GM/Y 5012-2024

北斗短报文密码技术应用研究

密码行业标准化技术委员会
CRYPTOGRAPHY STANDARDIZATION TECHNICAL COMMITTEE

2024 年 12 月

摘 要

北斗短报文是北斗卫星导航系统区别于其他三大卫星导航系统(美国的 GPS,欧洲的 Galileo 和俄罗斯的 GLONASS)的特色功能和突出优势。它将短信和导航相结合，具有覆盖范围广、建设周期短、投资成本低等优势，在智能交通、精准农业、电力监控等多个行业拥有广泛的应用。但是，北斗卫星导航系统在设计之初仅考虑了系统本身运行的安全，在短报文通信民口应用的安全性设计方面非常薄弱，存在潜在的安全风险，需要对其进行基于密码的安全防护以保障系统安全运行。目前，国内外暂无关于北斗短报文民口应用的密码技术应用标准规范，针对北斗短报文数据传输通信的特点，设计北斗短报文结合商用密码的安全防护方案,形成《北斗短报文密码技术应用研究》报告，解决北斗短报文通信的数据安全问题，为构建安全可靠的北斗短报文通信应用提供保障。

本研究报告共有七章，第一章概述北斗短报文密码技术应用的相关政策背景、技术支撑背景及本次研究的目标；第二章介绍北斗短报文密码技术应用在国内外的现状和发展趋势，以及标准化现状；第三章分析北斗短报文通信的特点，抽象出共性、关键性问题，提出安全防护的需求，制定研究内容、技术线路，提出解决方案的总体架构，应用于不同场景中的方案模型并进行对比分析；第四章根据第三章所提 E2EE-CKM 方案及应用场景，提炼出其中的安全需求、加密模型、密码应用技术框架，形成规范性要求，作为后续标准制定的基础；第五章介绍目前北斗短报文密码技术应用案例；第六章对北斗短报文密码技术应用的标准化工作进行研究；第七章对报告内容进行总结。附录 A 为北斗短报文密码应用的具体方案。

关键词：北斗卫星，北斗短报文，商密算法，安全传输，加密

目 录

摘要 I
目录 II
专用术语（符号、变量、缩略词等）的注释表 III
前言 IV
北斗短报文密码技术应用研究 1
1. 概述 1
1.1 背景 1
1.2 研究目标 2
2. 发展现状 3
2.1 国外现状 3
2.2 国内现状 3
2.3 发展趋势 14
3. 北斗短报文安全现状及密码技术研究 16
3.1 需求分析 16
3.2 研究内容 19
3.3 主要难点 19
3.4 技术路线 19
3.5 解决方案 20
4. 通用模型研究 26
4.1 研究概述 26
4.2 安全需求分析 26
4.3 加密通用模型 27
4.4 密码应用技术框架 28
4.5 安全性分析 31
5. 北斗短报文密码应用案例 33
5.1 交通运输部课题研究应用 33
5.2 北斗短报文加密方案推广应用 35
6. 标准化研究 38
6.1 采标计划 38
6.2 标准研究思路 38
6.3 标准化建议 38
7. 总结 40
参考文献 41
附录 A 北斗短报文密码应用方案 42
A.1 系统框架 42
A.2 密码算法 42
A.3 密钥体系 45
A.4 密码协议设计 46
A.5 安全性分析 55
A.6 典型方案部署 56

专用术语（符号、变量、缩略词等）的注释表

BDS	北斗卫星导航系统（BeiDou Navigation Satellite System）
HMAC	带密钥的杂凑运算（Keyed-Hash Message Authentication Code）
MAC	消息鉴别码（Message Authentication Code）
RDSS	卫星无线电定位系统（radio determination Satellite system）
RNSS	卫星无线电导航业务（Radio Navigation Satellite System）
ZUC	祖冲之序列密码算法或祖冲之算法

前 言

本研究报告任务来源于2019年密标委向中电科网络安全科技股份有限公司（原名成都卫士通信息产业股份有限公司）下发的《北斗短报文密码技术应用研究》的编制任务。

本研究报告项目承担单位中电科网络安全科技股份有限公司成立编制工作组，编制单位包括北京北斗星通导航技术股份有限公司、厦门雅讯网络股份有限公司、北京国脉信安科技有限公司、兴唐通信科技有限公司、成都九洲电子信息系统股份有限公司等多家单位。

本研究报告得到袁峰、高能两位专家的指导，主要研究人员有张舒黎、张立廷、王雍、王现方、张正烜、宁军、庞子涵、韦昌荣等。

北斗短报文密码技术应用研究

1. 概述

1.1 背景

北斗卫星导航系统是我国自主发展、独立运行的全球卫星导航系统，为军、民用户提供了快速定位、实时导航、精密授时等服务功能。北斗卫星导航系统最大的特色在于有源定位和短报文特色服务。它将短信和导航结合，区别于世界上其他几大导航定位系统。随着北斗卫星导航系统的逐步全球化，北斗短报文通信在民用领域的应用不断扩充，在交通运输行业的“两客一危”车辆监控管理、远洋渔业通信、无人自动驾驶、农业精耕、电力监控、水文监测以及应急救援等各个领域发挥着重要作用。目前，在民口应用中，北斗短报文数据都是以明文方式进行传输，传输敏感数据时存在安全保护需求，国家层面相继出台了相关的政策法规指出北斗短报文密码技术应用的必要性，相关政策如下：

1) 政策背景

国家层面政策法规：

《中华人民共和国网络安全法》：建设关键信息基础设施，保证安全技术措施同步规划、同步建设、同步使用。

《中华人民共和国测绘法》：新增“监督管理”章节，明确建立地理信息安全管理制度和技术防控体系，并加强对地理信息安全的监督管理。

《中华人民共和国密码法》：关键信息基础设施强制性要求使用密码进行保护，同步规划、同步建设、同步运行密码保障系统。

《“十三五”国家信息化规划》提出，构建关键信息基础设施安全保障体系，要加强密码应用，国家互联网大数据平台建设，要推进数据加解密、完整性验证等安全技术的应用。

《“十四五”国家信息化规划》提出，建设基础网络、数据中心、云、数据、应用等一体协同的安全保障体系。开展通信网络安全防护，研究完善海量数据汇聚融合的风险识别与防护技术、数据脱敏技术、数据安全合规性评估认证、数据加密保护机制及相关技术检测手段。

《金融和重要领域密码应用与创新发展工作规划（2018-2022）》提出，促进密码在新一代国家交通控制网、多式联运信息资源共享、北斗导航中的应用。

《“十四五”信息通信行业发展规划》提出，把建设新型数字基础设施作为“十四五”发展重点之一，提出全面部署新一代通信网络基础设施，促进北斗卫星导航系统在信息通信领域规模化应用。

其他相关政策法规：

《测绘地理信息领域重要信息系统商用密码应用规划（2016－2020 年）》明确提出推进基准站网商用密码应用，推进面向社会服务的测绘地理信息政务信息系统商用密码应用，建立健全商用密码应用标准体系。

《关于规范卫星导航定位基准站数据密级和管理的规定》普通基准站观测数据采用专网或商用密码手段加密保护后向数据中心进行传输。

2) 技术背景

北斗短报文通信的数据传输及关键业务数据安全需要密码技术提供保障。目前，国内北斗短报文民口应用普遍未使用安全防护技术，相应的密码应用标准规范也尚未形成，存在潜在的安全风险。在这样的形势下，研究一套行之有效、符合我国国情的北斗短报文密码技术应用标准体系势在必行。北斗短报文通信应用可以在数据安全防护层面充分利用现有商密技术的应用成果，真正让商密算法为北斗短报文系统的安全自主提供支撑保障，促进我国信息安全事业的发展与壮大。

1.2 研究目标

1） 主要研究内容

通过北斗短报文通信应用场景研究，分析其业务流程环节存在的安全风险和威胁隐患，提出北斗短报文应用加密技术方案，保障北斗短报文通信的安全性。主要包含如下研究内容：

a） 研究北斗短报文通信多场景应用，进行安全需求分析；

b） 研究北斗系统短报文数据传输加密、密钥管理等技术；

c） 设计一套北斗短报文安全通信加密方案。

2） 研究思路

根据北斗系统短报文通信的研究，制定如下的研究思路：

a） 安全风险分析及安全需求挖掘：通过北斗短报文通信在不同业务场景中的应用研究，充分提炼抽象出北斗系统短报文通信在民口应用的共性和关键问题；分析北斗短报文通信模式，挖掘出其中的安全隐患，梳理安全防护需求；

b） 关键技术研究：研究北斗短报文端到端传输加密技术包括总体架构、密码算法、密钥体系、密码协议设计等；研究商用密码与北斗短报文协议融合技术，基于短报文设计数据、管理、控制通道，设计嵌入密码的报文格式、协议流程，实现数据安全传输、密钥安全分发等功能。

3） 目标或交付物

根据北斗短报文加密技术研究，提出《北斗短报文密码技术应用研究》报告，解决短报文通信应用数据加密安全，为北斗系统短报文通信应用安全提供技术储备和理论支撑。

2. 发展现状

2.1 国外现状

北斗系统采用了 RNSS 和 RDSS 双模结构体制，不但具有 GPS 的导航、定位和授时功能，同时还提供 RDSS 双向短报文信息服务，即卫星通信的功能，是全球首个在定位、授时之外集报文通信为一体的卫星导航系统，这一点是其他三大卫星导航系统(美国的 GPS,欧洲的 Galileo 和俄罗斯的 GLONASS)所不具备的，这也是北斗系统的核心优势。它通过空间卫星将信号传输到接收机上，既可以避免传输距离近的弊端，又可以提高通信质量。北斗系统的信号范围已覆盖整个亚太地区，根据国家北斗系统建设战略，2020 年北斗系统信号已覆盖全球。由于国外三大卫星导航系统 GPS、Galileo、GLONASS 均不具备短报文功能，所以本章节此处不展开阐述。

2.2 国内现状

2.2.1 北斗短报文技术应用现状

2.2.1.1 北斗短报文通信技术

短报文发送端和接收端通过出站、入站链路形成一个 M 型的通信机制。短报文发送端将生成的短报文发送给卫星，卫星收到短报文后通过卫星链路发送给地面中心站；地面中心站收到信息后通过用户管理系统确定用户有效性，待确认通过后将短报文通过卫星链路转发给短报文接收端；即完成一次完整的短报文通信过程。北斗短报文通信模型如图 2-1 所示。

