北斗导航系统信息安全研究

王斯梁 冯 暄 陈 翼 蔡友保
(四川省计算机研究院 成都 610041)
(westone_wang@163.com)

Research of Information Security in Beidou Navigation System

Wang Siliang, Feng Xuan, Chen Yi, and Cai Youbao
(*Institute of Computer Science of Sichuan Province, Chengdu* 610041)

Abstract At present, the third generation of Beidou has been deployed. Beidou system will provide navigation positioning and communication data transmission services for global users. Beidou has been widely used in transportation, land and resources, disaster prevention and mitigation, agriculture, forestry and water conservancy, surveying and mapping exploration, emergency rescue and other fields in China. However, the information security related technical standard system of Beidou system is not perfect, and the cipher application is few. This paper first analyzes the composition of Beidou system and the published technical standards. The security risks in each link of Beidou system are concluded in the paper. Then, the information security assurance system of Beidou system is introduced according to the requirements of Classification Protection. Aiming at the unique short message application of Beidou system, an encryption solution based on three-layer key mechanism and symmetric encryption algorithm is proposed. Considering the security and the processing performance of Beidou terminal, the solution can be applied to the short message encryption field of Beidou in civil application.

Key words Beidou navigation system; information security assurance system; short message; three level schemes of key hierarchy; encryption solution

摘 要 目前北斗3代系统已完成部署,北斗系统将为全球用户提供导航定位和通信数传于一体的服务.北斗系统在我国已广泛应用于交通运输、国土资源、防灾减灾、农林水利、测绘勘探、应急救援等领域,但北斗系统信息安全相关技术标准体系尚未完善,密码应用方案较少.首先解析了北斗系统的组成及已发布的标准体系情况,分析了北斗系统各个环节存在的安全风险,然后参照等级保护要求提出了北斗系统的信息安全保障体系.针对北斗系统独有的短报文应用,给出了基于3层密钥机制和对称加密算法的加密方案,方案综合考虑了安全性和北斗终端的处理性能,能较好地应用于北斗民口的短报文加密领域.

收稿日期:2020-08-20
基金项目:四川省科技厅高新技术重大专项(2020YFG0030)

关键词　北斗导航系统；信息安全保障体系；短报文；3 层密钥机制；加密方案

中图法分类号　TP301

北斗卫星导航系统（以下简称北斗系统）按照“3 步走”战略建设发展，2020 年全面建成北斗 3 号系统，为全球用户提供导航定位和通信数传于一体的服务[1].

北斗系统相关产品已广泛应用于交通运输、国土资源、防灾减灾、农林水利、测绘勘探、应急救援等领域，立足于服务我国，辐射全球[2].

国务院印发《“十三五”国家战略性新兴产业发展规划》，明确建设自主开放、安全可靠、长期稳定运行的国家民用空间基础设施，加速卫星应用与基础设施融合发展[3].

本文解析了民用领域北斗系统运行机制、标准体系现状，分析了北斗系统存在网络安全需求，参考网络安全等级保护要求，给出了北斗系统的信息安全保障措施.针对北斗导航独有的短报文应用，给出了传输安全的密码应用解决方案，方案综合考虑北斗终端性能和密码应用的安全性.

1　北斗导航系统简介

北斗系统具备导航定位和通信数传两大功能，提供 7 种服务，具体包括：面向全球范围，提供定位导航授时、全球短报文通信和国际搜救 3 种服务；在我国及周边地区，提供星基增强、地基增强、精密单点定位和区域短报文通信 4 种服务[4].

北斗系统的组成由空间系统、地面系统和用户系统 3 部分组成[5].北斗系统空间段由地球静止轨道卫星、倾斜地球同步轨道卫星和中圆地球轨道卫星 3 种轨道卫星组成混合导航星座.北斗系统地面段包括主控站、时间同步站和监测站等地面站.北斗系统用户段包括北斗终端、应用系统与应用服务等[6].国内已有北斗系统的相关技术标准发布，主要集中在船载、车载导航系统通信方面，已发布的标准如表 1 所示：

