

一种新型的应急卫星通信 VPN 技术研究

周 前

(南京邮电大学 通信与信息工程学院 江苏 南京 210000)

摘 要: 在处理我国公共安全突发状况和自然灾害时,利用卫星通信系统进行通信十分重要。一个好的卫星通信系统可以安全、快速、经济地完成通信任务,同时可以联动力量、指挥中心、决策支撑系统和现有移动、固定通讯网络构成统一的应急联动指挥系统。传统 VPN 技术一般应用于企业网在因特网等网络上的延伸,提供高性能、低价位的网络接入,在此基础上对其进行改进优化。通过向中国电信卫星通信公司租用一条数据专线,各终端通过大 S 卫星联入互联网,各应急平台和应急指挥中心通过 VPN 网关组成一个完整的应急系统,使用 UDP 协议与卫星传输数据,并用 IPSec 协议保护数据安全,构成在大 S 卫星通信网上的逻辑通信专网,使得各集团、各部门、各用户的卫星通信终端之间组成自主管理的通信专网。由于卫星通信网的独特优势,将使这样的通信专网具有非常好的应急通信鲁棒性。

关键词: 应急卫星通信; VPN 技术; S 卫星; IPSec 协议; UDP 协议

中图分类号: TP302

文献标识码: A

文章编号: 1673-629X(2018)02-0163-04

doi: 10.3969/j.issn.1673-629X.2018.02.035

Research on a New Emergency Satellite Communication VPN Technology

ZHOU Qian

(School of Telecommunications and Information Engineering, Nanjing University of
Posts and Telecommunications, Nanjing 210000, China)

Abstract: It is very important to use the satellite communication system to communicate in the process of dealing with public safety emergencies and natural disasters. An excellent satellite communication system can complete the communication task safely, quickly and economically. At the same time, it can join forces, command center, decision support system and the existing mobile, fixed communication network to constitute a unified emergency linkage command system. Traditional VPN technology is generally applied to the enterprise network in the Internet and other networks on the extension, to provide high-performance, low-cost network access, with its improvement and optimization on the basis. Through the China Telecom Satellite Communications Corporation to rent a data line, each terminal accesses into the Internet through the large S satellite, and the emergency platform and emergency command center form a complete emergency system through the VPN gateway. The use of UDP protocol and satellite for data transmission, and IPSec protocol to protect data security, a logical communication network is constituted on a large S satellite communication network, which makes the satellite communication terminals from the groups or departments or users composed of self-management of the communications network. Due to the unique advantages of the satellite communication network, such a communication network will have unprecedented emergency communication robustness.

Key words: emergency satellite communications; VPN technology; S satellite; IPSec; UDP

0 引 言

卫星通信广泛应用于应急救援工作^[1],但是目前每个应急救援卫星通信系统相对独立运行,虽然在紧急事件发生后,可以相互支援^[2],但由于没有应急卫星通信联动指挥调度系统的支持,同时也没有完善的联动机制,使得统一的指挥协调和资源整合成为空谈^[3]。

VPN 指在公有网络中通过一个私有通道来创建一个安全的私有连接,将远程用户、分支机构、职能部门等核心网络连接起来,形成一个扩展的核心私有网络^[4]。然而,该 VPN 系统方案都是基于 TCP/IP 协议进行数据传输,在卫星通信网络高延时、高误码率的环境下,此 VPN 系统基本无法使用。基于传统 VPN 的 VOIP 业务,在卫星通信网络环境下的使用效果也非常差^[5]。

为了解决上述问题,需开发出一款在 S 卫星通信环境下,可以正常提供数据传输,进行业务处理的

收稿日期: 2017-03-06

修回日期: 2017-07-13

网络出版时间: 2017-11-15

基金项目: 国家自然科学基金(61271234)

作者简介: 周 前(1992-),男,硕士研究生,研究方向为卫星通信技术。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20171115.1436.048.html>

VPN 系统,将网络中的 TCP 协议数据转为 UDP 协议数据,在卫星通信网络中传输,提高传输效率,并在 VPN 接入网关系统中进行数据加密、封装处理。该系统的特点是安全、保密、经济和自主管理。

1 VPN 技术

虚拟专用网络(VPN)属于远程访问技术,利用公用网络架设专用网络,进行加密通讯,VPN 网关通过对数据包的加密和数据包目标地址的转换实现远程访问^[6]。

VPN 被定义为通过一个公用网络(通常是因特网)建立一个临时的、安全的连接,是一条穿过混乱的公用网络的安全、稳定的隧道^[7]。

针对不同的用户,VPN 有三种解决方案:远程访问虚拟网应用于客户端到网关,企业内部虚拟网应用于网关到网关,企业扩展虚拟网应用于企业与合作伙伴企业网构成 Extranet^[8]。