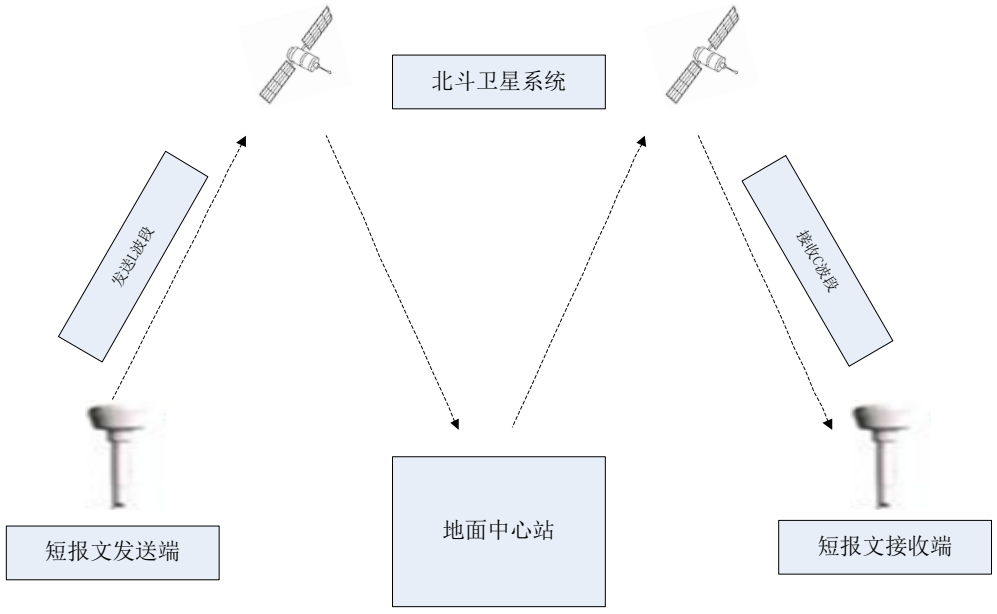


图 2-1　北斗短报文通信系统通用场景

北斗短报文通信涉及到两个协议，分别是 4.0 协议和 2.1 协议。

4.0 协议的全称是《北斗一号用户机数据接口要求》，版本 4.0，2006 年 11 月发布，简称 4.0 协议。4.0 协议为二进制格式，接口数据传输基本格式如表 2-1 所

示：

表 2-1　短报文 4.0 协议格式示例

指令	长度	用户地址	信息内容					校验和
通信申请 $TXSQ	16 bit	24 bit	信息类别 8bit	用户地址 24bit	电文长度 16bit	是否应答 8bit	电文内容最长 1680bit	8 bit

内容	长度	用户地址	信息内容							检验和
通信信息 $TXXX	16 bit	24 bit	信息类别 8bit	发信方地 24bit	发信时间 H 8bit	发信时间 M 8bit	电文长度 16bit	电文内容最长 1680bit	CRC 标志 8bit	8 bit

目前民用北斗卡中，用户可输入的信息最长为 78 个字节。通信信息类别的 8bit 组成如下所示：

表 2-2　短报文通信信息类别示例

报文通信 3bit	密钥 1bit	通信类别 2bit	传输方式 1bit	口令识别 1bit
010	固定填 0	00 特快通信 01 普通通信	0 汉字 1 代码	0 通信 1 口令识别

“密钥”这个标识是给系统用的，固定填“0”。入站通信申请时则由用户机根据本机对 IC 卡的自检情况，在入站信息中具体填入有无密钥。如果填 1，系统会认为是加密信号，按加密信号处理，解密后发给接收方，以乱码形式呈现。通过对民口应用了解得到，此处固定填 0，如果需要加密，可以在通信内容里面重新定义字段标识是否加密。目前通过调研了解到，北斗短报文通信民口应用此处大多未做加密设置。

2.1 协议的全称是《北斗卫星导航系统用户终端通用数据接口（预）》，版本 2.1，2014 年 8 月发布，简称 2.1 协议。2.1 协议为文本格式，接口数据传输格式以语句的方式定义，以通信信息输出语句 TXR 为例，语句格式如下：

$--TXR,xxxxxxxx,x,hhmm,c--c*hh<CR><LF>

其中，“$”表示一条语句的开始，“hh”表示和校验字段，对“$”到“*”之间的字符执行 XOR（异或）运算所得。通信的电文内容在“c--c”位置，内容必须以有效的 ASCII 字符表示，除去一些预留字符，能在电文内容出现的有效字符范围大小为 89 个。目前民用北斗卡中，用户可输入的信息最长也为 78 个字节。

上述为北斗二号短报文通信情况。北斗三号短报文最多可输入 1000 字节信息，但报文格式基本保持一致。本研究重点面向北斗二号系统，但相关技术可拓展应用于北斗三号系统。

2.2.1.2　北斗短报文密码技术

目前，民用北斗短报文通信应用大多未采用密码技术进行安全保护，市场应用未得到规范化，与无具体的规范标准可以遵循有着很大的关系。一些行业用户、科研机构结合实际需求，对短报文实施密码保护，保障短报文的通信安全。在电力行业，通过在短报文终端前装置安全网关，采用非对称与对称结合的机制，实现身份认证、数据加密等安全功能。在石油行业，通过在短报文终端上内置加密模块，对

采集数据进行加解密，保护石油管网数据的安全。在交通行业，对铁路机车上的北斗短报文通信数据进行加密，确保敏感数据的应用安全。总的来说，部分行业领域（如石油、电力等）已经意识到安全需求的重要性，并积极应用密码技术。通过调研多行业多领域，对已有的民口短报文密码应用进行归纳总结，得到密码技术与密码产品的应用情况如图 2-2 所示：

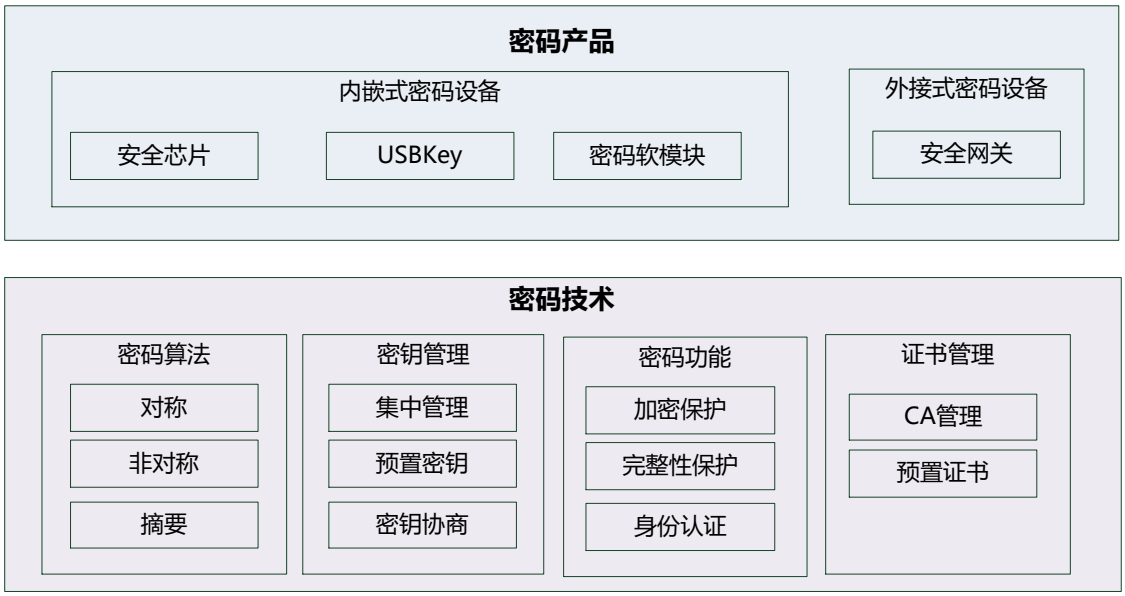


图 2-2　北斗短报文密码技术现状

密码技术：在密码算法方面，采用 RSA、AES 等国际密码算法，与采用 SM2、SM3、SM4 等密码算法两种情况都存在。在密码功能方面，大多数场景只对短报文数据进行对称加密，一些特定场景也对短报文通信进行身份认证以及短报文数据的完整性保护。在密钥管理方面，存在着集中密钥管理与设备自行管理两种情况，其中设备自行管理也分为预置密钥和协商密钥两种模式。在证书管理方面，一般为两种模式。其一为一次性预置证书的形式，其优点是可操作性强、实现简单，缺点也很明显，即无法进行基于证书的生命周期管理，无法做到基于证书的管控；另一种为配置 CA 的方式，进行离线/在线的形式进行证书的签发、更新、撤销、冻结等，这需要通过网络或者手动的方式和 CA 进行通信，适用于管理性很强的专用短报文场景中，很难在大规模的商用场景中开展实施。

密码产品：为北斗短报文终端上部署的密码产品分为两类。其一为短报文终端内嵌的形式，即把加密芯片、USBKey、密码软模块等密码设备嵌入到短报文终端上，赋予数据加密、身份认证等能力，形成一体化安全的短报文终端。其二为短报文终端外接安全网关的形式，即在短报文终端与网络出口间接入安全网关，实现短报文协议转换、数据过滤的同时，保障短报文通信数据的安全保护以及通信身份的安全认证。

2.2.2　北斗短报文市场现状

北斗系统短报文将短信息和导航结合，是中国北斗卫星导航系统的独特发明，也是一大优势，无论是军事价值还是民用价值都备受业界肯定。短报文在行业应用范围不断拓展，产值也呈逐年上涨趋势。北斗短报文现主要应用在交通、远洋渔业及应急救援等行业领域中。交通运输部参与搜救的海事、救助船舶上大量安装北斗

短报文终端，截至 2019 年，已累计向涉海用户推广近百万套北斗报警设备，显著提高海上遇险对象搜救效率，减少海上遇险伤亡人数。此外，短报文在电力抄表、水利统计、石油管网统计、大众市场等其他领域中也有很多应用，目前市场规模不大，但市场前景良好，正在持续发展和扩张中。2008 年汶川大地震中它的出色表现，在黄金时间抢救了无数人的生命，在应急救援的关键时刻肩负着保护人民生命财产安全的重任，是必不可少的北斗应用。

最近几年，随着华为 MATE 50、P60、MATE X3、nova 11 Ultra、中兴 Axon 50 Ultra 5G 手机、华为手表 Ultimate 非凡大师等集成北斗短报文“直连卫星”功能的产品的推出，北斗短报文或将成为高端系列产品的标配。北斗短报文技术与大众消费产品实现完美结合，代表着距离北斗短报文消费级产品进入“平民百姓家”的日子，已经不远了。

2.2.3 北斗短报文应用现状

北斗短报文是中国北斗卫星导航系统的特色功能，每次可以发送几十个汉字的数据内容，覆盖全中国全境，被广泛应用于野外、公网通信不畅通及通信传输数据量小等行业领域。下面将介绍北斗短报文常用的应用领域。

2.2.3.1 北斗短报文应用领域

1）交通运输

交通运输具有点多、线长和面广的特点，涉及时空基准信息实时性强、数量大、精度及可靠性要求高。北斗系统能提供实时导航、快速定位、精确授时、位置报告和短报文通信服务功能，与交通运输行业需求高度契合。因此，交通运输一直也是北斗系统应用最为重要的市场。采用北斗短报文的通信方式，即使在无线通信网络不能覆盖的偏远地区同样可以使用，能够及时得到信息指示，实现应急管控。