表 1　北斗系统已发布的相关标准列表

标准名称	分类
《GB/T 27605—2011 卫星导航动态交通信息交换格式》	信息交换
《JT/T 591—2004 北斗一号民用数据采集终端设备技术要求和使用要求》	终端
《GB/T 26782.1—2011 卫星导航船舶监管信息系统第 1 部分：系统组成与功能定义》	监管信息系统
《GB/T 26782.2—2011 卫星导航船舶监管信息系统第 2 部分：系统信息交换协议》	监管信息系统
《GB/T 30287.1—2013 卫星定位船舶信息服务系统第 1 部分：功能描述》	信息服务系统
《GB/T 30287.2—2013 卫星定位船舶信息服务系统第 2 部分：船用终端与服务中心信息交换协议》	信息服务系统
《GB/T 30287.3—2013 卫星定位船舶信息服务系统第 3 部分：信息安全规范》	信息安全
《GB/T 23434—2009 运输信息及控制系统车载导航系统通信信息集要求》	通信要求
《SJ/T 11304—2005 卫星定位车辆信息服务系统第 1 部分：功能描述》	信息服务
《SJ/T 11305—2005 卫星定位车辆信息服务系统第 2 部分：车载终端与服务中心信息交换协议》	信息交换
《JT/T 794—2011 道路运输车辆卫星定位系统车载终端技术要求》	车载终端
《JT/T 796—2011 道路运输车辆卫星定位系统平台技术要求》	系统平台
《JT/T 808—2011 道路运输车辆卫星定位系统终端通信协议及数据格式》	终端通信
《JT/T 809—2011 道路运输车辆卫星定位系统平台数据交换》	系统平台
《GB/T 29841.3—2013 卫星定位个人位置信息服务系统 第 3 部分：信息安全规范》	信息安全

从标准的分布情况来看，信息安全相关标准仅 1 项，主要是解决位置服务隐私数据保护，而密码应用、身份认证、态势感知等北斗领域信息安全行业标准有待完善.

2 北斗导航系统信息安全保障体系

2.1 信息安全需求

1）北斗导航应用

国产北斗导航类软件中使用高精度亚米级数据的安全风险较多，包括位置数据采集、处理、存储等流程缺乏审查机制，数据传输过程尚未采取安全措施，数据易遭窃取.

2）北斗终端

北斗终端的应用环境存在安全风险，接口及数据传输协议、差分协议等无审查机制和信息安全措施，未授权用户可获取高精度北斗终端或通信终端上的数据.

3）运营服务与场景应用

北斗综合信息服务系统是基于北斗导航技术，利用计算机网络、通信和大数据等多种技术，提供多场景下的位置服务的应用系统.

北斗系统的运营服务和场景应用需要将北斗位置数据结合不同的行业需求，北斗系统的位置数据在传输和应用过程中存在着被篡改和泄露的安全风险.

从已有文献资料分析可知，北斗系统具体信息安全需求如表2所示：

表2 北斗系统的安全需求

北斗系统		信息安全风险来源
基础产品	硬件	1）板载系统漏洞无防护机制 2）板载系统无访问控制 3）高精度北斗芯片、模块、板卡易被非法开启，无预警机制 4）高精度北斗芯片、模块、板卡物理接口较多，无端口访问控制机制
	软件	1）高精度导航软件的接入无限制，底层数据有被破解的风险 2）数据处理软件可能存在后门漏洞，无审计机制
	数据	1）数据无加密防护措施，易被窃取 2）数据传输过程中的数据完整性无法保证
终端产品	授时终端	授时终端可能存在系统漏洞，终端易被接入和操作
	通信终端	1）通信终端易受电磁干扰，影响通信稳定性 2）通信终端数据无加密，易被窃取
	导航终端	1）导航终端有被非法开启、操作或非法网络接入的风险 2）导航终端互联时无身份认证和访问控制机制
	测量终端	1）测量终端无人工保护时容易受到非法攻击 2）测量终端通信无加密措施，数据可被截获 3）测量终端接入无控制手段，数据输出也都是明文传输，极易被窃取
系统应用及运营服务	系统应用	1）北斗系统综合应用涉及以太网、光纤、无线网络等多种传输方式，易被监听及入侵 2）数据缺少加密方式
	运营服务	1）单向身份鉴权，攻击者可以伪造CORS基准站 2）越权访问 3）计算环境存在的安全风险包括终端、网络设备、数据库等存在安全隐患

2.2 信息安全保障体系

北斗系统充分利用计算机网络和卫星通信技术，以云计算、大数据等技术架构，构建以位置数据服务为核心的信息系统.北斗系统架构如图1所示.

1）北斗基准站

地面部署的北斗基准站实时接收北斗导航卫星发送的定位信息，将信息通过专用网络发送给其对应的数据中心（地面中心站）.

