

# 基于移动终端和云的航天器在轨监视系统设计

刘 鹏, 王晓晨, 刘 超, 李 成, 王志会, 赵文彦  
(北京空间飞行器总体设计部 北京 100094)

**摘要:** 传统的航天器在轨监视体系为集中模式, 应急处置时存在时效性低、对在岗值班人员专业要求高等问题。随着在轨航天器数量的急剧增加, 亟需引入移动安全技术, 支持在可信网络传输环境下移动终端的安全接入和快速响应, 实现线上、线下的航天器设计、在轨管理技术力量有效综合利用。设计了一种基于移动终端和云平台的航天器在轨监视系统, 通过原型系统的实际测试, 验证了系统在技术上成熟可行, 能够实现航天器管理相关人员在远离任务中心的情况下, 通过移动终端以安全可靠的方式便捷地接入后端云平台, 及时掌握航天器在轨运行状况。

**关键词:** 移动终端; 云平台; 航天器; 在轨监视

中图分类号: TP311 文献标识码: A 文章编号: CN11-1780(2021)01-0031-09

## Design of in-orbit spacecraft monitoring system based on mobile terminal and cloud platform

LIU Peng, WANG Xiaochen, LIU Chao, LI Cheng, WANG Zhihui, ZHAO Wenyan  
(Beijing Institute of Spacecraft System Engineering, Beijing 100094, China)

**Abstract:** The traditional in-orbit spacecraft monitoring system is based on centralized mode, with the problems of low timeliness and high professional requirements for on-duty personnel in the case of abnormal disposal. With the rapid increase in the number of spacecrafts in orbit, it is imperative to introduce mobile security technologies to support the secure access and rapid response of mobile terminals in a trusted network transmission environment, this pattern can also make an effective comprehensive utilization of online/offline spacecraft design and in-orbit management technologies. This article proposes a design scheme of in-orbit spacecraft monitoring system based on mobile terminal and cloud platform. Through the test of prototype system, it is verified that the spacecraft management experts can access to the back-end cloud platform and monitor the status of spacecrafts through the mobile terminal in a reliable way while being far away from the task center.

**Key words:** Mobile terminal; Cloud platform; Spacecraft; In-orbit monitoring

## 引 言

航天器遥测参数具有类型多、数据量大和变化复杂等特点, 自动化的在轨实时监视系统能够避免仅依靠人工监测带来的效率低、漏检多、及时性和准确性差等诸多问题, 具有十分重要的应用价值<sup>[1]</sup>。传统的航天器在轨监视体系为集中模式, 实时监测报警、遥测数据可视化分析等测控系统均部署在测控中心内部专用网络中<sup>[2-4]</sup>, 当发生遥测参数报警时, 首先由在岗值班人员进行判读分析, 确认发现问题后再联系相关支持人员赴现场, 集中开展数据分析工作和故障处置。这种工作模式存在时效性低、对在岗值班人员专业要求高等问题。尤其在出现重大异常时, 大规模人员集中监视和异常处置分析的需求与疫情防控要求的矛盾愈发凸显。

随着云技术和移动互联网技术的快速发展, 国外各先进宇航机构已开始探索基于移动终端 APP 的方式实现安全可靠的远程监视, 如空间威胁的日益严峻迫使美军提出构建企业级地面系统 (EGS) 以进行转型, 以采用通用的测控系统完成所有军事卫星的测控, 该系统基于云基础设施提供共享服务和专门服务, 用户可通过通用和专用 APP 以加密方式接入, 从而减少操作人员, 提高系统效率, 降低运维成本<sup>[4]</sup>; NASA 和 Capitol Technology University 共同开展的 Hermes 项目实现了利用手机接收和控制亚轨

道卫星, 系统建立在通用的网络设备以及商用智能手机终端基础上, 可通过访问 web 页面方式实现遥测数据的监视和对卫星的控制<sup>[5]</sup>; 法国泰雷兹阿莱尼亚宇航公司通过开发在轨管理手机专用 APP, 经过专业安全措施后, 可使用手机进行在轨卫星遥测监视, 能够保障技术人员第一时间了解在轨卫星的状态以及遥测参数的变化趋势。目前, 国内各测控部门尚没有实现基于移动终端的航天器在轨监视, 某些航天器研制部门在自有新技术验证卫星的在轨管理工作中, 通过手机 APP 和互联网实现了较为简单的远程监视, 但并未引入安全机制。

为此, 本文依据移动监视的安全性和扩展性需求, 参考其他行业移动安全体系架构, 给出了一种基于移动终端和云平台的航天器在轨监视系统设计, 以期为我国未来航天器高效运行管理提供一种新的手段。