SSL VPN 是以 HTTPS 为基础的 VPN 技术,工作在传输层和应用层之间,充分利用 SSL 协议提供的基于证书的身份认证、数据加密和消息完整性验证机制,可以为应用层之间的通信建立安全连接。SSL VPN 广泛应用于基于 Web 的远程安全接入,为用户远程访问公司内部网络提供安全保障^[9]。

IPSec VPN 是基于 IPSec 协议的 VPN 技术,由 IPSec 协议提供隧道安全保障。IPSec 是一种端到端的确保基于 IP 通讯的数据安全性机制。

隧道技术是 VPN 的基本技术,类似于点到点连接技术。它的基本过程就是在数据进入源 VPN 网关后,将数据“封装”后通过公网传输到目的 VPN 网关后再对数据“解封装”。“封装/解封装”过程本身就可以为

原始报文提供安全防护功能,所以被封装的数据在互联网上传递时所经过的逻辑路径被称为“隧道”^[10]。VPN 的隧道协议主要有三种: PPTP、L2TP 和 IP-Sec^[11]。

身份认证技术主要用于移动办公的用户远程接入的情况,通过对用户的身份进行认证,确保接入内部网络的用户是合法用户,不同的 VPN 技术能提供的用户身份认证方法不同, L2TP 依赖 PPP 提供的认证。认证通过以后再给用户分配内部的 IP 地址,通过此 IP 地址对用户进行授权和管理^[12]。

加密技术就是把能读懂的报文变成无法读懂的报文。加密对象有数据报文和协议报文之分,能够实现协议报文和数据报文都加密的协议安全系数更高。SSL VPN 支持数据报文和协议报文加密。SSL VPN 采用公钥体制进行加密。公钥体制加密跟对称密钥加密的差别在于加密和解密所用的密钥是不同的^[13]。

数据验证技术就是对收到的报文进行验货。采用一种称为“摘要”的技术。“摘要”技术主要采用 HASH 函数将一段长的报文通过函数变换,映射为一段短的报文。在收发两端都对报文进行验证,只有摘要一致的报文才被认可^[14]。L2TP 本身不提供数据验证技术,但可结合 IPSec 协议一起使用,使用 IPSec 的数据验证技术。在 IPSec 中验证和加密通常一起使用,对加密后的报文 HMAC 生成摘要,提供数据的安全性。HMAC 利用 Hash 函数,以一个对称密钥和一个数据包作为输入,生成一个固定长度的输出,这个输出被称为完整性校验值 ICV(integrity check value)。由于在 Hash 运算时包含了密钥,即使用户同时修改了数据和摘要也可以被识别出来^[15]。表 1 为常用安全技术和使用场景。

表 1 常用安全技术和使用场景

	GRE	L2TP	IPSec	SSL VPN
保护范围	IP 层及以上数据	IP 层及以上数据	IP 层及以上数据	应用层特定数据
适合场景	Intranet VPN	Access VPN, Extranet VPN	Intranet VPN, Access VPN	Access VPN
身份验证	不支持	支持,基于 PPP 的 Chap、PAP、EAP 认证	支持,采用 IP 或 ID+口令或证书进行数据源认证; IKEv2 拨号方式采用 EAP 认证进行用户身份认证	支持,用户名+口令+证书对服务器进行认证,也可以进行双向认证
加密技术	不支持	不支持	支持	支持
数据验证	支持	不支持	支持	支持
如何使用	GRE over IPSec	L2TP over IPSec	单独使用 IPSec,或通过 IPSec 保护 GRE、L2TP	SSL VPN

2 星通信 VPN 系统

该 VPN 系统首先向中国电信卫星通信公司租用一条数据专线,系统通过这条数据专线接入 Internet

网,集团内部的大 S 卫星通信终端用户首先通过卫星通信网接入 Internet,然后通过安装在卫星通信终端的拨号软件与该系统 VPN 网关进行 L2TP+IPSec VPN 连接,接入 VPN 服务器后的集团用户之间通过软交换