2）数据中心

数据中心（地面中心站）接收来自基准站的卫星定位数据，作脱密处理、差分校准等计算，将计算得出的差分校准值通过互联网或者数字广播的

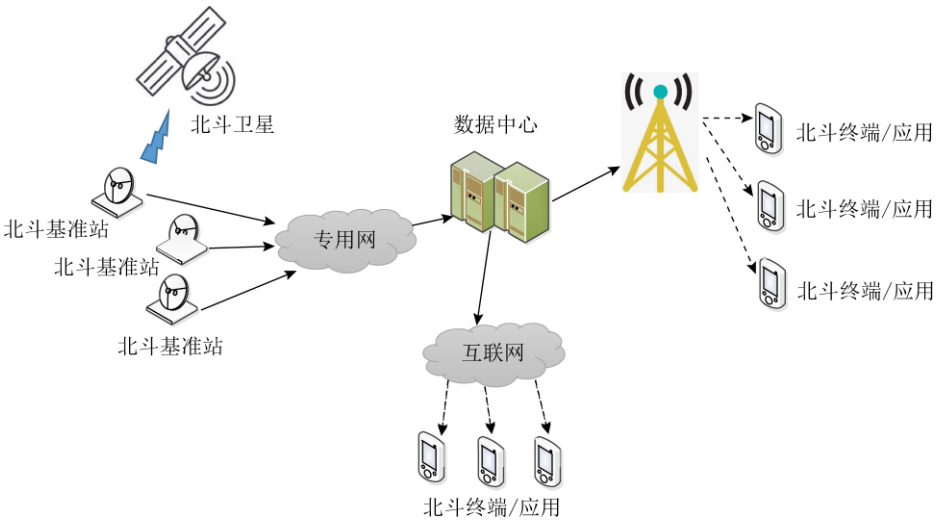

图 1　北斗系统运行架构

方式发送给有北斗终端用户.

3）北斗终端及应用

通过互联网请求或广播接收的方式获取来自数据中心的差分校准值，修正北斗卫星的定位数据，获取精确的导航定位信息.

从等级保护 2.0 角度，北斗系统同样存在着物理安全、网络安全、应用安全、数据安全等诸多安全风险，需要构建以态势感知为核心的网络安全防御体系，以抵御各类潜在的安全风险和隐患.

数据中心要针对物理环境和服务器访问行为进行管控，确保数据存储和访问安全；导航数据通过互联网传输时需要采用数据加密和身份认证等措施，确保数据的完整性和机密性；北斗终端在使用及应用导航数据时，应采用身份认证、访问控制、数字签名、安全审计、可信评估等安全措施，确保用户接入北斗网络的安全可控，确保导航数据不被泄露和篡改.

短报文通信是北斗系统特有的功能，在国防、民生和应急救援等领域都具有广泛的应用前景.在民口短报文应用中，由于目前缺乏必要的安全防护措施，严重制约了短报文的应用.

3　短报文加密方案

北斗系统的短报文通信具有用户机与用户机、用户机与地面控制中心间双向数字报文通信功能.短报文可 1 对 1 和 1 对多进行通信，可广泛应用于各类应急救援应用场景中.

目前，北斗短报文在通信传输过程中，通过数据中心（地面中心站）把报文信息以明文的方式传输给短报文接收端，未作任何加密防护处理，这样会导致报文信息很容易被截获，造成严重的安全隐患.

北斗短报文存在 2 种不同的协议：北斗 4.0 协议和北斗 2.1 协议.4.0 协议为二进制格式，逐渐被 2.1 协议取代.2.1 协议为文本格式，兼容 RDSS（卫星无线电测定业务）和 RNSS（卫星无线电导航业务）[7].北斗短报文支持字节数量有限，需选择效率较高的加密算法.

考虑到北斗终端处理能力有限和北斗短报文长度的限制，可采用 3 层密钥体系，使用对称加密体制，实现短报文的传输加密，加密方案如图 2 所示.

步骤 1.密钥管理中心通过可信的安全通道（USBKey 或是离线灌注密钥等方式）下发密钥，包括北斗终端持有的终端密钥和地面中心持有的主密钥，终端密钥分别发送给各个终端和地面中心，地面中心还接收主密钥.密钥管理中心定期更新已申领终端密钥者的北斗终端 ID 号，并将其推送给地面中心.地面中心利用北斗终端的 ID 号随机产生密钥加密密钥，并用主密钥进行加密存储.地面中心利用加密密钥加密终端密钥进行存储，这些加密存储均采用对称密钥算法实现.