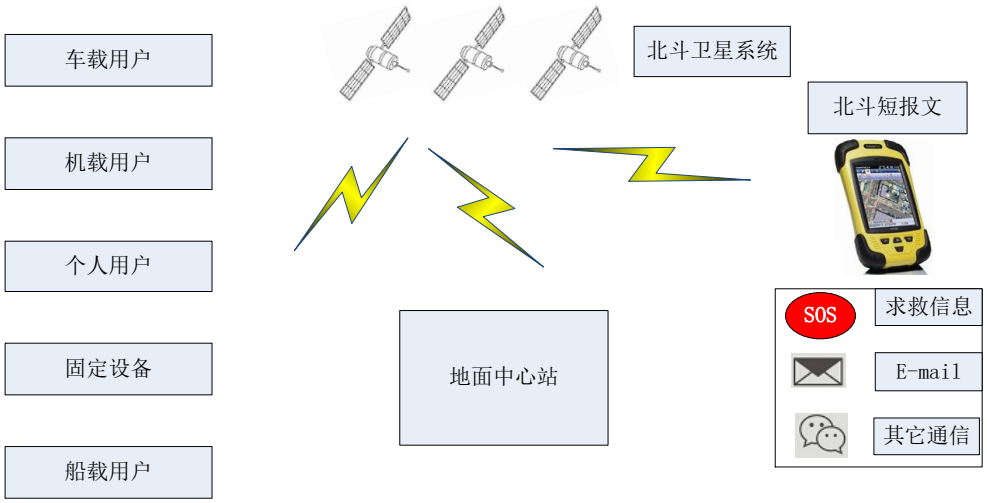


图 2-3 北斗短报文交通运输行业场景

在车载、机载、船载等用户上安装北斗定位终端，通过北斗短报文通信功能，在没有手机信号覆盖的地方，通过北斗手持机可以将车的位置信息及通信信息发送出去，使其他车获知当前情况。对于“两客一危”车载用户、船舶用户等监管有着十分重要的应用价值。

2）电力数据传输

目前很多电表数据都是自动采集，而我国一些偏远地区因为缺乏通信公网，所采集的数据无法传输回电力部门，必须派人上门人工采集，数据采集难度大，成本高。因此，使用自动抄表技术，配合北斗短报文传输手段，将数据传输到电力部门，可以解决此类问题。系统结构：北斗用电信息传输系统主要包含两大部分:北斗用电信息采集主站与采集终端，如图所示。主站端通过架设北斗多卡机群组成北斗收发通道，北斗前置服务器运行前置软件，提取出有效的应用层数据。通过这种结构实现现场设备与主站的互通互联，远程抄表与控制等一系列功能。

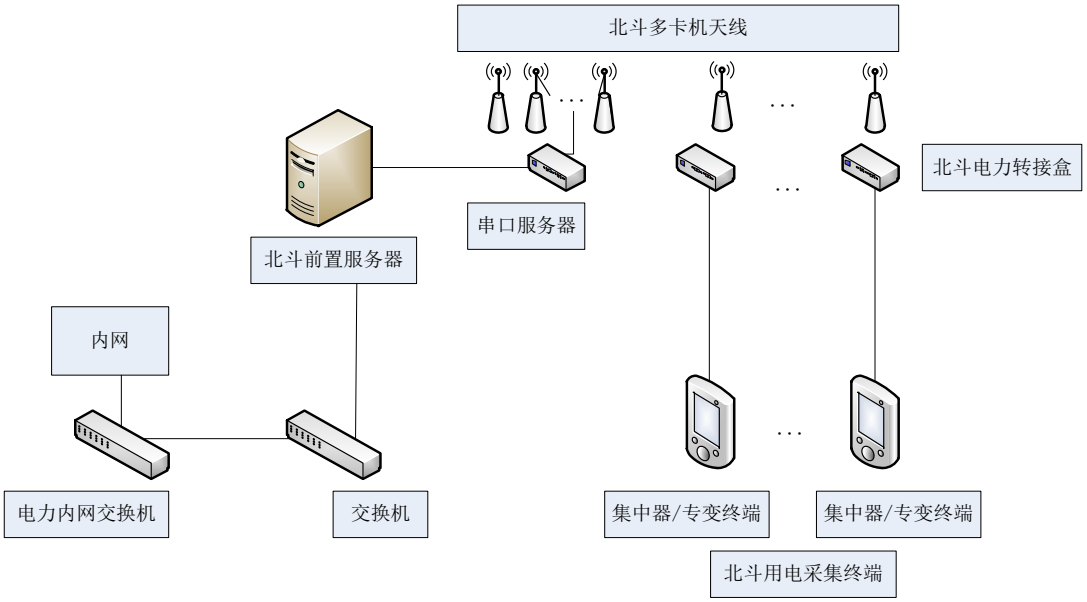


图 2-4　北斗用电信息安全传输场景

3）农业

北斗卫星导航技术结合遥感、地理信息等技术，使得传统农业向智慧农业加快发展，降低生产成本，提高劳动生产率，提高了劳动收益。由于，很多农场地处偏远，没有公共通信网络，因此使用北斗短报文功能进行通信。如下智慧放牧场景中，通过北斗短板文，获取牲畜的位置信息。

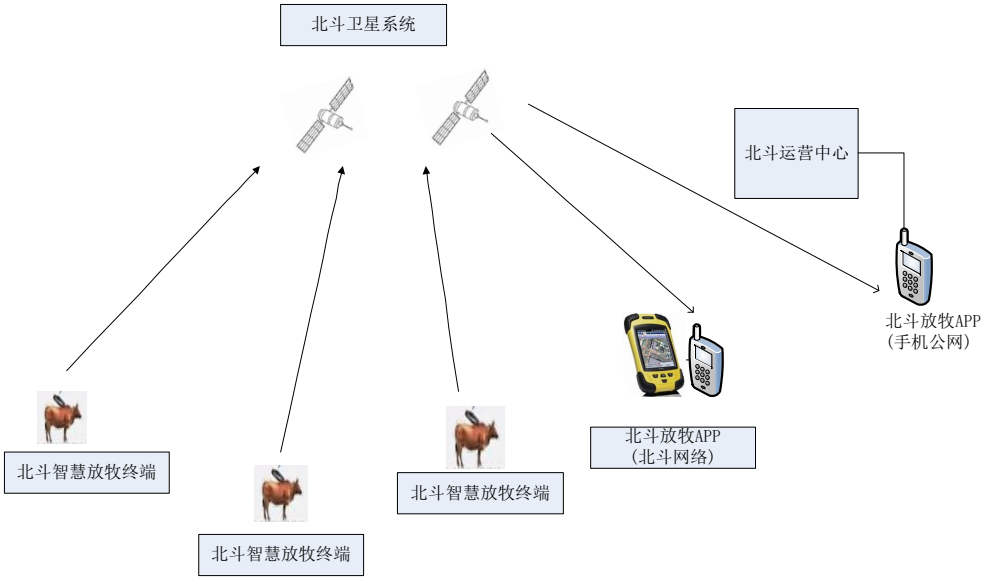


图 2-5　北斗智慧放牧的场景

4）远洋渔业

海洋的公网信号比陆地更弱，距海岸二三十海里后已经没有公网信号了。对于海洋气象的研究、渔船监管都需要数据传输通信，使用北斗短报文作为传输手段，可以极大地降低传输成本（其他卫星的成本非常高）。渔船上安装北斗终端，一方面可以通过该系统连接渔政部门，实现捕鱼作业监控，另一方面也为渔民提供应急通信手段，解决个人通信，紧急救援通信的问题。