## 1 系统设计

### 1.1 总体架构

传统的航天器监视系统部署运行在小范围内部专用局域网络中, 与外部网络环境物理隔离。如果想实现基于移动终端的远程监视, 就必须与外部复杂的网络环境互连, 整个系统的复杂性和安全可靠性能较现有系统来说要大幅提高, 这就要求必须对整个系统进行非常规范的顶层架构设计。在研究如何定义必要的接口规范实现内网各功能子系统和外网移动终端之间的高效协同工作的同时, 更要充分研究如何实现很高的系统安全性和可靠性, 以支持长期稳定运行; 此外, 未来用户的应用场景可能会多样化, 还应研究如何提升系统扩展性以实现可信移动终端数量可扩充, 需要将云相关技术和传统的航天器在轨管理业务充分结合, 提出一种全新的在轨移动监视体系。

为了保障移动信息系统在美国政府和军队中的安全应用, 美国国防部、国土安全部、国家安全局等多个部门在 2012 至 2013 年先后出台了《移动设备战略》<sup>[6]</sup>、《移动能力包》<sup>[7]</sup>、《移动安全参考体系》<sup>[8]</sup>等政策与标准, 以指导移动信息系统安全防护体系的建设和技术的研发。无论是美国联邦政府给出的《移动安全参考体系》, 还是目前在警务、政务、金融、电力等其它领域的移动安全接入平台<sup>[9-12]</sup>, 总体上的体系架构均分为移动终端区、无线网络区、安全接入区、内网区。移动终端通过一系列的安全认证、加解密、准入控制、权限控制等安全解决方案, 可信地接入业务内网中。基于移动终端的航天器在轨监视系统从本质上来说也是一种移动信息系统, 因此, 本文在充分参考这些成熟安全体系架构以满足安全性需求的基础上, 综合考虑随着近些年我国在轨航天器数量急剧增加, 存在大规模移动用户并发访问的场景, 引入云平台提供高性能接入服务以满足扩展性需求, 从而将整个系统架构设计为移动终端、安全接入、移动服务、域间交换、内网业务五个子系统, 如图 1 所示。

① 移动终端子系统。该子系统主要包括可信移动终端设备及安装的 APP 软件, 并对移动终端的硬件、操作系统和应用软件进行安全加固, 保证终端计算环境、资源和网络访问的安全和控制。在普通智能移动终端上通过 SIM 卡贴膜或插入 TF 卡的方式植入可信芯片, 实现到安全接入子系统端到端的通信加密; 或进一步在定制的可信移动终端上对操作系统进行安全增强组件加固保护, 基于 PKI 体系和完整性校验算法, 对主控制器的引导过程、进程加载过程、应用的安装过程全程进行可信度量 and 校验。

② 安全接入子系统。该子系统主要包括防火墙、网关、CA 身份认证、移动终端管控、数字证书管理等功能, 基于移动电子身份证书实现移动终端和安全接入子系统之间的双向身份认证, 保证持有合法身份证书的移动终端才能接入, 防止非法移动终端接入合法网络; 保证移动终端与安全接入子系统之间的通信是建立在安全加密通道之上, 确保基于公共电信运营商网络传输过程数据机密性和完整性。

③ 移动服务子系统。该子系统是移动终端安全接入后访问的服务端, 主要基于云平台提供实时遥测推送、实时报警推送、遥测趋势查询、在轨信息查询、数据分析计算、权限认证、日志审计等服

务，支持大规模移动用户并发访问时高效弹性扩展。

④ 域间交换子系统。该子系统主要包括网闸、数据交换代理等设备，实现内网业务子系统与移动服务子系统之间的网络隔离和信息安全交换，所需业务数据由内网业务子系统经过处理后单向推送至移动服务子系统，数据交换代理前置和后置服务器对数据协议进行过滤，只允许符合遥测数据、报警信息和相关文件等协议的数据通过。日常监视时用户只能访问到移动服务子系统，从而确保中心内网中核心业务子系统的安全。

