一种基于硬件虚拟化地面测控安全防护技术

文◆无锡航天江南数据系统科技有限公司 朱兆国 尹 山 王晶晶
京济通信科技（无锡）有限公司 蔡天蓉

引言

为解决传统地面测控密码设备数量众多、各星密码服务独立配置隔离性差、星座测控密码资源管理能力弱等问题，采用硬件虚拟化以及虚拟测控服务能力轻量级封装和编排技术，虚拟测控服务以云化应用方式运行于独立、安全隔离的虚拟密码机，调用独立的硬件虚拟化 VF 虚拟密码功能单元实现测控业务机密性、完整性保护，达到服务云化应用、硬件级隔离和星座测控密码资源独立配置管理的能力。

基于此，本文提出一种基于硬件虚拟化地面测控安全防护技术，在成熟的云平台基础上，利用硬件级虚拟化[1]、测控密码服务能力的轻量级封装和编排技术，解决传统地面测控密码设备数量众多、各星密码服务独立配置隔离性差、星座测控密码资源管理能力弱等问题，为卫星通信网络大规模卫星测控安全提供技术支撑。

1 国内外研究现状

1.1 地面测控安全现状

卫星测控信息安全属于专用领域，基本无国外的研究信息。目前，在国内卫星测控信息安全领域，2020 年前以多合一设备形式实现地面测控星地链路数据安全防护，即一台设备实现几颗卫星的测控数据加解密处理。2021 年开始，国内提出百合一设备，即一台设备实现上百颗卫星的测控数据加解密处理。实现机制主要存在以下问题。

（1）未采用虚拟化技术，在同一硬件和操作系统内，软件直接调度实现多个任务的加解密处理。（2）设备所承载的所有卫星的服务、服务运行资源和密码资源未做相互隔离。（3）以软件动态库或专用算法卡形式提供密码运算服务，未做算法运算隔离。

1.2 硬件虚拟化技术现状

硬件虚拟化最早是 20 世纪 70 年代 IBM 首先提出并使用，到 21 世纪初随着计算机技术和数据中心的飞速发展，Intel 和 AMD 分别推出了 Intel-VT 和 AMD-V 技术，为虚拟化提供了额外的硬件支持。

硬件虚拟化是一种对计算机或操作系统的虚拟。在硬件虚拟化层面，现代虚拟化技术通常是全虚拟和半虚拟的混合体。常见的虚拟化技术如 VMWare、Xen 和 KVM，能够同时支持全虚拟化和半虚拟化。硬件虚拟化方式提供的虚拟机，独立运行着一个完整的操作系统，在同一台物理宿主机上存在大量相同或者相似的进程和内存页，导致较大的性能损耗。因此，硬件虚拟化也被称为重量级虚拟化，在同一宿主机上能够同时运行的虚拟机数量有限。

硬件物理平台本身提供了对特殊指令的截获和重定向支持。支持虚拟化的硬件，是一些基于硬件实现软件虚拟化技术[2]的关键。在基于硬件实现软件虚拟化的技术中，硬件是实现虚拟化的基础，硬件（主要是 CPU）会为虚拟化软件提供支持，实现硬件资源的虚拟化。

目前，硬件虚拟化技术广泛应用于数据中心、云平台等大数据处理高并发应用场景，在金融、电信、政务、电子商务等行业得到广泛推广。

2 测控安全防护需求分析

卫星通信网络建设面向集约化、智能化、自动化的发展要求，考虑

作者简介：朱兆国（1979—），男，山东泰安人，硕士研究生，高级工程师，研究方向：信息安全。

到未来不同轨道卫星频繁发射的特点，所有卫星发射和在轨运行工作，对于测控将产生巨大的需求，将存在各种难以预测的风险和威胁，也将对传统的测控方法、组织模式以及测控资源建设和分配产生巨大冲击，催生诸如一体化测控、基于云技术的测控等一系列新的测控技术。

基于硬件虚拟化的地面测控加密技术，在成熟的云平台基础上，利用硬件级虚拟化、测控密码服务能力的轻量级封装和编排技术，解决传统地面测控密码设备数量众多、各星密码服务独立配置隔离性差、星座测控密码资源管理能力弱等问题，为卫星通信网络大规模卫星测控安全提供技术支撑。