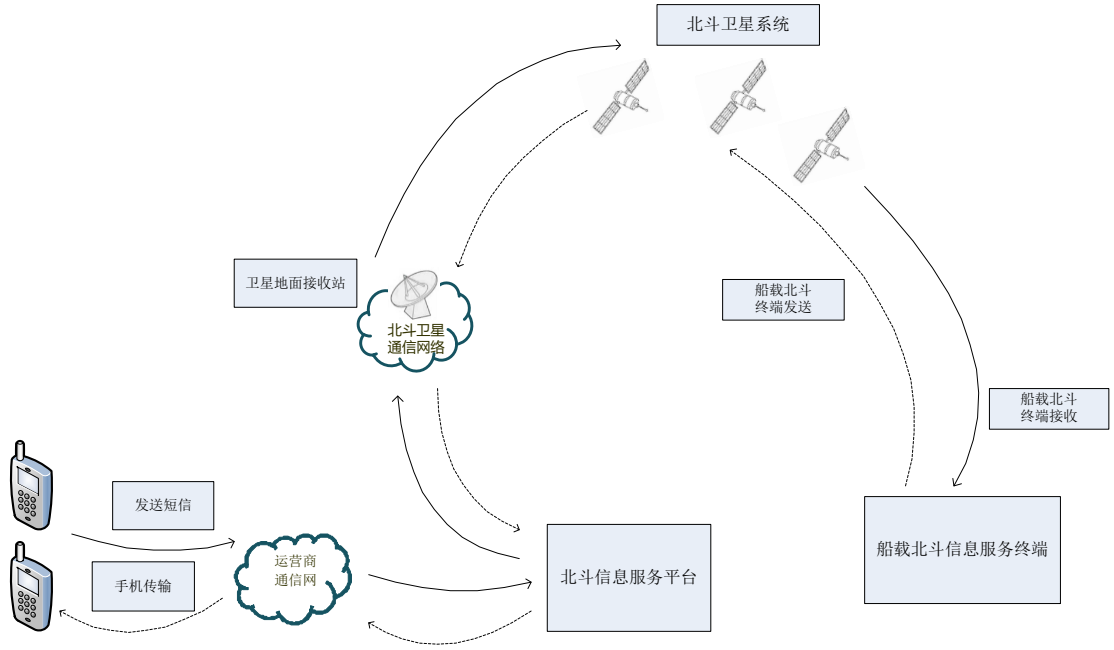


图 2-6　北斗短报文通信在海洋渔业的场景

5）环境监测

通过北斗卫星系统的短报文的通信功能对水利、桥梁、边坡等数据进行传输监测。下图为水利监测场景：

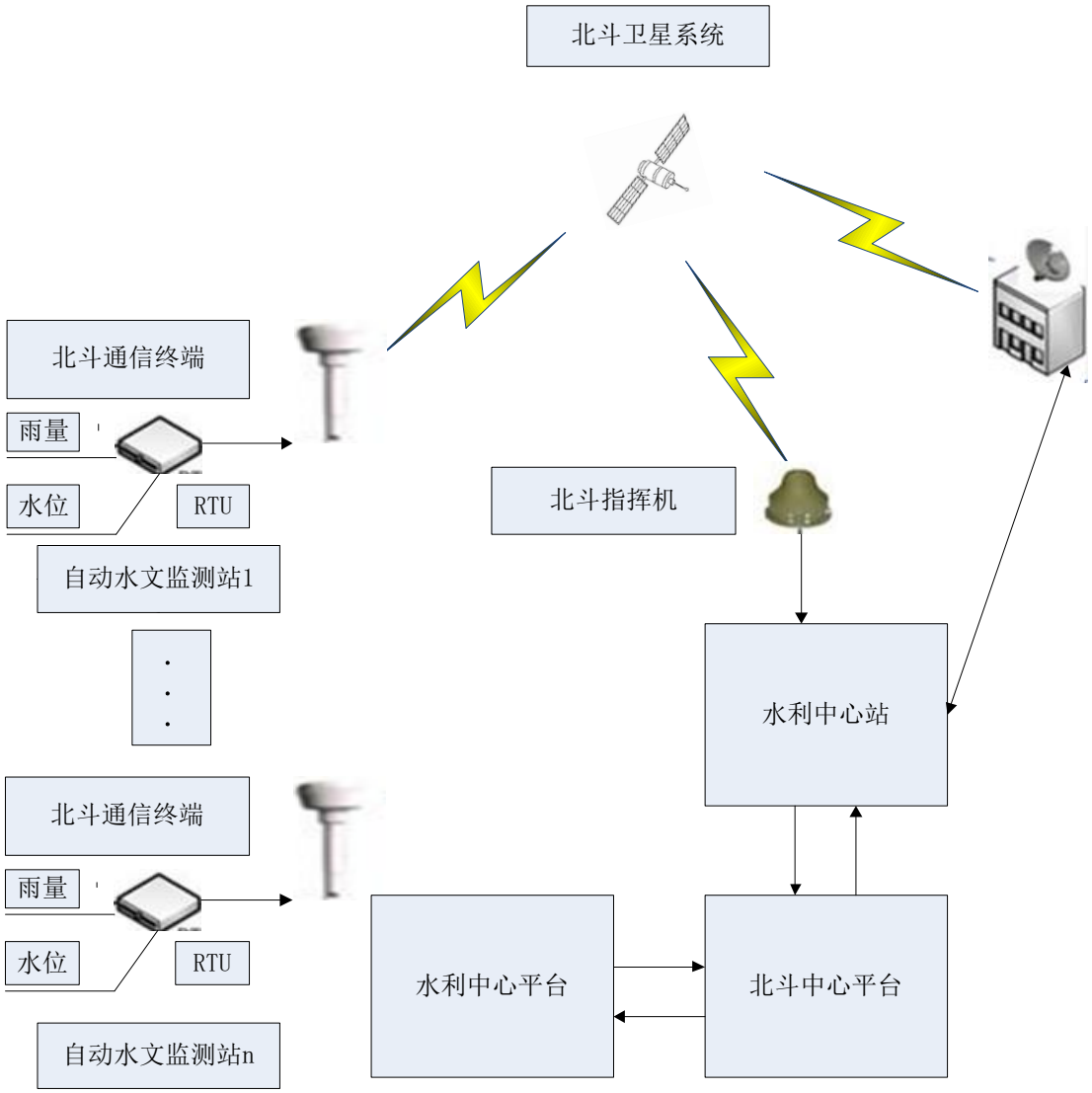


图 2-7　北斗短报文通信在水利监控的场景

6）应急救援

北斗应急救援系统由地面应急救援指挥中心、移动应急救援指挥分中心和应急救援单兵系统三部分组成。依托通信卫星及其他辅助通讯设备可实现图像、语音、相关数据的上传下发；依托北斗定位导航通讯卫星实现准确定位，基于北斗短报文的应急指挥与综合显示。

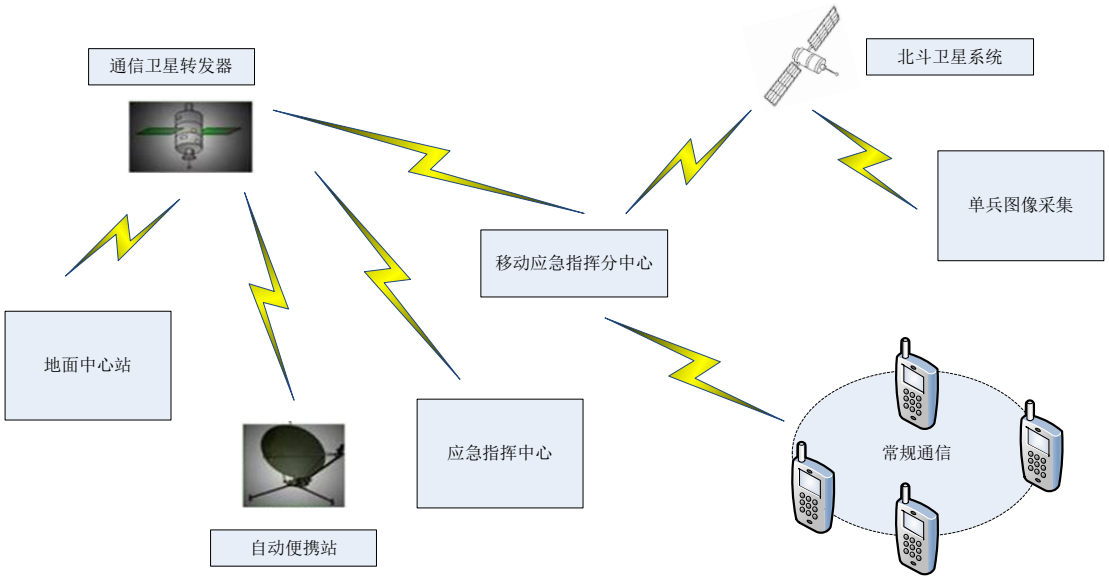


图 2-8　北斗短报文通信在应急救援场景

7）个人通信应用

野外作业人员、驴友等是经常出入在没有公网通信信号地区的人员，使用具有北斗芯片的手机依然可以和卫星通信，采用北斗短报文的通信功能，实现与外界的通信，告知家人自己在哪里，这对于户外生存、野外旅行等有十分重要的价值。

8）北斗三号短报文拓展更多应用场景

随着北斗卫星导航系统的不断完善和升级，北斗短报文技术也在不断发展创新。2020 年 7 月，我国北斗三号全球卫星导航系统正式建成，开始向全球开放。新一代北斗系统的短报文通信技术能力有了突破性的提升，相较于前两代，北斗三号短报文单次最长支持 1000 个汉字，系统容量达 1800 万次/小时，可实现语音、图片等内容的信息传输，进一步丰富了应用场景。

2.2.3.2　典型场景的安全问题

选择交通运输、应急救援、远洋渔业三个典型场景，分析短报文的应用情况及存在的安全问题。

在交通领域，北斗短报文的主要应用场景为“两客一危”车辆。“两客一危”车辆是指从事旅游的包车、三类以上班线客车和运输危险化学品、烟花爆竹、民用爆炸物品的道路专用车辆。北斗短报文在“两客一危”车辆中的应用场景如 2-9 所示。

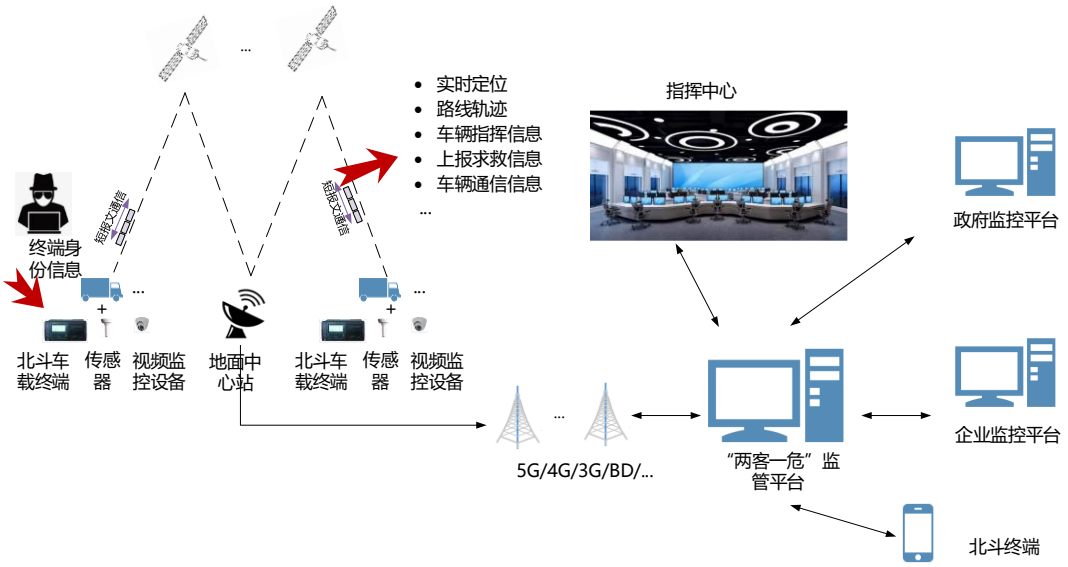


图 2-9　北斗短报文在“两客一危”应用场景

在“两客一危”的车辆中安装北斗车载终端、传感器及视频设备，将车辆位置信息、车辆运行状态及车与车间通信等信息即时上报“两客一危”的监管平台。通过监管平台，指挥中心、政府监控平台、企业监控平台及用户终端均可以获取车辆信息，便于对车辆状况进行实时监控。

通过对“两客一危”平台短报文业务流程的梳理，分析得到短报文在“两客一危”平台中面临的主要安全问题：

1) **北斗车载终端安全问题**：北斗车载终端以北斗卡做为它的唯一身份认证，但是这张卡未进行基于密码的保护，攻击者可以通过北斗通信协议（对外公开），模拟终端设备，接入到北斗应用网络中，对网络内的其他设备进行攻击，造成无法挽回的损失。

2) **短报文数据及应用安全**：“两客一危”车辆在运行过程中，会使用北斗车载终端发送车辆实时定位、路线轨迹、车间通信及车辆指挥等方面的数据，这些数据在通信过程中都存在着较大的安全风险。

   a) **车辆实时定位数据**：车辆在行进过程中，会通过短报文周期性地上报车辆实时位置信息，以便“两客一危”平台能够及时掌握各相关车辆的位置信息，进行统筹调度和安排。车辆定位信息为重要数据，尤其是运输危险品车辆的实时位置信息更属于敏感涉 M 信息，这些信息均为明文的形式进行传输，若在通信过程中短报文被非法截获，定位数据被泄露，相关车辆可能会遭到有预谋的抢劫、破坏，甚至是恐怖分子的袭击，这将对国家和人民的生命财产造成巨大的损失。

   b) **车辆路线轨迹数据**：攻击者可以截获短报文，得到车辆的出发地点、目的地点、汇合地点、行驶区间等轨迹信息，进而根据车辆运行趋势，推断出车辆的用途及行进计划，提前布局，扰乱车辆行驶秩序，实施抢劫破坏，造成大量损失。另一方面，车辆工作人员（如驾驶员）也可以非法控制车载终端，随意篡改轨迹信息，欺骗系统平台，进行破坏活动。

   c) **车辆指挥信息**：指挥中心可以通过短报文向车辆发送调度指令，如：车

队什么时候出发、车队行进规则、车队集合时间、突发事件通知（如：道路施工，绕道行驶等）。若此类信息被攻击者掌握，进行篡改和仿冒，并发布伪造信息给车辆，那么车辆的运行状态将无法控制，车辆可能会遭受各种安全问题，由此，给国家带来巨大损失。

d) **上报求救信息：**车辆或驾驶员出现突发事件时（如遭受抢劫、突遇恶劣天气、迷路等），可以通过车载终端上报求救信息，若此信息被攻击者篡改、破坏，这将极大影响救援的及时性和准确性，最终可能会决定救援的成效。

e) **车辆通信信息：**“两客一危”车辆往往组队行进，车辆之间会通过车载终端进行短报文通信（如：协商车队事宜等）。车辆之间的通信信息如果被破坏，将影响车辆的正常运营，降低运输效率，提高运营成本，给企业带来损失。

在应急救援应用场景中，用户携带单兵设备（北斗终端），在无网络覆盖的恶劣区域开展救援行为（抗震救灾、高山求助、荒漠救援等）。北斗短报文在应急救援的应用场景如 2-10 所示。