⑤ 内网业务子系统。该子系统运行在任务中心内网中，具备航天器在轨数据实时接收与处理、实时监测报警、健康评估、在轨大数据管理等核心业务功能。

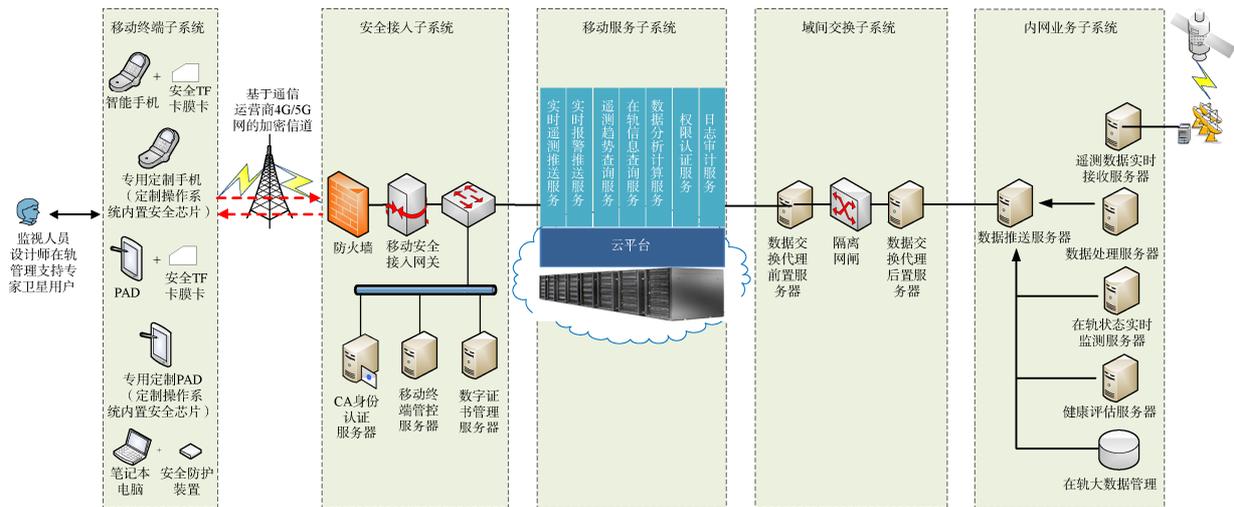


图 1 系统架构  
Fig. 1 System structure

### 1.2 安全机制设计

本系统设计的这五个子系统环环相扣，形成了终端加固、信道加密、认证接入、访问控制、网闸隔离、安全管理和审计监控等七大安全措施，共同构成独立完整的安全接入体系，满足了用户的身份安全、终端安全、网络传输安全、信息接入安全、信息交换安全等五大安全需求。本节给出了安全机制的详细设计。

在移动互联网金融领域，用户的人物关系图谱对于平台方来说预先是不可知的，一些移动支付软件如支付宝、微信等支持账号密码在异地登录，与手机没有强关联绑定，理论上用户 A 可以使用用户 B 的手机，并以用户 C 的账号和密码进行登录，因此存在账号混用、非法登录、非法授权等风险，需要在后台进行基于“环境、设备、偏好、账户、身份、行为、交易、关系”等多个维度全方位进行实时风险检测和控制。但是对于航天器测控业务来说，以航天器为关联对象，其用户单位、测控单位及研制单位之间各相关责任人是按要求预先设定好的，人物关系图谱对于操作人员和任务中心均是预先可知的。因此，本系统采用用户特征+安全芯片/数字证书+手机硬件特征（IMEI 号）+SIM 卡唯一编号（IMSI 号）的四码强关联绑定模式，实现人机匹配特征认证、终端与系统基于硬件标识+PKI 体系认证、APP 与业务平台实现令牌认证的三重安全认证机制，确保身份信息和认证安全可控，相关操作只能由符合要求的用户通过相匹配的终端完成，防止出现非法登录、非法授权、非法入侵等安全风险。

#### 1.2.1 终端安全设计

移动终端是移动业务应用系统的具体承载者，在本系统中，可以选择市场上通用的智能手机、PAD、笔记本电脑等各种普通智能终端，也可以选用经过定制的专用移动安全智能终端。其中，普通

智能终端必须在配备了安全智能卡和安装了安全服务软件后, 才能被允许接入安全接入子系统。根据移动终端形态的不同, 终端安全智能卡相应的有多种形式, 包括可插入的外置安全智能 TF 卡、可贴在手机 SIM 卡上的安全智能膜卡、通过 USB 连接的外置终端安全防护装置等; 专用移动安全智能终端则内置了安全引导、内核安全增强、沙箱和组件间安全通信机制、硬件安全模块、安全防护和管控组件等核心安全功能, 可以提供从硬件层到系统层再到应用层的多层级完整终端安全环境<sup>[13]</sup>, 防止出现非法刷机、非法入侵、对系统进程的非法定篡改、防逆向破解等风险。