步骤 2.北斗发送端内置密码模块，利用获取的终端密钥 Sender-Key，采用对称加密算法，加密

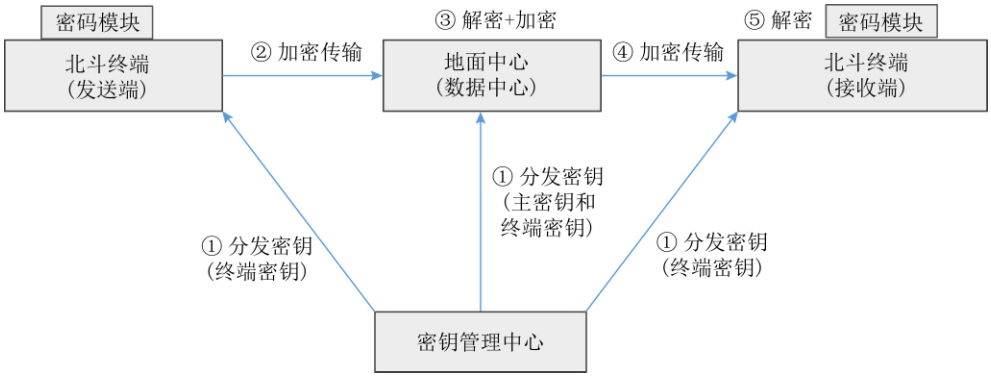

图2 北斗系统加密方案

报文，并编码传输至地面中心.

步骤3.地面中心获取北斗终端发送过来的密文信息，根据终端ID(ID-sender)，使用主密钥解密出密钥加密密钥EncrKey-sender，并利用EncrKey-sender解密获取终端密钥Sender-key，利用Sender-key对接收密文进行解密，获取接收终端ID(ID-receiver)信息，根据ID-receiver，由主密钥解密获取密钥加密密钥EncrKey-receiver，利用EncrKey-receiver获取接收端的终端密钥Receiver-key.上述加解密过程均使用对称密码算法实现.

步骤4.地面中心利用终端密钥Receiver-key加密报文，编码发送至接收终端.

步骤5.接收终端接收到密文，利用终端密钥Receiver-key解密报文，并解码获取短报文内容.

从安全性分析，本方案采用3层密钥体制，层层向下加密，各层密钥都得到安全存储，终端密钥和主密钥通过USBKey分发或离线灌注分发，确保了安全性.其次，本方案中均采用对称加密算法，大量的加解密工作主要在地面中心(数据中心)完成，加解密效率较高，适用于北斗卫星链路环境.

4 结束语

现阶段北斗3代已完成部署，民口北斗位置服务将全面展开，位置数据应用将与个人隐私数据和企业商业行为全面关联.恶意用户在获取位置数据时也同时获取行动轨迹信息，造成个人隐私数据和企业的商业数据泄露.因此，北斗数据通信加密以及防窃取、防篡改将成为制约北斗系统大范围民用的主要因素.

随着我国网络安全法和密码法的颁布实施，关系到国计民生的重要信息系统及关键基础设施均需要使用国产商用密码技术，对敏感信息进行保护[8].北斗系统作为重要的关键基础设施，更应规划和落地国产商用密码的应用标准研究和解决方案研发.

本文从信息安全角度提出北斗系统安全需求和保障体系，对北斗系统独有的短报文应用场景进行安全分析，提出了较为实用的传输加密方案.后续可在北斗系统密码应用标准体系、网络安全标准体系等方面开展研究.通过建立技术标准体系，规范业界厂商应用北斗导航数据，促进北斗系统信息安全保障体系早日建立.

参 考 文 献

[1] 中国导航系统管理办. 北斗卫星导航系统发展报告[OL]. (2019-12-03)[2020-08-20]. http://www.beidou.gov.cn

[2] 国务院新闻办. 中国卫星北斗导航系统白皮书[OL]. (2016-06-09)[2020-08-20]. http://www.beidou.gov.cn

[3] 国务院. “十三五”国家战略性新兴产业发展规划的通知[OL]. (2018-02-24)[2020-08-20]. http://www.gov.cn/zhengce/content/2016-12/19/content_5150090.htm

[4] 杨元喜. 北斗卫星导航系统的进展、贡献与挑战[J]. 测绘学报，2017，1(3)：12-16

[5] 吴海玲. 北斗卫星导航系统发展与应用[J]. 导航定位学报，2015，5(2)：35-38

[6] 贠敏，葛榜军. 北斗卫星导航系统及应用[J]. 卫星应用，2012，5(7)：44-49

[7] 魏小强，张雁丘. 北斗卫星导航系统及其应用[J]. 电子技术与软件工程，2016，2(16)：47-51

[8] 国密局. 深入学习贯彻《中华人民共和国密码法》[OL]. [2020-04-25]. http://www.oscca.gov.cn/sca/ztzl/xcgcmmf/

王斯梁

博士，高级工程师，主要研究方向为网络安全和密码应用.

westone_wang@163.com

陈　翼

高级工程师，主要研究方向为企业信息化管理和云计算.

yi.chen@scsics.com

冯　暄

硕士，高级工程师，主要研究方向为信息系统设计和云计算安全.

xuan.feng@scsics.com

蔡友保

工程师，主要研究方向为科技项目申报和云计算.

caiyoubao@scsics.com