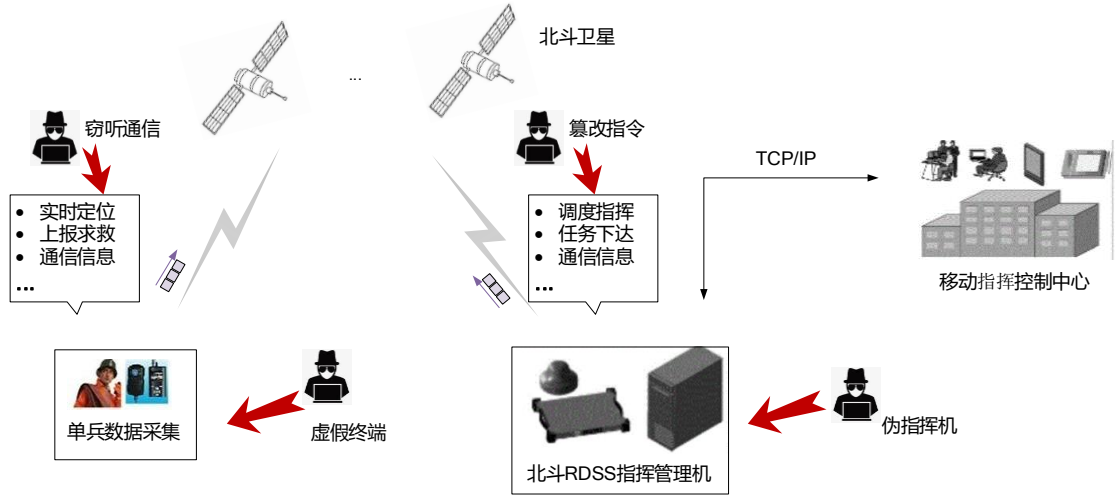


图 2-10　北斗短报文在应急救援应用场景

用户携带的单兵设备具备北斗短报文功能，能够进行通信和定位。单兵设备之间可以通过短报文相互通信，也可以向指挥管理机（北斗终端）上报定位信息、求救信息以及通信数据。指挥管理机通过 TCP/IP 网络与移动指挥中心相连，将指挥中心生成的指令通过短报文的形式向单兵设备分发，实现对单兵设备的指挥和控制。

通过对应急救援短报文业务流程的梳理，分析得到短报文在应急救援场景中面临的主要安全问题：

1) **伪造指挥机：**指挥管理机是具备管理能力的短报文终端。指挥管理机可以向下辖的所有单兵设备发送指令、下达任务，其重要性不言而喻。如果非法人员潜入系统，通过替换、仿冒、中间人攻击等方式实现伪指挥机，对单兵设备进行非法控制，必定造成系统的混乱，严重扰乱救援工作的开展。

2) **虚假终端：**一般而言，一个用户配备一个单兵设备。如果有攻击者使用其他北斗终端，模拟单兵设备，对指挥机实施欺骗，则可以顺利接收系统指令，知晓救援行动，并对其进行针对性的破坏。

3) **短报文数据及应用安全：**单兵设备会同管理指挥机上报实时定位数据，如果此类数据被泄露，参与救援的人员动向将会暴露，可能导致救援行动遭

受有预谋的破坏。管理指挥机向单兵设备分发任务、指挥调度，如果此类短报文数据被非法篡改，则可能导致行动失败甚至会影响施救人员自身的安全。在救援过程中，救援人员可以使用单兵设备进行远程通信、交互信息，这些信息中可能包含敏感数据，如果被监听，则行动内容可能会暴露，影响整个行动。

在远洋渔业应用场景中，渔船通过安装北斗船载终端，实现基于短报文的“船-船”通信，同时与北斗远洋渔业服务中心通信以实现求助、救援、指挥等功能。北斗短报文在远洋渔业的应用场景如 2-11 所示。

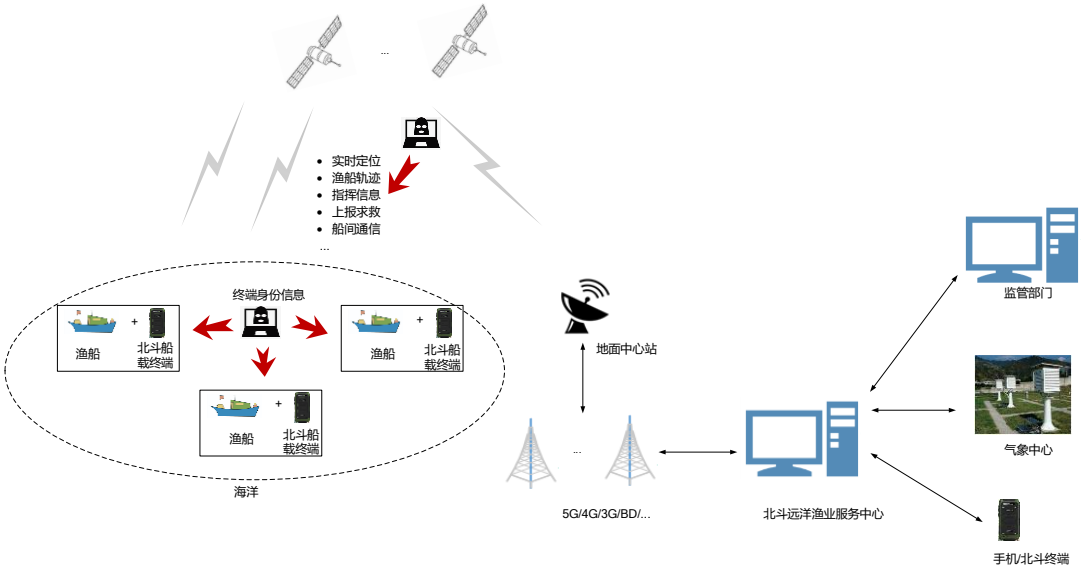


图 2-11　北斗短报文在远洋渔业应用场景

短报文在远洋渔业场景中面临的主要安全问题如下：

1) **渔船终端身份：**在我国，每一台出海远洋的渔船均要求配置北斗船载终端，以便在无信号覆盖的海域中保持通信。北斗船载终端使用北斗卡（北斗号码）标识身份，该信息易遭受篡改、仿冒。非法渔船通过身份仿冒的方式，伪造为合法渔船，在系统内保持通信，对业务造成影响。

2) **短报文数据及应用安全：**当渔船在涉及领土问题的海域中行进时，可能会遭受他国军事管制，此时短报文的定位功能便显得格外重要，它能够证明渔船的行动轨迹。如果此类数据被非法篡改，势必造成不必要的误会，甚至影响“国-国”的关系。当渔船遭遇恶劣天气、海盗袭击等突发事件时，可以通过短报文向远洋渔业服务中心求救，相关信息如果被篡改、破坏，将会造成巨大的人生财产损失。渔船可以以船队的形式，在一片海域协同作业，这个时候基于短报文的“船-船”通信就显得很有必要，如果相关信息被篡改、破坏，必将影响生产效率、工作成效。

2.2.4　标准化现状

国际卫星导航相关的标准：

1) Satellite Earth Stations and Systems (SES); Satellite Component of UMTS/IMT-2000; Multimedia Broadcast/Multicast Services; Part 2: Architecture and functional description TS 102 442-2

2) GEO-Mobile Radio Interface Specifications (Release 2); General

Packet Radio Service; Part 4: Radio interface protocol specifications; Sub-part 8: Mobile Radio Interface Layer 3 Specifications; GMPRS-1 04.008 V2.3.1 ETSI TS 101 376-4-8-2008

国内卫星导航相关的标准：

1) 北斗卫星导航术语 BD110001-2015
2) 北斗卫星导航系统短报文服务技术要求 （标准号未知）
3) 北斗一号民用数据采集终端设备技术要求和使用要求 JT/T591-2004
4) 北斗地基增强系统行业/区域数据中心入网技术要求 （标准号未知）
5) 北斗地基增强系统安全保密要求 （标准号未知）
6) 卫星定位船舶信息服务系统第 3 部分:信息安全规范 GB/T 30287.3-2013
7) 北斗一号民用车(船)载终端设备技术要求和使用要求 JT/T592-2004
8) 卫星定位个人位置信息服务系统 第 3 部分：信息安全规范 GB/T 29841.3-2013
9) GB/T 37937-2019《北斗卫星授时终端技术要求》
10) JT/T 766.1-2019《北斗卫星导航系统船载终端 第 1 部分：技术要求》

标准协调性分析：

北斗短报文是我国自主研发的北斗卫星导航系统所具备的独特功能，国外尚无与北斗短报文相关的标准作为参考。国内相关标准主要集中在北斗系统功能及技术要求、北斗系统应用规范要求等层面，暂无从密码技术层面对北斗短报文安全保障提出规范要求，影响北斗短报文在安全性要求较高的行业推广应用。

现有的短报文技术标准，虽然对短报文的服务质量和通信方法有所规范，但并未对短报文通信过程中的加密防护和安全认证需求进行明确，因此，有必要制定针对短报文安全通信的标准。现有的短报文行业应用标准，虽然针对车载、船用等场景提出了短报文终端的接入和使用方式，但是并没有对终端的安全管控、环境安全以及数据保护等方面的需求进行规定，因此，有必要制定针对短报文终端安全防护的标准。现有的短报文运营服务标准，虽然涉及了短报文服务的运营和数据流转，但在北斗系统与互联网融合应用趋势下，业务数据的安全保护需求并未得到满足，因此，有必要制定针对短报文数据应用的安全标准。

随着北斗系统及短报文应用越来越广泛，安全隐患突出，亟需制定北斗短报文密码技术应用相关标准。

2.3 发展趋势

北斗短报文是我国自主研发的北斗卫星所具备的独特功能，目前已覆盖全球，国外应用较少，国内北斗短报文在民用领域的应用不断拓展。在交通运输行业的“两客一危”车辆监控管理、远洋渔业通信、应急救援、电力监控及水文监测以等各个领域发挥着重要作用。

1) 技术发展趋势。

2018 年 12 月 27 日，北斗三号基本系统完成建设，开始提供全球服务。2019 年 12 月 16 日，北斗三号面向全球导航服务的最后一组 MEO 卫星——第 52、53 颗北斗导航卫星终于落子于北斗“大棋盘”的中圆地球轨道。至此，北斗三号在该轨道上规划的 24 颗卫星已全部到位，标志着全球系统核心星座部署完成，将为全球用户提供性能优异的导航服务，以及全球短报文通信、国际搜救等特色服务，以及覆盖中国和周边地区的星基增强和精密单点定位服务能力。而相较于其他三大卫星导航系

统，短报文通信服务是我国北斗三号卫星系统的独家秘笈。不仅可以授时定位，提供动态分米级、静态厘米级高精度服务，还具备“发短信”能力，且不限制信号区域，即使是无人区也能实现。在中国及周边地区，北斗三号单次报文长度可发送 1000 汉字，全球单次通信能力 40 汉字。短报文的通信的字节数的大幅增加，改善目前民用只有 78 字节数的容量，大大拓展北斗短报文的应用领域。