普通终端和定制安全终端的区别及安全分类组合应用场景如图 2 所示。

产品形态	安全终端类型	安全组合形态	安全特性	功能及应用场景
智能手机	定制安全手机	软件: 定制安全系统 (ROM) 预置安全增强组件 应用软件加固 硬件: 手机板载安全芯片 或内置安全智能TF卡 或内置安全智能膜卡	1) 增强安全系统 2) 设备管控 3) 应用管控 4) 内容管控 5) 双系统隔离 6) 安全身份认证 7) 安全加密通信	终端运行环境安全 终端设备管控安全 应用安装校验 应用运行监控 硬件身份认证 数据传输安全 可以针对业务软件或APP所需权限、系统服务做适配、调整 (如推送实时在线、系统定位、WIFI管控等)
	普通智能手机	软件: 应用软件加固 硬件: 插入外置安全智能TF卡 或在手机SIM卡上贴安全智能膜卡	1) 安全身份认证 2) 安全加密通信	硬件身份认证 数据传输安全 对应用软件或APP无特殊支持, 有些系统权限可能无法调用
平板电脑	定制安全平板	软件: 定制安全系统 (ROM) 预置安全增强组件 硬件: 手机板载安全芯片 或内置安全智能TF卡 或内置安全智能膜卡	1) 增强安全系统 2) 设备管控 3) 应用管控 4) 内容管控 5) 双系统隔离 6) 安全身份认证 7) 安全加密通信	终端运行环境安全 终端设备管控安全 应用安装校验 应用运行监控 硬件身份认证 数据传输安全 可以针对业务软件或APP所需权限、系统服务做适配、调整 (如推送实时在线、系统定位、WIFI管控等)
	普通平板	软件: 应用软件加固 硬件: 插入外置安全智能TF卡	1) 安全身份认证 2) 安全加密通信	硬件身份认证 数据传输安全 对应用软件或APP无特殊支持, 有些系统权限可能无法调用
笔记本		通过USB连接外置终端安全防护装置	物理双系统隔离 内置安全芯片 安全加固操作系统 远程设备管控 数据存储加密 集成4G通信模块	外部双系统引导; 外部系统安全加固, 可信引导、内核增强、应用管控; 内置4G通信模块, 基于安全芯片实现安全通信; 提供透明存储加/解密功能, 保证存储数据安全可靠。

图 2 移动终端安全分类组合及应用场景

Fig. 2 Mobile terminal security classification combination and application scenarios

数据传输加密需要密码算法的支撑, 目前, 大多数系统中使用的密码算法都是 RSA、MD5 等国外的密码算法<sup>[14]</sup>, 本系统则采用基于我国密码管理局批准的 SM1、SM2 国产密码算法, 实现移动终端到安全接入子系统端到端的通信加密, 通过 SSL 国密版安全传输协议 MAC 计算和多重校验, 保证数据在传输过程中的机密性和完整性。其中, SM1 其加密算法不公开, 密钥长度和分组长度均为 128 位, 强度与 AES 相当。SM2 算法就是 ECC 椭圆曲线密码机制, 但在签名、密钥交换方面不同于 ECDSA、ECDH 等国际标准, 而是采取了更为安全的机制。

### 1.2.2 APP 安全设计

目前, 移动终端 APP 开发模式主要有 3 种<sup>[15]</sup>。①本地开发模式 Native APP。该模式具有非常强的兼容性, 为用户提供良好的交互功能。由于要根据移动终端的差异设计不同版本的应用程序, 因此, 维护和升级成本高, 操作复杂, 可移植性差, 推广应用不便。②Web 开发模式 Web APP。它是针对智能移动终端开发的 Web 站点, 客户端显示的数据都存储在服务器中, 客户端只需通过浏览器访问即可。因此, 具有跨平台性, 开发效率较快, 维护成本低, 可推广性强, 但在离线模式方面功能要比本地开发

模式弱, APP 无法调用手机的硬件 API, 功能受到一定限制。③混合开发模式 Hybrid APP。它是上述两种方式的结合, 可以用 Java Web 技术或另一种不针对某具体系统的第三方开发技术实现应用的功能。APP 同时具有了跨平台性和不错的硬件资源调用能力。

本系统采用混合开发模式, 业务功能模块利用 HTML5 网页开发模式来实现的, 本地不存储业务数据, 同时, 利用 Java 封装外壳, 用于安全服务接口调用。这样做的优点在于: ①满足安全性要求, 支持调用终端的安全服务软件, 且移动终端显示的数据都存储在服务器中, 本地不存储业务数据, 安全性较高。②满足可信移动终端功能可扩展的需求, 当需要对终端功能进行升级时, 不需要更新每一台终端, 只需要升级服务器端功能即可, 客户端 APP 重新登录后即重加载新功能。