3 基于硬件虚拟化地面测控安全防护设计

地面测控安全防护基于硬件虚拟化技术，采用“硬件虚拟化平台 + 硬件虚拟化 PCIe 密码卡”构建一套完整的虚拟测控平台。

硬件虚拟化平台机采用一套完整的硬件虚拟化技术，实现 CPU、内存和存储资源、网卡等硬件级虚拟化，实现虚拟机之间 CPU、内存和存储资源、网卡的完全隔离、密码算力资源的完全隔离以及网络资源的完全隔离，进一步实现硬件级隔离和操作系统级隔离，最终实现每个虚拟机完全隔离，虚拟机进程间互不干扰。

硬件虚拟化 PCIe 密码卡虚拟化成多个虚拟功能 VF，每个虚拟功能 VF 具备独立的 I/O 通道资源和独立虚拟密码运算资源，可实现多个通道算法密码部件的独立、并发算法运算处理，且每个通道的通信带宽和算法运算资源不会发生被抢占的情况。

虚拟测控服务运行于硬件虚拟化平台虚拟化出的虚拟密码机中，采用不同的服务 IP 地址、服务域名或服务端口，采用不同的安全通道对外提供测控安全服务，通过硬件虚拟化通道访问密码卡的 VF 虚拟功能实现密码运算。

4 虚拟化测控安全防护实现

4.1 虚拟化测控安全防护平台系统架构

虚拟化测控安全防护平台（以下简称“虚拟测控平台”）采用硬件虚拟化技术实现完整的硬件环境硬件级虚拟化，虚拟出的每个虚拟机具备独占的 CPU、内存和存储、网络等资源，并具备完整的操作系统，虚拟机之间 CPU、内存和存储、网络等资源和操作系统等完全隔离，实现硬件级隔离和操作系统级隔离，虚拟机进程间互不干扰 [3]。同时，采用的硬件虚拟化密码卡亦采用硬件级虚拟化技术，单卡可支持虚拟化“1 个 PF+31 个密码运算 VF 虚拟功能”，每个 PF 和 VF 具备约 100Mbps 算法运算服务能力。

虚拟测控平台硬件采用“双路 20 核处理器（32 线程）+3 张硬件虚拟化密码卡”，部署 31 个虚拟机、3 个 PF 和 93 个 VF，每个虚拟机分别绑定 3 张国产硬件虚拟化密码卡的 1 个 VF，如此，每台虚拟测控平台具备 1 个宿主机、31 个虚拟测控密码机，每个虚拟测控密码机拥有 3 个 VF。

单颗卫星的测控数据加解密总性能要求一般不大于 1Mbps，每个 VF 密码算法能力不小于 100Mbps，远高于 6 颗卫星的测控加解密性能总和。因此，每个虚拟测控密码机具备 3 个 VF、部署 6 颗卫星的虚拟测控安全防护服务时，在满足测控加解密性能的前提下，可实现 VF 通道的冗余，在提高可用度的同时，具备很高的可靠性。

由上所述，单台虚拟测控平台可支持 186 颗卫星的测控加解密服务。

4.2 硬件虚拟化 PCIe 密码卡实现

硬件虚拟化 PCIe 密码卡划分为 3 个层次，即接口协议层、虚拟硬件层和硬件资源层，主要设计实现如下。

（1）接口协议层。接口协议层是密码卡与宿主机系统进行通信的部分，其中 PCIe 协议、SR-IOV 协议直接负责加密卡和主机的数据通信，SR-IOV 协议层能够将底层硬件抽象成不同的设备，并对上层的数据包进行解析和转发。功能接口层根据数据包的相关信息，将数据进行处理和转发。（2）虚拟硬件层。在 SR-IOV 协议下，硬件被抽象成 PF 和 VF，均具备相关的密码功能。一个密码卡的基本功能模块主要包括密钥管理模块（生成、存储、销毁等）、SM2/SM3/SM4 等国密算法。PF 和 VF 均具备这几个功能模块，同时 PF 中的设备管理单元对 VF 进行配置和管理。（3）密码运算。具有对称密码运算、公钥密码运算以及密码杂凑运算等密码运算功能，其中对称密码运算采用国密 SM4 算法 [4]，公钥密码运算采用 SM2 公钥密码算法 [5]，密码杂凑运算采用 SM3 密码杂凑算法 [6]。