2）应用领域发展趋势。

随着北斗三号系统建成，北斗短报文单次通信能力提高，应用领域从国内发展到世界，行业应用范围更加广泛，带来社会经济价值的提高。在身份鉴别、数据的安全性、数据传输安全等各个方面，都存在安全防护需求，这将是北斗短报文通信民口应用在发展过程中需要发展和解决的问题。

3）安全应用发展趋势。

应用发展广泛，安全防护需求迫切，防护薄弱，安全体系研究尚未构建，针对此方面的安全研究是后期发展趋势；随着北斗的发展，商密算法在北斗短报文的应用处在试点阶段，需要发展标准体系研究，理论化指导北斗结合商密应用；通过发展北斗短报文技术产品设计、北斗+商密产业链整合，提高北斗短报文民用应用安全保障。北斗短报文通信与商密技术的结合将是北斗系统民口应用发展中非常重要的一个阶段。亟需规范北斗短报文通信中的商密技术应用，从顶层制定相关标准规范要求，填补北斗短报文通信在此方面的缺失，提高北斗短报文通信民口应用的安全。

3. 北斗短报文安全现状及密码技术研究

3.1 需求分析

3.1.1 北斗短报文应用情况分析

北斗短报文被广泛应用于传输数据量少、缺少公网通信的行业应用领域，如交通运输、渔业、石油、电力、水利、救援等。这些行业关系国计民生，一旦出现安全问题，势必影响国家安全及人民幸福。

北斗短报文终端往往安装于汽车、渔船、管道、指挥站等基础设施中。一旦短报文终端出现安全问题（如：非法攻破、非授权使用等），相关基础设施将面临安全风险，整个业务系统甚至都会遭到影响。

随着短报文在各行各业的深入应用，短报文数据安全问题日渐显现。比如，在交通运输行业，车辆以短报文的形式传递地理位置、指挥管控、异常上报等重要信息，实现车辆位置监控、车辆救援等功能，相关的定位控制数据一旦被截获，车辆的安全将无法保障；在远洋渔业，渔船通过短报文传递渔船位置、远洋求救等信息，其数据安全问题更是关乎渔民人生安全及国家主权安全；在能源行业，系统通过短报文传递电力抄表、石油管网等信息，相关数据直接反映消费账单、国家资产等信息，重要性不言而喻。此外，在大众消费领域，部分民用手机逐步支持短报文通信，个人隐私存在安全风险。

3.1.2 北斗短报文安全风险分析

通过对各行业北斗短报文应用现状及安全现状的梳理和分析，得出北斗短报文的安全风险主要体现在短报文终端安全及短报文通信安全两个方面。其中，短报文通信安全更是其安全痛点，需要重点研究。

3.1.2.1 终端安全隐患

终端不具备标识身份的唯一性，容易被人为更换。黑客通过模拟与软件平台的通信协议（对外公开），能够模拟采集设备，接入到北斗应用网络中，对网络内的其他设备进行攻击。

3.1.2.2 数据信息及传输过程的安全隐患

北斗短报文通信传输过程中，以明文的方式通过短报文的传输协议（对外公开）传输给地面中心，再由地面中心把报文信息传输给短报文接收端，这个过程中未做任何加密防护处理。这样将出现报文信息易被截获，定位等重要信息被泄露及接收方接收到的数据缺少真实性等严重的安全隐患。

1）数据篡改破坏

目前，民用北斗短报文在传输时未进行任何安全防护，这样易导致北斗短报文传输时遭受攻击。虽然北斗短报文自带“校验和”（该校验和是对短报文的主体部分进行异或所得），但这种完整性保护强度较弱，并不能防止对短报文电文内容的破坏和篡改。例如，发送端将电文内容以明文发送，短报文经广播后，敌手可截获短报文，并能对电文内容和校验和进行修改，然后敌手再伪装成发送端将修改的短报文广播发送。经卫星和地面中心站转发后，接收端对收到的短报文进行验证，此时校

验和能通过验证，但电文内容已被篡改，接收端对此并不知悉。最终导致接收端收到了错误的信息，或收到了无法解析的乱码。

2）数据重放攻击

短报文在传输过程中，被攻击者拦截并重发给北斗短报文接收设备，使得短报文通信系统被重放攻击。短报文终端设备接收到冗余信息，将会影响短报文通信业务的正常使用，造成短报文终端通信堵塞，严重时将导致系统被破坏。

3）敏感信息泄露

若短报文直接以明文传输电文内容，则敌手可截取广播的短报文，直接获得电文的原始信息。发送端发给特定接收端的电文内容已被敌手全部获得，一些重要敏感信息的泄露将会造成无法挽回的损失。

3.1.2.3 常见的攻击类型

攻击类型分为主动攻击和被动攻击，以下分别进行分析。

主动攻击：主动攻击会导致某些短报文数据的篡改和虚假短报文数据的产生。这类攻击可分为篡改、伪造消息数据和终端拒绝服务。重放攻击也属于主动攻击。重放攻击是指攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的。

被动攻击：被动攻击中攻击者不对短报文信息做任何修改，主要是通过窃听、流量分析等方式获取重要数据。针对这种攻击，可以通过数据加扰的方式来进行防御。

3.1.3 北斗短报文密码应用需求分析

为满足北斗短报文安全需求，需要深入研究北斗短报文密码应用需求，促进商密算法在北斗短报文的应用，北斗短报文密码应用需求体现在如下四个方面：

1） 机密性保护需求

机密性是密码对数据提供保护的重要功能之一。具体来说，机密性是不将有用信息泄漏给非授权用户的特性。可以通过信息加密、身份认证、访问控制、安全通信协议等技术实现，信息加密是防止信息非法泄露的最基本手段，主要强调有用信息只被授权对象使用的特征。在发送北斗短报文时，接受方都是特定的用户机，发送方可能会期望发送的信息只有目标机能获取，密码提供的数据机密性可以解决这个问题。

若短报文直接传输明文信息，则敌手窃听到短报文后，可以直接获得原始信息。如果采用密码技术对数据先加密，短报文传输的是原始信息的密文，此时，即使敌手窃听到了短报文消息，在没有密钥的情况下，其无法得到真实的原始信息，进而可以避免信息泄露带来的损失。

2）完整性保护需求

完整性是保护数据不受非授权改变的特性。完整性保护的目的是通过阻止威胁或探测威胁，保护可能遭到不同方式危害的数据的完整性和数据相关属性的完整性。许多开放系统应用都有依赖于数据完整性的安全需求。这类需求可以提供包括用于其它安全服务(如认证、访问控制、机密性、审计和不可否认性)中的数据完整性保护。对数据加密也可用于保证其完整性。假定被保护的数据项拥有一些冗余，加密传输冗余能保证数据完整性的效果，这就使得如果一个入侵者不知道加密的密钥而修改了密文的一部分，会导致在解密的过程中产生不正确的信息。

若短报文直接传输信息没有进行完整性保护，一方面，当传输发生错误时，短报文的接收者可能会解析出错误的误导信息；另一方面，敌手可对传输的信息进行

篡改或进行消息重放攻击，进而导致短报文的接收者解析出误导的信息。如果采用密码技术对数据进行完整性保护，则短报文的接收者可对不满足完整性的消息直接丢弃，进而避免上述情况的发生。

3）真实性保护需求

短报文终端通过唯一 ID 对设备进行标识，短报文终端存在被仿冒的风险，需要通过密码方式保证设备身份的真实性。民用短报文通信使用民用的北斗通信链路未做安全防护措施，没有通信回执，通过身份验证能增加对北斗短报文通信传输中发送者的身份信任，验证使用者的身份以及系统中信息的来源可靠性。

4）安全方案技术需求

短报文的传输模式有三种，汉字、代码以及混合传输模式，在前两种的模式中，对用户输入的内容有特定的要求（例如，在汉字模式下，若用户输入英文字符，则短报文无法发出）。目前，主流的传输模式都采用混合传输，即用户可同时输入汉字和英文字符。短报文传输选择不同的传输模式并不影响对短报文加解密算法的设计。

在 4.0 协议中，接口数据传输时电文内容以二进制格式表示，设计加解密算法时，明密文空间的字符内容无特定限制，仅有长度限制。

在 2.1 协议中，北斗终端将用户输入的内容编码为短报文规定的有效字符，有效字符为所有可印刷的 ASCII 字符(HEX20 到 HEX7F)，并去除一些预留字符(HEX24，HEX2A，HEX2C，HEX5C，HEX5E，HEX7E，HEX7F)。对短报文通信的内容进行加密时，考虑对现有北斗终端的工作模式尽可能降低影响，我们采用先加密后编码的方式，此时密文空间无限制，只需要保证加密后短报文的长度不超限。

目前，民用北斗卡采用的 4.0 协议和 2.1 协议均要求输入长度最长为 78 个字节（如 39 个汉字）。综上所述，安全方案需要满足以下特性：安全保护前后的短报文长度需满足不长于 78 个字节，保护后的短报文没有扩张或有极小长度的扩张。

在北斗短报文密码技术场景中，在北斗短报文终端设备中的密码实现，其供电由终端提供；密管中心的密码机、服务器由机房进行供电，不受电源的限制。采用北斗短报文传输通道实现密钥安全传输，无需配置额外的密码通信通道。民用北斗短报文采用分钟卡的频率发送报文，暂无延时的限制与约束。

北斗短报文密码技术需求内容如表 3-1 所示。

表 3-1　北斗短报文密码应用需求

密码应用	项	子项	密码技术需求
北斗短报文密码技术需求	短报文通信安全	短报文加密	使用加密技术，加密短报文数据，实现短报文内容的机密性保护。
		短报文完整性保护	使用完整性保护技术，对短报文数据进行完整性保护，防止短报文被非法篡改和破坏。
		短报文数据真实性验证	应当基于密码技术，对短报文发送端的身份进行显示或隐式的验证，防止非法终端发送伪冒短报文。
	短报文终端安全	终端身份安全	基于密码技术，对终端身份进行安全标识，防止终端伪造，防止针对终端的非法访问。
北斗短报文密码产品需求	为短报文终端配置国家密码管理局核准的安全芯片、密码软模块、密码中间件等密码产品。		

密码应用	项	子项	密码技术需求
北斗短报文密码支撑需求	密码算法		使用国家密码管理局批准的商用密码算法
	密码协议		使用国家密码管理局批准的基于商用密码算法的密码协议。
	密钥管理		使用国家密码管理局核准的密钥管理系统。
北斗短报文应用场景密码需求	电源供给、通道限制、延时要求的限制与约束		在北斗短报文密码技术场景中，北斗短报文终端设备中的密码实现，其供电由终端提供；密管中心的密码机、服务器由机房进行供电，不受电源的限制。采用北斗短报文传输通道实现密钥安全传输，无需配置额外的密码通信通道。按照北斗短报文民用通信频率，加、解密所需时间小于 1 分钟。