应用 APP 发布前, 需提交 APP 安装包, 由统一认证服务对 APP 进行 HASH 运算, 生成 APP 摘要值, 并使用签名证书对应私钥对摘要值进行签名, 最终生成 APP 授权文件合并入 APP 安装包, 生成带签名信息的安装包。后续 APP 调用统一认证服务时, 由统一认证客户端对 APP 进行签名验证, 重新计算 APP 摘要值, 并读取签名授权文件, 调用终端安全芯片内根证书公钥验证签名证书合法性, 再使用签名证书公钥验证签名值, 并比对签名数据内摘要值与当前计算得到的摘要值是否一致, 从而确定 APP 身份可信、数据完整可靠。

### 1.2.3 接入认证机制

本系统的移动终端用户在使用 APP 时的接入认证机制主要分为 3 个步骤:

① 人机匹配特征认证。系统支持传统 PIN 码以及基于指纹生物特征两种认证方式, 当用户打开移动终端上的应用 APP 时, 会首先调用安全服务, 提示用户输入安全智能卡 PIN 码或是验证指纹, 从而得到安全智能卡芯片的使用权限。

② 建立加密安全隧道。人机匹配特征认证通过后, 终端调用安全智能卡芯片获取数字证书, 基于国密 SSL 协议与后台安全接入网关之间进行身份认证、密钥协商以建立加密安全隧道。之后, 通过系统 API 获取终端 IMEI 和 SIM 卡的 IMSI, 组成授权请求, 由安全接入网关根据用户后台绑定关系, 验证当前终端与用户数字证书是否一致, 并根据用户身份权限, 生成 ACL 策略信息(终端可访问目标地址路由信息)下发至终端, 以限定用户访问权限和范围。

③ APP 认证。加密安全隧道建立后, 统一认证客户端读取 APP 应用标识、安全芯片里的数字证书向统一认证服务发起统一认证请求, 获取用户 token 信息, 回传给 APP; APP 再以 token 作为身份凭证, 向业务后台发起身份认证请求, 由业务后台向统一认证服务验证 token, 读取对应的用户名、权限等信息回传 APP, 从而完成用户、终端接入身份认证过程。

## 1.3 高弹性云平台设计

传统的航天器监视系统部署在内部专网中, 并发访问终端数量少, 难以支撑灵活的规模伸缩、服务和数据的申请释放等需求, 存在性能和规模瓶颈, 不适用于大规模用户并发访问的场景。而随着航天器数量的急剧增加, 如果每个航天器的设计师、在轨管理人员和用户均能通过可信终端进行移动监视, 这就要求系统的可信移动终端和后端内网环境应具备如下功能: ①可信移动终端数量可动态扩充; ②可信移动终端的应用功能可灵活扩展; ③后端环境可根据移动终端数量实现资源的高效弹性扩展; ④后端环境可应对大规模移动终端的动态接入和快速响应; ⑤后端环境支持的航天器容量可扩展。

在美军、NASA、ESA 的航天地面软件系统中, 已开始大规模利用云技术提升系统的性能、弹性、灵活性, 降低成本。本系统针对航天器数量急剧增加带来的复杂业务需求, 考虑大规模移动终端用户并发访问的应用场景, 将分布式存储、容器 Docker 及虚拟化等云相关技术和传统的航天器在轨管理业务充分结合, 在移动服务子系统中构建高弹性在轨监测服务云平台。参考目前云计算平台主要分为 IaaS (Infrastructure as a Service)、PaaS (Platform as a Service) 和 SaaS (Software as a Service)<sup>[16]</sup>三层服务, 本系统设计的云平台也分为基础层、平台服务层和应用服务层共三层, 总体架构设计如图 3 所示。

① 基础层, 包括虚拟化平台和服务器、网络、安全、存储、备份等子系统, 旨在将云平台的计

算资源、网络资源和存储资源等基础硬件设施虚拟化后进行池化管理, 统一调配使用, 具备弹性伸缩机制。在系统建成后, 通过增设服务器、网络设备和存储容量即可支持未来新业务扩展。

② 平台服务层, 包括容器云、微服务、分布式数据库、消息中间件、运维与监控等平台化服务, 为上层各业务应用服务的稳定运行提供统一标准化云服务支撑。



图 3 在轨监测服务云平台架构

Fig. 3 In-orbit monitoring service cloud platform architecture

③ 应用服务层, 与移动终端交互的各种应用拆分成实时遥测推送服务、实时报警推送服务、遥测趋势查询服务、数据分析计算服务等多个不同的服务, 每个服务采用微服务架构封装成标准化的、高内聚低耦合的计算服务, 在 Docker 容器里进行独立部署、独立维护、独立扩展, 相关数据从 Kafka 消息中间件订阅获取, 通过 WebSocket 方式与移动客户端进行实时交互。

