2009(12)

[9] 梅云红. 计算机网络安全隐患与防范策略的探讨[J]. 计算机与信息技术，2007(09)

[10] 国家保密局. BMB20-2007《涉及国家秘密的信息系统分级保护管理规范》[S]. 2007

[11] 国家保密局. BMB22-2007《涉及国家秘密的信息系统分级保护测评指南》[S]. 2007

(上接第 322 页)

于策略模型的安全访问控制。下面给出本文涉及到的安全模型的安全性分析。

本文通过运用基于安全域隔离模型，设计在 MILS 架构下的访问控制机制实现方法，有效解决了几方面的安全问题：

(1)非法的资源访问。每个分区内应用任务的访问请求都要被监控，判断主体请求的操作是否合法，以确保在符合安全策略规则的条件下能够访问被请求的资源，从而保护系统的安全。

(2)身份伪装。访问鉴权的过程中，首先要对请求的主体的身份标识进行验证，验证的方法可以采用密码学中公钥证书的签名验证或者基于对称密钥的 HMAC 验证码，从而保证请求主体身份的合法性，有效防止非法应用任务获取资源导致敏感信息泄漏。

(3)信息泄露。系统通过安全监控器对请求消息的拦截与鉴权，并依据多级安全的强制访问控制策略对不同级别的消息进行隔离，能够有效防止不同安全级别间的消息出现敏感信息的泄露[8]。

(4)隐秘通道。系统通过采用 BLP 模型进行多级安全的强制访问控制，并采用通常禁止不同密级的应用任务之间进行访问请求，从而能够有效避免基于时间和空间的信息流隐蔽通道的存在。而当个别不同安全级别的应用任务间需要跨级访问时，需要通过安全审计中心进行特别记录，并在记录中增加访问操作的发生时间和敏感信息摘要，用于安全管理员的后期审计维护。

5.2 系统性能分析

本文设计的安全操作系统的性能测试环境为：目标机 CPU 是 PPC7447，主频 1GHz，宿主机操作系统为 WinXP，目标机操作系统是安全嵌入式操作系统。采用相同的测试用例，在本方案规定的测试环境中，测试代码优化/非优化、CACHE 打开情况下的操作系统基本性能。完成操作系统下主频 1GHz 的 PPC7447 目标机运行性能测试。方法：将用于测试的计算应用程序移植到操作系统中，在代码优化/非优化情况下进行该项测试。其中包括：常规运算型用例，其赋值语句占 55%，控制语句占 32%，过程/函数调用占 15%；双精度浮点运算的用例；大计算量的控制率计算用例。经过在测试环境中运行，增加安全访问控制机制的安全操作系统的性能下降约 10%左右。

结束语 在安全嵌入式系统中，操作系统不仅作为整个系统的功能性平台，还作为系统的安全平台对整个系统的安全性产生影响。本文对基于微内核的安全嵌入式系统模型进行研究，不仅能够保证各分区的隔离安全性、信息流的可控性，还能基于微内核的特点构建多重独立安全体系，进一步增强系统的安全性。基于微内核系统由于结构简单，在具体实现时能够保证嵌入式系统的实时性能，因此能较好地解决安全嵌入式系统设计中安全与性能之间的平衡问题。

参 考 文 献

[1] Alves-Foss J, Taylor C, Oman P. A Multi-layered Approach to Security in High Assurance Systems[C]// Proceedings of the Hawaii International Conference on System Sciences. January 2004

[2] Rushby J M. The Design and Verification of Secure Systems[J]. ACM Operating Systems Review, 1981, 15(5): 12-21

[3] Rushby J M. Proof of Separability: A Verification Technique for a Class of Security Kernels[J]. Computer Science, 1982, 137: 352-367

[4] Boettcher C, Rushby J. The MILS component integration approach to secure information sharing[C]// the 27th Digital Avionics Systems Conference. October 2008: 26-30

[5] 黄玉琪，张建平，马利. 基于三权分立原则的安全操作系统结构设计[J]. 计算机应用与软件，2010，27(8)：159-162

[6] 韩立毛，赵跃华，马祥顺. 嵌入式操作系统的内核安全研究与设计[J]. 计算机工程与设计，2010，31(14)：3233-3236

[7] Bell D, LaPadula L. Secure Computer Systems: a Mathematical Model[R]. Technical Report MTR-2547 (Vol. II). MITRE Corp., Bedford, MA, May 1973

[8] Brien R O, Rogers C. Developing application on LOCK[C]// Proceedings of Symposium Research in Security and Privacy. Oct 1991: 206-214