技术实现语音通信,同时实现包括短信、Email、文字聊天、图片及视频收发等综合业务。

如图1所示,各种卫星通信终端,如卫星手持终端、便携式卫星地球站以及车载、船载等终端,通过大S卫星通信网联入互联网,大S卫星通过主站与VPN

网关与各个应急平台以及应急指挥中心进行通信。该系统利用卫星VPN技术,完全满足各级联动单位平时的集群调度需求和普通语音需求,并且具有极高的可靠性。

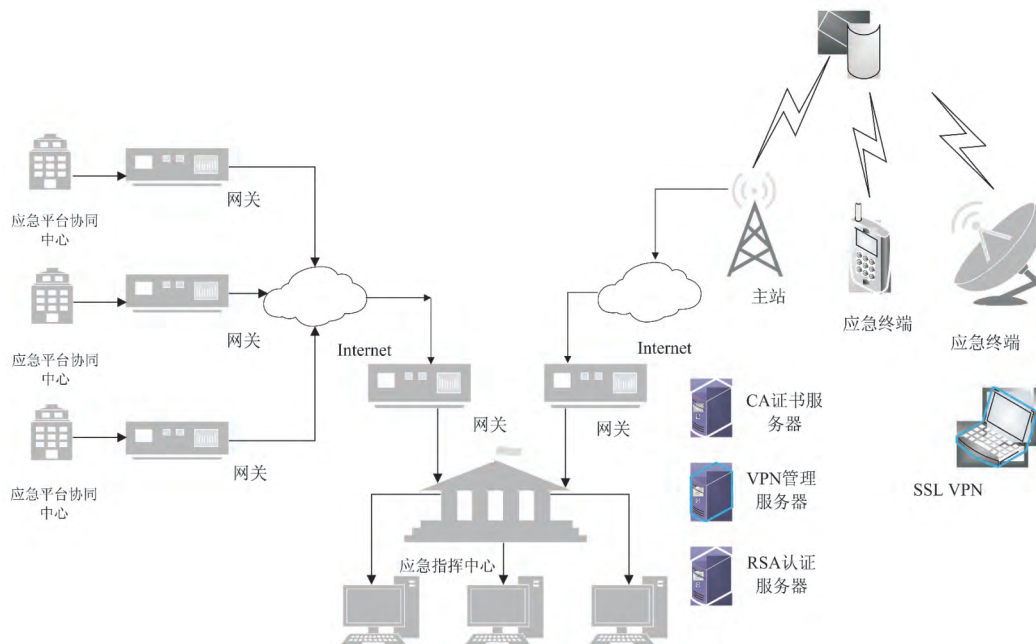


图1 卫星通信 VPN 网络链路拓扑图

2.1 大S卫星通信网简介

大S通信卫星有3个关口站分别设在北京、广州和成都,关口站与地面交换网络相连接,使用C频段卫星通信链路,与卫星通信,同时,该卫星也使用S频段卫星通信链路,109个波束覆盖全国,可与卫星手持终端、便携式卫星地球站以及车载、船载、机载卫星地球站进行通信。

2.2 系统组成

系统由终端APP子系统、VPN接入安全网关子系统、认证管理子系统、VPN管理子系统四个部分组成。

终端APP子系统负责终端VPN拨入功能,在客户端上安装APP客户端软件。图2为卫星通信客户端子系统。用户通过卫星通信网接入到Internet,就可以通过APP拨号与VPN网关之间建立IPSec隧道。