### 1.4 基于移动终端的海量遥测数据趋势快速无损查询设计

在移动终端上, 仅仅以列表形式实时查看关键参数遥测的当前数据值尚不能满足航天器在轨健康评估和异常分析的需求, 还需要提供长时间段的历史遥测数据趋势曲线查询功能, 但是这类查询涉及的数据量很大, 而移动终端又存在可视化屏幕小、显示维度少等问题, 假设检索 100 万条数据并全部显示, 按目前智能手机分辨率一般为 1280×720 像素到 2560×1440 像素来计算, 则 X 轴上每个像素需要显示约 500 个数值, 终端用户只能够看到这 500 个点堆叠后在最大值到最小值之间的一条竖线, 既看不清楚, 如此巨大的数据交互量也严重影响查询性能。因此, 如何能够基于移动终端实现准确而快速的海量遥测数据趋势曲线绘制是需要解决的一个关键问题。本系统借鉴层次细节模型 LOD (Level-Of-Detail) [17]思想, 基于分布式存储技术, 结合在轨遥测数据的特点, 设计出了一种适用于可信移动终端的海量遥测数据趋势快速无损查询方法, 其基本设计思路描述如下:

在本系统后端的云平台中, 海量遥测数据被按时间排序和等时间间隔切片后, 由分布式数据库系统通过 MD5 算法, 将连续的数据块均匀分配到不同的数据库服务器节点中存储。这样一方面可以均衡负载使多个服务器节点并发完成数据检索任务, 消除性能瓶颈; 另一方面可以使数据库具有高弹性, 能够随着未来数据容量的增加而动态扩展。具体实现时, 针对每一个切片, 以其中中心点的时标作为该切片的 key 索引, 切片内各遥测点的 8 字节时标只需采用相对于该 key 的 4 字节相对偏移量表示即可, 从而大幅压缩存储空间。此外, 利用大部分遥测数据变化比较缓慢, 特别是状态字数据在稳态下长时间没有变化的特点, 系统在等时间间隔切片方法的基础上, 进一步将遥测数据中值重复的点进行分离存储。在原有的切片 S 中, 只存储值发生变化的点, 分离出不变化的时间点, 并存储于另一个切片 S' 中, 从而可以抛弃重复的数据值, 进一步压缩存储空间, 如图 4 所示。若需要分析数据变化情况 (如设备开关机次数), 或统计一段时间区间内的数据极值点 (如温度、电流的波动情况), 均可直接检索原切片 S 中的数据, 提升检索命中率和系统性能。若需要查询全部数据, 只需将 S 和 S' 两个切片的数据全部检索出进行拼接即可。

在本系统前端的移动终端中, 系统依据查询时间比例尺动态提供两级查询模型: 第一级为特征值

抽样查询，第二级为全细节原样查询。当用户查询的数据趋势时间范围大于 15 分钟时，启动的是第一级特征值抽样查询模型，即由云平台中的遥测趋势查询服务基于上述分布式压缩存储算法，依据终端分辨率计算出 X 轴上每个像素点对应时间区间内所有遥测工程值的最大值和最小值并返回，客户端绘图时只需绘制这两点之间的连线即可。采用这种方法，无论查询多长时间的数据，返回给终端的数据点数都是固定的，且与采用全部数据绘图显示效果完全相同，不仅可以满足海量遥测数据趋势曲线快速绘制的性能需求，而且极大降低了系统的资源消耗。当用户想进一步了解趋势细节，将查询时间比例尺放大至 15 分钟以内时，则动态调整为第二级全细节原样查询模型，即云平台原样查询出相应时间范围所有的数据点返回。此外，系统还设计了一个环形缓冲区，在空闲的时候预取当前显示图形前后一段时间的数据，如果左右移动曲线，系统会直接从数据缓冲区返回数据，可进一步提高查询性能。