4.3 虚拟测控服务实现

虚拟测控服务采用模块化设计，运行于虚拟测控平台虚拟

化出的虚拟测控密码机内部，经由业务网络实现测控业务数据与外部进行交互，采用服务接口形式和专用测控服务协议对外提供测控服务。此外，经由在线管理 / 同步网络，实现虚拟测控服务与管理系统之间的设备 / 状态管理、在线密码管理等消息 / 指令的交互，实现虚拟测控服务间现主备状态、任务状态同步消息的数据交互。

虚拟测控平台为了拥有更好的操作性、可用度，虚拟测控服务应具备云化应用、迁移和切换等功能。通过管理系统，可将虚拟测控服务在线下发并部署至虚拟测控密码机，实现云化应用[7]。

管理系统将虚拟测控密码机作为独立的密码机和虚拟测控密码服务进行设备管理，每个 VSM 都具备两对设备身份 ECC 密钥对，分别为设备签名密钥对和设备加密密钥对。当进行虚拟测控服务迁移时，管理系统通知源和目的虚拟测控密码机，由源和目的虚拟测控密码机之间建立安全通道，将源虚拟测控密码机虚拟测控服务、密钥、任务配置和任务状态等迁移到目的虚拟测控密码机，实现虚拟测控服务的迁移。

虚拟测控服务切换主要为虚拟测控密码机之间虚拟测控服务地切换，包括自动切换和人工切换。首先，自动切换时，按照启动运行时间判决主备，时间早的为主份，时间晚的为备份，当不同虚拟测控服务在同一时间段启动运行时，通过 SN 标识判决主备，SN 数值小的虚拟测控服务自动作为主份，SN 数值大的作为备份。其次，人工切换时，通过管理系统工人判决某一虚拟测控服务为主份，当前虚拟测控服务为备份且需成为主份时，此虚拟测控服务收到密码管理系统的指令后，按照指令内容切换至主份状态，并通过主备份通告消息告知其余的虚拟测控服务均切换为备份状态，实现虚拟测控服务切换。

5 虚拟化测控安全防护验证

按照实现的虚拟测控平台，每台虚拟测控平台具备 1 个宿主机、31 个虚拟测控密码机，每个虚拟测控密码机拥有 3 个 VF，共部署 186 个虚拟测控服务。从测控业务加解密、虚拟测控服务迁移 / 切换以及单台设备支持虚拟测控服务数量等方面进行测试验证。

（1）测控业务加解密验证。虚拟测控平台收到遥控帧加密请求后，对任务的虚拟测控服务进行遥控加密处理，并正确响应遥控密文。收到遥控帧加密或遥测帧解密请求后，对应任务的虚拟测控服务进行遥测解密处理，并正确响应遥测明文。（2）虚拟测控服务迁移 / 切换。管理系统向虚拟测控平台发起虚拟测控服务迁移流程，源虚拟测控密码机将指定的虚拟测控服务迁移至目的虚拟测控机，通过管理系统发起流程到结束的网络抓包完成流程可见，虚拟测控服务迁移时间约 196ms。（3）单台设备支持虚拟测控服务数量。单台虚拟测控平台部署 31 个虚拟化测控密码机，每个虚拟密码机部署 6 颗卫星虚拟测控服务，具备 186 颗卫星虚拟测控服务能力。

结语

基于硬件虚拟化的地面测控加密技术，在成熟的云平台基础上，利用硬件级虚拟化、测控密码服务能力的轻量级封装和编排技术，解决传统地面测控密码设备数量众多、各星座密码服务独立配置隔离性差、星座测控密码资源管理能力弱等问题，为卫星通信网络大规模卫星测控安全提供技术支撑。

引用

[1] 于淼,戚正伟.NewBluePill深入理解硬件虚拟机[M].北京:清华大学出版社,2011:167.

[2] 王春海.虚拟化技术指南[M].北京:机械工业出版社,2017.

[3] 国家密码局.GM/T 0104-2021云服务器密码机技术规范[Z].2021.

[4] 全国信息安全标准化委员会.GB/T 32907-2016SM4分组密码算法[Z].2016.

[5] 全国信息安全标准化委员会.GB/T 32918-2016信息安全技术SM2椭圆曲线公钥密码算法[Z].2016.

[6] 全国信息安全标准化委员会.GB/T 32905-2016 SM3密码杂凑算法[Z].2016.

[7] 全国信息安全标准化委员会.GB/T 35293-2017信息技术云计算虚拟机管理通用要求[Z].2017.