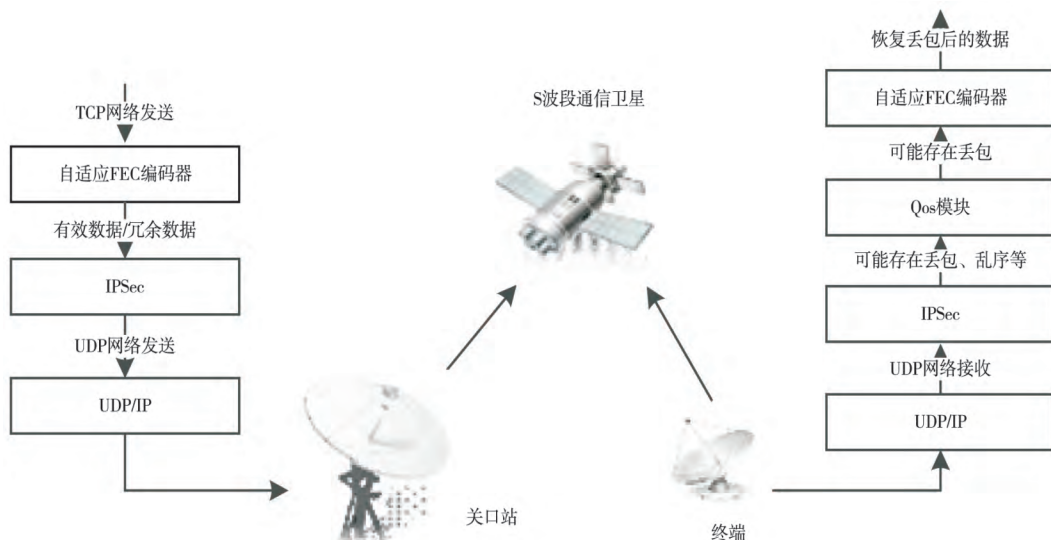


图2 卫星通信客户端子系统

APP拨号的安全策略包括IPSec、IKE和NAT等,强化VPN系统的安全性。IPSec使特定的通信方之间

在IP层通过加密与数据源验证等方式,来保证数据包在网络上传输时的私有性、完整性、真实性。

APP 拨号软件可以通过 PPP 协商向 VPN 申请 IP 地址。由于此 IP 地址的分配是由 VPN 隧道对端分配的,其保密性更高,被攻击的可能性也更小。同时 APP 支持 IPSec/IKE 加密。IPSec 为 IP 协议栈提供在 IP 层实施的一系列安全服务,为 IP 及其上层提供保护。拨号软件通过支持 IPSec 提供数据加密、数据完整性验证、数据身份验证,以及防重发功能。APP 支持 IPSec 隧道模式和传输模式。拨号连接过程中可以选择“静态密码”、“RSA 动态口令卡”、“SecKey USB Token”等方式,可以更安全地验证用户的身份。

VPN 接入安全网关系统是系统的核心部件,可采用 HA 双机热备份方案或采用两台安全网关产品运行 VRRP 协议方式实现主从热备份。安全网关作为局端核心设备提供安全 VPN 接入功能,通过防火墙对原地址区分用户进行 ACL 访问权限控制。

认证管理子系统通过 RADIUS Proxy 功能与 RSA ACE Server 配合实现一次性密码认证功能,或采用 Quidway SecKey USB 卡方式进行身份认证。

SecKey 可以减少拨号用户身份信息被盗用的风险,为拨号用户提供身份认证信息的安全存储、基于硬件的双因素用户认证、客户端配置“即插即用”以及 license 管理等功能。

使用双因素方式提供用户身份验证安全性,同时通过减少拨号的配置管理工作来提高用户的工作效率,优化远程访问 VPN 用户的部署工作,经济有效地管理用户,减少维护成本。

VPN 管理子系统提供业务信道的分配与交换和对 VPN 进行监控管理。该子系统以用户实际配置任务为驱动、提供 IPSec VPN 业务配置向导,指导用户进行 IPSec VPN 设备配置,构建 VPN 网络。

3 结束语

应急联动中的各个部门,在 VPN 系统提供多层次、立体化的指挥系统下,不仅可以不受干扰地工作在各部门的专网中,还可以在级别更高、权利更大的部门的统一管理和指挥调度下,实现跨部门联动。卫星通信的独特优势使这样的通信专网具有前所未有的应急

通信鲁棒性,利用卫星通信 VPN 技术,建立联动系统涵盖集群调度及普通语音功能,完全满足合计联动单位平时的集群调度需求和普通语音需求。

参考文献:

- [1] 王海涛.应急通信发展现状和技术手段分析[J].电力系统通信,2011,32(2):1-6.
- [2] 李文峰.现代应急通信技术[M].西安:西安电子科技大学出版社,2007.
- [3] SIERGIEJCZYK M.Availability of the motorway emergency communications[J].Journal of Konbin,2008,5(2):291-306.
- [4] 胡鼎.SSL VPN 身份认证的研究[D].合肥:安徽大学,2013.
- [5] 邢玉领,谢鹰,张涛.应急通信发展策略研究[J].邮电设计技术,2009(9):33-36.
- [6] 杨铎.基于 MPLS VPN 技术的组网的设计与实现[D].长春:吉林大学,2014.
- [7] 刘洪强.基于 SSL 协议的 VPN 技术研究与实现[D].济南:山东大学,2008.
- [8] 程思,程家兴.VPN 中的隧道技术研究[J].计算机技术与发展,2010,20(2):156-159.
- [9] 蒋东毅,吕述望,罗晓广.VPN 的关键技术分析[J].计算机工程与应用,2003,39(15):173-177.
- [10] 孙培松.VPN 发展趋势及竞争策略研究[D].北京:北京邮电大学,2008.
- [11] 王柱.基于 IP 城域网的 MPLS VPN 规划与性能分析[D].天津:天津大学,2006.
- [12] 倪剑虹,吕光宏.基于 VPN 的不同实现方式的技术研究[J].计算机应用研究,2005,22(7):257-260.
- [13] PERTA V C, BARBERA M V, TYSON G, et al. A glance through the VPN looking glass: IPv6 leakage and DNS hijacking in commercial VPN clients[C]//15th privacy enhancing symposium. [s.l.]: [s.n.], 2015.
- [14] FAN Yaqin, LI Chi, SUN Chao. Based on combination of L2TP and IPSec VPN security technology research[J]. Journal of Networks, 2012, 7(1): 141-148.
- [15] GAURAVARAM P, HIROSE S, ANNADURAI S. An update on the analysis and design of NMAC and HMAC functions[J]. International Journal of Network Security, 2008, 7(1): 49-60.