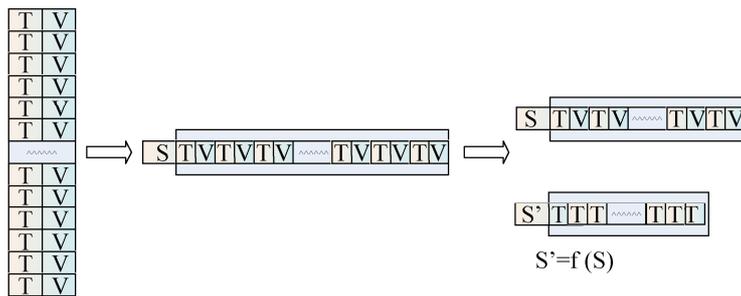


图 4 时间-值分离存储切片  
Fig. 4 Time-value separate storage slice

## 2 系统验证及应用前景分析

本文设计的基于移动终端和云平台的航天器在轨监视系统已经通过了原型系统的测试和验证，其安全体系经专家鉴定能够符合国家网络安全等级保护第四级安全技术要求，达到了在航天器在轨管理任务中工程应用的水平。通过在智能手机上部署了加密膜卡和 APP 软件，相关在轨管理人员在此次新冠肺炎疫情期间能够在家中方便、安全地接入中心系统，实时监视亚太九号、亚太 6C 等出口商业卫星的真实在轨遥测数据和报警信息，查看遥测数据历史趋势进行故障分析，在满足疫情防控要求的前提下顺利完成了日常监视任务。系统显示效果如图 5 所示。

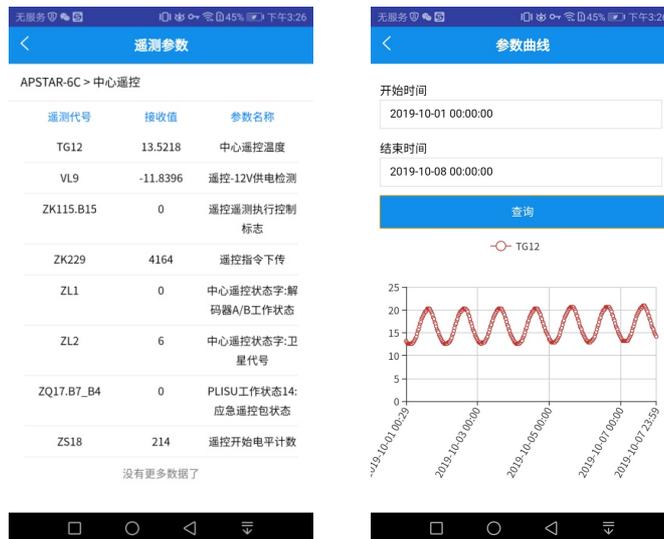


图 5 系统应用实例  
Fig. 5 System application example

未来, 本系统将逐步向其它领域的航天器和设计师队伍推广应用, 支持在可信网络传输环境下大规模移动终端的动态接入和快速响应, 能够将线上、线下的航天器设计和在轨管理技术力量进行有效综合利用, 实现航天器健康状态信息直达航天器管理人员, 使航天器管理相关人员在远离任务中心的情况下也能及时掌握航天器在轨运行状况, 有效参与应急处理, 提高任务快速响应能力和故障处理成效。

### 3 结束语

本文基于调研和需求分析, 给出了一种基于移动终端和云平台的航天器在轨监视系统设计, 通过原型系统的实际测试, 验证了系统在技术上成熟可行, 能够实现航天器管理相关人员在远离任务中心的情况下, 通过移动终端以安全可靠的方式便捷接入后端云平台, 及时掌握航天器在轨运行状况, 有效参与应急处理, 提高任务快速响应能力和故障处理成效。后续在转化为实际工程应用时, 还需要依据《中华人民共和国密码法》, 结合军民商用卫星不同的数据密级和应用要求进行进一步适应性评估和完善, 包括密码算法和技术方面应当符合法律、法规的规定和国家标准、行业标准的有关要求, 密码产品方面应通过国家密码管理相关部门批准; 此外, 还需要进一步提升云平台的成熟度, 基于深度数据挖掘提供一站式健康评估和处置决策支持服务, 能够将后端的预警信息主动实时推送至用户端, 实现被动性事后支持向主动性事前支持的转变。