3.2 研究内容

基于北斗短报文应用场景及安全形势，研究北斗短报文密码应用技术，重点针对短报文通信安全问题，提出基于商用密码的北斗短报文密码应用方案。

3.3 主要难点

考虑到北斗短报文通信的独特性以及行业应用的发展趋势，研究和制定适用于北斗系统的短报文密码技术方案面临着以下挑战：

1) 北斗短报文终端民口应用采用分钟卡机制，单次通信频率为每分钟一次，且通信报文长度不超过 78 字节。当实施完整性保护性保护手段时，报文长度将会扩张，因而影响通信的效率，需要通过技术手段来减轻/规避这种影响。
2) 在不改变现有北斗短报文通信机制的状况下，密钥及证书的生命周期管理将显得非常困难。需要制定适合于短报文通信场景的密钥及证书管理方式。
3) 短报文应用领域较多，场景存在着差异性。在对短报文进行安全保障时，需要根据具体场景，实施不同的密码技术手段，但同时也需要遵循统一的密码技术框架。
4) 北斗系统发展，后期北斗短报文通信容量随之发生变化，密钥管理调随之需求调整等。
5) 其他技术问题：如果采用所有终端预置主密钥的方式，需要解决预置密钥的安全性问题，否则一台设备的密钥被泄露，所有终端都将面临被攻击的隐患；有些场景中，地面站可能需要参与加解密，此时，需要对地面站密码技术进行规定等等。

3.4 技术路线

1）以商用密码为技术手段，构建合规的安全体系。

根据密码应用合规性要求，本研究从算法、协议、模块、芯片、系统等全方位提供基于商用密码的技术保障，满足北斗短报文机密性、完整性、和（或）真实性的安全需求，确保短报文的应用安全。

2）以短报文通信为切入点，实现端到端安全防护。

系统性梳理短报文业务及资产，对短报文应用进行体系性安全防护，重点切入短报文通信传输，对短报文通信数据进行端到端的安全防护，灵活设计数据传输的机密性、完整性防护方案，保护重要、敏感的短报文数据在通信过程中的安全。

3）密码与短报文协议融合，充分结合短报文特点。

在广泛分析短报文业务特点和安全风险的基础上，本研究融合短报文通信技术，在保留短报文通信协议的基础上，构造基于商用密码的安全载荷，设计密管模式和报文保护方式，同时预留空间（扩展），满足短报文的发展规划。

3.5 解决方案

3.5.1 总体架构

北斗短报文通信加密总体架构遵照安全标准体系和安全管理体系，以密码基础和密码产品为支撑，为北斗短报文通信提供机密性、完整性和真实性的密码服务，建立短报文密码应用的保障体系。总体架构如图 3-1 所示：

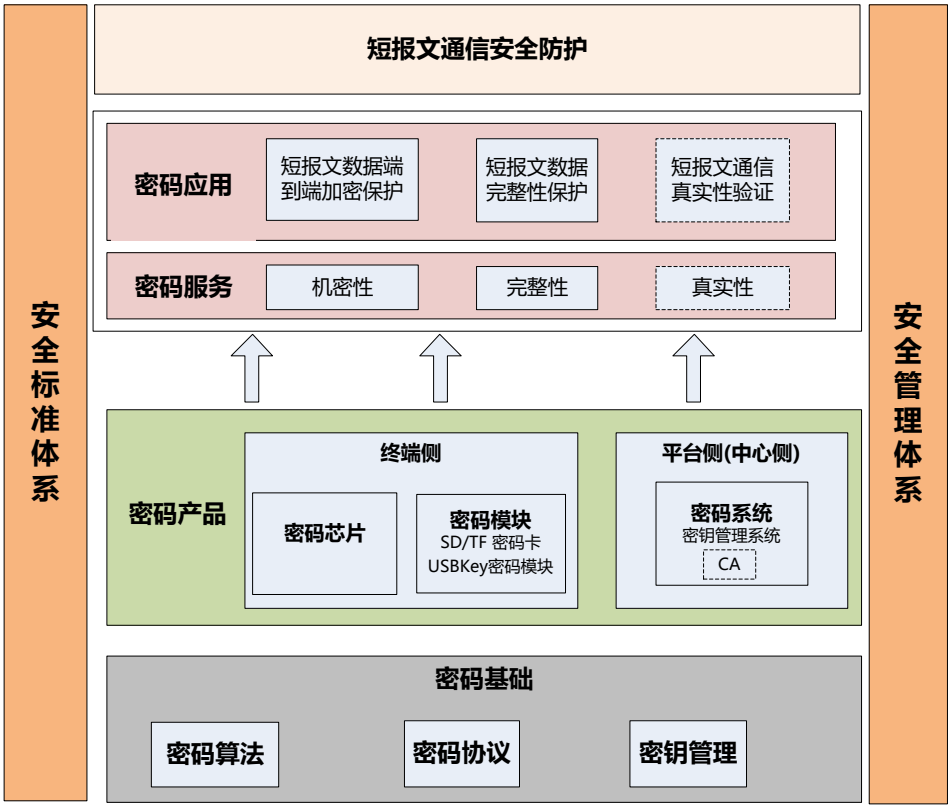


图 3-1　北斗短报文通信加密总体架构图

注：CA 及相应的真实性保护设为虚框，原因是受北斗民用分钟卡和传输字节的限制，采用非对称的方式不适应于大多数的短报文的通信场景，数字证书的应用作

为可选应用。

3.5.2 方案模型

针对北斗短报文通信加密，考虑三种技术体制：对称密码体制、非对称密码体制、标识密码体制。在对称密码体制中，使用对称密钥标识短报文终端身份，通过对称加密实现端到端的传输保护。在非对称密码体制中，使用数字证书标识短报文终端身份，通过对称加密实现端到端的传输保护。在标识密码体制中，使用设备标识表示短报文终端身份，通过对称加密实现端到端的传输保护。

目前，民用北斗短报文通信频次是 1 分钟 1 次，每次最多只能传输 78 个字节。若采用非对称密码体制，中间过程中需要传输证书及签名值，证书的大小往往超过 1000 字节，签名值的大小超过 100 字节，单个证书及签名值的传输将需要超过 10 次的短报文通信，这将极大的制约短报文通信。此外，非对称密码体制采用多次认证交互的方式，这将进一步增加协议通信数据量，极大地降低短报文传输数据的性能，影响短报文正常的业务发展。但是，随着北斗三号系统的建成，短报文数据传输量将大大提升，这时可以考虑采用非对称密码体制。

虽然标识密码在部分物联网场景、邮件系统、电子政务领域中有一定的应用，但其自身成熟度有限、应用模式还处于探索中，可以作为后续研究的方向。此外，标识密码还存在一些问题制约其应用：标识密码运算开销很大，对密码性能要求较高，影响行业用户应用效率；标识密码需要对私钥进行托管，存在私钥托管的安全问题，随着密管系统的规模变大，密管的级联也存在瓶颈。

本研究重点针对对称密码体制，提出适宜的加密方案。本研究重点考虑 SM4、SM3、ZUC 等算法及相关商密标准规定的算法模式。此外，一些新的对称密码算法及加密模式（如 GCM 模式），能提高对称加密的性能，可以应用在一些创新领域，本研究不逐一展开设计。

结合短报文通信特点，本研究提出四种对称加密方案模型。其中，方案模型 1 和 2 为地面中心站不参与加解密的情况，方案模型 3 和 4 需要地面中心站参与加解密（对地面中心站进行改造）。密管中心与北斗终端之间的通信采用卫星通信链路，通过北斗短报文来承载密钥管理的通信，无需设置额外的密钥传输通道。由于短报文长度限制，各类模型均应支持短报文加密策略可选。

在介绍 4 类方案模型前，首先介绍如下两种密钥的定义：

设备主密钥：为北斗终端预置的对称密钥，用于标识北斗终端身份，实现北斗终端与密管中心的通信认证、以及会话密钥的传输保护，不同于设备自身安全密钥体系的保护密钥。

会话密钥：为对称密钥，实现短报文数据的传输保护。

方案模型 1 命名为 E2EE-KA（End to End Encryption with Key Agreement，带有密钥协商的端到端加密），指的是地面中心站不参与加解密且无在线密管方案。

在北斗终端设备出厂时，将设备主密钥预置进设备中，身份唯一标识。当需要传输短报文时，北斗短报文收、发双端通过北斗短报文通信协商会话密钥，双方基于会话密钥进行端到端的加解密。方案中推荐使用硬件加密模块。E2EE-KA 的短报文加密通信过程如图 3-2 所示：

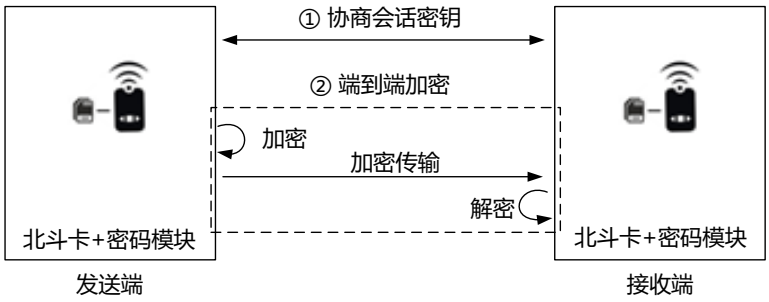


图 3-2　E2EE-KA 方案模型

方案模型 2 命名为 E2EE-CKM（End to End Encryption with Centralized Key Management，集中式密钥管理的端到端加密），指的是地面中心站不参与加解密但有在线密管方案。

密管产生设备主密钥，将其写入北斗终端设备，实现用户注册，并在需要时更新设备主密钥。密管中心产生会话密钥，将会话密钥安全分发给北斗终端设备。当需要传输短报文时，北斗短报文收、发双端基于会话密钥进行端到端的加解密。方案中推荐使用硬件加密模块。E2EE-CKM 的短报文加密通信过程如图 3-3 所示：

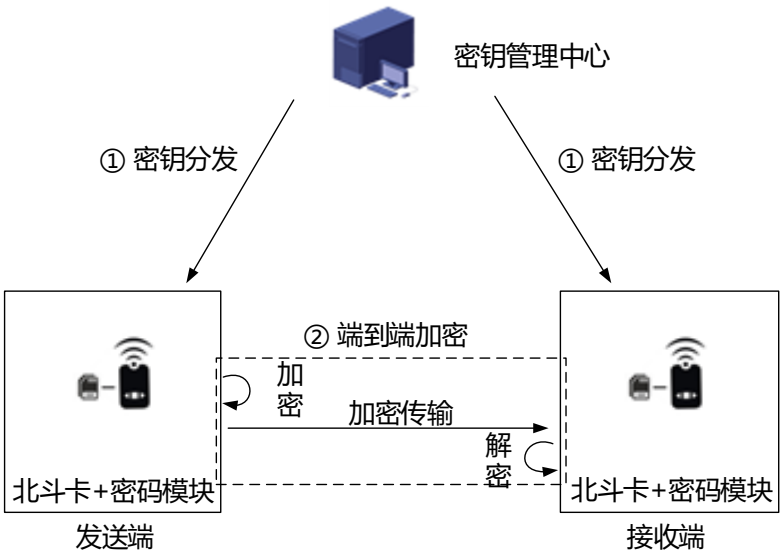


图 3-3　E2EE-CKM 方案模型

方案模型 3 命名为 GRE-KA（Ground Relay Encryption with Key Agreement，带有密钥协商的地面中转加密），指的是地面中心站参与加解密但无在线密管方案。

前面两种方案考虑的场景是地面中心站作为中转，不参与短报文通信过程中的加解密。若考虑地面中心站参与短报文通信过程中的加解密，在地面中心配备密码设备（如：密码机），地面中心的密码设备负责数据的转加密。在北斗终端设备出厂时，将设备主密钥预置进设备中，身份唯一标识。当需要传输短报文时，北斗短报文发、收端分别与地面中心通信协商双方共享的会话密钥；北斗短报文发端加密短报文并将其发送给地面中心；地面中心先解密短报文再重新加密短报文，并将短报