### 参考文献

- [1] 刘鹏, 周永辉, 颜灵伟, 等. 基于 Pushlet 架构的航天器在轨实时监测报警系统[J]. 航天器工程, 2012, 21(3): 61–65.  
LIU Peng, ZHOU Yonghui, YAN Lingwei, et al. Real-time monitoring and alarming system for spacecraft in-orbit based on pushlet structure[J]. Spacecraft Engineering, 2012, 21(3): 61–65.
- [2] 肇刚, 崔卫华. 航天测控中心系统自主可控建设的研究与思考[J]. 飞行器测控学报, 2015, 34(4): 303–308.  
ZHAO Gang, CUI Weihua. Research and reflections on the construction of the proprietary and controllable aerospace TT&C central system[J]. Journal of Spacecraft TT&C Technology, 2015, 34(4): 303–308.
- [3] 张晓清, 潘清, 龚波. 欧洲航天地面软件系统发展研究[J]. 装备学院学报, 2015, 26(2): 88–93.  
ZHANG Xiaoqing, PAN Qing, GONG Bo. Research on the development of European space mission ground software system[J]. Journal of Equipment Academy, 2015, 26(2): 88–93.
- [4] 杨红俊. 美军航天测控企业级地面体系的发展[J]. 电讯技术, 2017, 57(7): 841–848.  
YANG Hongjun. Development of U. S. military enterprise ground architecture for space TT&C[J]. Telecommunication Engineering, 2017, 57(7): 841–848.
- [5] Project Hermes: Use of smartphone for receiving telemetry and commanding a satellite[EB/OL]. <https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20160013619.pdf>.
- [6] Office of DoD chief information officer. Department of defense mobile device strategy[S]. Version 2.0, 2012, 05.
- [7] National Security Agency. Mobility capability package, enterprise mobility[S]. Version 2.3, 2013, 11.
- [8] Federal CIO council and department of homeland security. Mobile Security Reference Architecture[S]. Version 1.0, 2013, 05.
- [9] 田野, 王彪, 刘丹. 基于大数据的一体化移动警务综合管控平台建设与应用[J]. 湖南科技大学学报(自然科学版), 2017, 32(1): 67–72.  
TIAN Ye, WANG Biao, LIU Dan. Construction and application of integrated mobile police management and control platform based on big data[J]. Journal of Hunan University of Science & Technology (Natural Science Edition), 2017, 32(1): 67–72.
- [10] 刘洋, 王俊人, 龚乐中. 政务安全移动办公需解决的关键问题与新发展方向[J]. 通信技术, 2017, 50(8): 1788–1793.  
LIU Yang, WANG Junren, GONG Lezhong. Key problem and new development for government secure mobile office[J]. Communications Technology, 2017, 50(8): 1788–1793.
- [11] 喻璐骅. 商业银行移动金融平台系统的设计与实现[D]. 长沙: 湖南大学, 2014.  
YU Luhua. Design and implementation of commercial bank mobile banking platform system[D]. Changsha: Hunan University, 2014.

- [12] 孙红强. 电力移动终端安全接入系统研究与实现[D]. 天津: 河北工业大学, 2015.  
SUN Hongqiang. Research and implementation of secure access system for power mobile terminal[D]. Tianjin: Hebei University of Technology, 2015.
- [13] 胡一博, 朱诗兵, 李长青. 移动智能终端安全体系研究[J]. 无线电工程, 2017, 47(9): 1-6.  
HU Yibo, ZHU Shibing, LI Changqing. Research on security architecture of mobile intelligent terminal[J]. Radio Engineering, 2017, 47(9): 1-6.
- [14] 赵宇亮, 胡威, 张冰, 等. 国家商用密码算法综述[C]. 2016 电力行业信息化年会论文集. 天津: 中国电机工程学会, 2016.
- [15] 李莉, 张超然, 刘丹, 等. 移动 APP 开发模式研究[J]. 长春理工大学学报(自然科学版), 2016, 39(5): 110-114,126.  
LI Li, ZHANG Chaoran, LIU Dan, et al. Research the development model of mobile applications[J]. Journal of Changchun University of Science and Technology, 2016, 39(5): 110-114,126.
- [16] 牛超. 基于容器的移动应用云平台关键技术研究[D]. 武汉: 华中科技大学, 2016.  
NIU Chao. A research on key issues of container-based cloud platform for mobile applications[D]. Wuhan: Huazhong University of Science and Technology, 2016.
- [17] 王青云, 罗泽. 基于 LOD 的海量地形数据并行渲染技术[J]. 计算机系统应用, 2017, 26(12): 200-206.  
WANG Qingyun, LUO Ze. Parallel rendering of massive terrain data based on LOD[J]. Computer Systems & Applications, 2017, 26(12): 200-206.

#### [作者简介]

- 刘 鹏 1981 年生, 硕士, 高级工程师, 主要研究方向为在轨管理智能技术。  
王晓晨 1979 年生, 硕士, 高级工程师, 主要研究方向为在轨管理智能技术。  
刘 超 1984 年生, 硕士, 工程师, 主要研究方向为在轨管理智能技术。  
李 成 1986 年生, 学士, 工程师, 主要研究方向为在轨管理智能技术。  
王志会 1988 年生, 学士, 工程师, 主要研究方向为在轨管理智能技术。  
赵文彦 1982 年生, 硕士, 工程师, 主要研究方向为数据管理与遥控技术。