文发送给接收端；接收端解密短报文。方案中推荐使用硬件加密模块。GRE-KA 的短报文加密通信过程如图 3-4 所示：

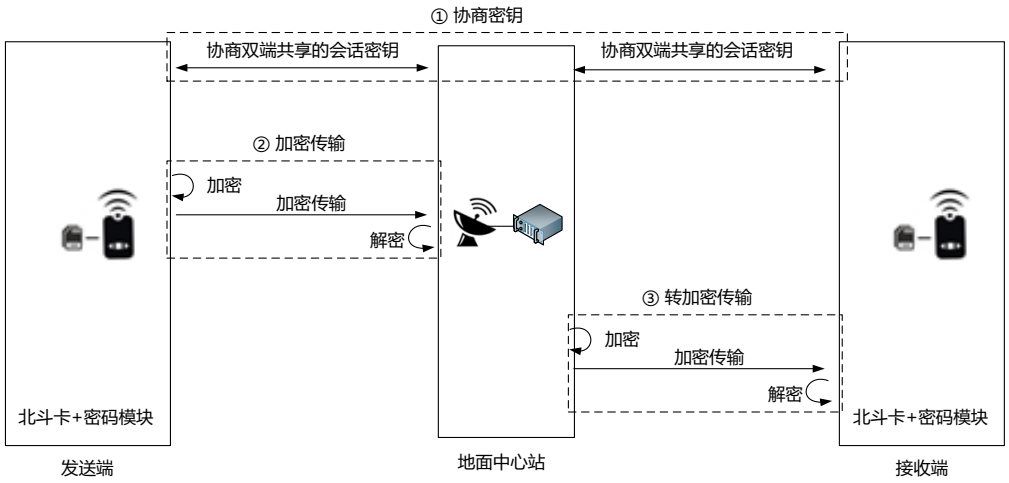


图 3-4　GRE-KA 方案模型

方案模型 4 命名为 GRE-CKM（Ground Relay Encryption with Centralized Key Management，集中式密钥管理的地面中转加密），指的是地面中心站参与加解密且有在线密管方案。

GRE-CKM 相较于 GRE-KA，增加了在线的密管中心。密管中心向发送端和地面中心站分发双端共享的会话密钥，同时密管中心向接收端和地面中心站分发双端共享的会话密钥。发送端对短报文进行加密，地面中心进行转加密后发送给接收端，接收端进行解密。方案中推荐使用硬件加密模块。GRE-CKM 的短报文加密通信过程如图 3-5 所示：

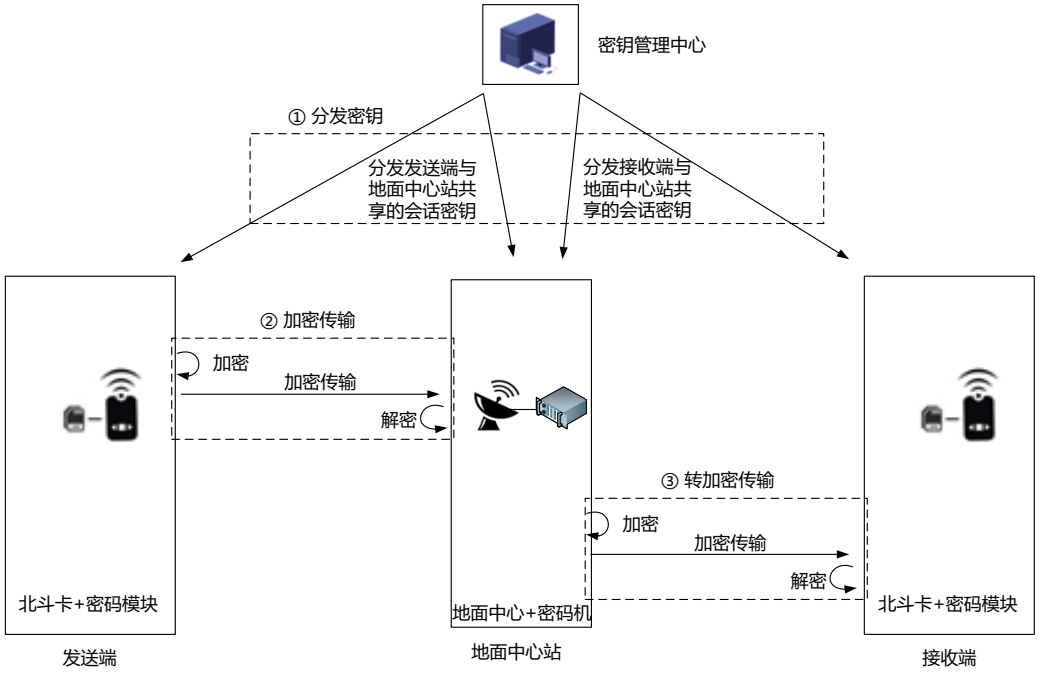


图 3-5　GRE-CKM 方案模型

3.5.3 对比分析

1）典型密码方案设计对比

下面描述4类方案的典型设计概要,通过4类方案的设计思想来进行对比分析。

方案 E2EE-KA：北斗终端出厂时预置相同的设备主密钥。北斗终端在短报文通信时,采用一次一密的方式,通过设备主密钥协商会话密钥并实现短报文通信保护。会话密钥的协商过程可采用通信双方发送密钥素材的形式实现。如 A 与 B 通信，A 产生随机数 Ra 并通过主密钥加密发送给 B,B 产生随机数 Rb 并通过主密钥加密发送给 A，最后通过 SM3（Ra||Rb||Ida||IDb）和截断方式得到双方共享的会话密钥。

方案 E2EE-CKM：附录 A 中描述了方案 E2EE-CKM 的一种具体实现细节。

方案 GRE-KA：北斗终端出厂时预置相同的设备主密钥，地面中心站也预置该主密钥。北斗终端在短报文通信时，采用一次一密的方式，一次通信包括两段加密流程。如 A 与 B 通信，C 为地面中心站。A 产生随机数 Ra 并通过主密钥加密发送给 C，C 产生随机数 Rc 并通过主密钥加密发送给 A，最后通过 SM3（Ra||Rc||Ida||IDc）和截断方式得到双方共享的会话密钥,A 通过该会话密钥将短报文加密后发送给 C,C 通过该会话密钥将短报文解密。C 产生随机数 Rc’并通过主密钥加密发送给 B，B 产生随机数 Rb 并通过主密钥加密发送给 C，最后通过 SM3（Rc’||Rb||Idc||IDb）和截断方式得到双方共享的会话密钥,C 通过该会话密钥将短报文加密后发送给 B。

方案 GRE-CKM：北斗终端、地面中心站均预置各不相同的设备主密钥。密管中心向北斗终端、地面中心站分别下发发端会话密钥 k1 及收端会话密钥 k2。如 A 与 B 通信、C 为地面中心站。A 使用 k1 加密短报文，发送给 C；C 使用 k1 解密短报文，再使用 k2 加密短报文，并发送给 B；B 使用 k2 解密短报文。通常，此类方式每隔一段时间（如 1 个月）更新会话密钥，而不再采用一次一密。

从方案设计层面考虑，方案 E2EE-CKM 与方案 GRE-CKM 在主密钥安全层面具有安全性优势。方案 E2EE-KA、GRE-KA 中的北斗短报文终端采用相同的设备主密钥，一旦密钥泄露，安全风险将会全网蔓延，存在着相当的安全隐患；方案 E2EE-CKM 与方案 GRE-CKM 中，不同北斗短报文终端采用不同的设备主密钥，安全性更好。此外，方案 E2EE-CKM 与方案 GRE-CKM 中，由密管中心分发密钥，无需在每次通信前交互密钥信息，能够减少通信开销，这对于分钟级的短报文通信而言，具备很好的现实意义。综上，方案 E2EE-CKM 与方案 GRE-CKM 具备方案设计层面的优势。

2）综合对比

基于以上四种北斗短报文加密通信方案，下面从安全能力、应用规模、改造难度、适用场景等方面对这四种方案模型进行对比分析，见表 3-2 所示：

表 3-2　短报文加密通信方案对比分析表

项目	E2EE-KA	E2EE-CKM	GRE-KA	GRE-CKM
安全能力	一般。 预置主密钥，密钥一旦泄露，全网终端都存在安全隐患。	高。 通过密管中心安全分发主密钥和会话密钥，有效降低密钥风险。	一般。 预置主密钥，密钥一旦泄露，全网终端都存在安全隐患。	非常高。 通过密管中心安全分发主密钥和会话密钥，有效降低密钥风险。
应用规模	中小规模局部范围使用。 系统规模增大将降低整体的安全	中大规模范围内使用。 可以合理设计密钥机制，确保系	中等规模范围内使用。 系统规模的增大，将会增加地面中	中小规模范围内使用。 鉴于密管需要频繁地与收端、发端、地

项目	E2EE-KA	E2EE-CKM	GRE-KA	GRE-CKM
	性。	统规模的增大不会明显影响系统的安全性。	心站的加解密压力。	面中心交互信息，系统规模的增大会显著增加密管压力，进而限制系统规模。
改造难度	容易。 只需要改造北斗短报文终端。	适中。 需要改造北斗短报文终端。需要增加密钥管理中心。需要设计密管中心与短报文终端间的通信。	较高。 需要改造北斗短报文终端和地面中心。需要更改地面中心的业务逻辑。	很高。 需要改造北斗短报文终端、地面中心。需要更改地面中心的业务逻辑。需要设计密管中心与短报文终端、地面中心间的通信。
适用场景	对安全性要求较低的小规模组织，如：户外驴友团组、小型科研组织、行业用户的分支机构。	传统的交通、渔业、救援、水利等大多数行业领域。	对安全性要求适中的普通领域，如大众用户、水利统计等。	对安全性要求较高且有集中管理需求的专用领域。如：某行业用户的保密机构、涉及国土安全的组织机构等。

从场景覆盖范围、实践改造难度、应用规模等方面来看，综合得出方案模型 E2EE-CKM 目前为最适合的北斗短报文加密通用方案，具备最高的普适应用性。因此，本研究将基于模型 E2EE-CKM 的加密方式，提出基于商用密码的北斗短报文加密通信方案。具体方案实现参见附录 A。

4. 通用模型研究

4.1 研究概述

本章将基于第三章所提 E2EE-CKM 方案及应用场景，提炼出其中的安全需求、加密模型、密码应用技术框架，形成规范性要求，对采用 E2EE-CKM 类似方案的密码应用工作提供必要的参考和指导。

4.2 安全需求分析

4.2.1 北斗短报文通信

短报文发送和接收端通过出站、入站链路形成一个 M 型的通信机制。短报文发送端将生成的短报文发送给卫星，卫星收到短报文后通过卫星链路发送给地面中心站；地面中心站收到信息后将短报文通过卫星链路转发给短报文接收端；即完成一次完整的短报文通信过程。

北斗短报文通信过程涉及北斗终端、北斗用户、北斗终端管理员，相应的业务模型如图 4-1 所示：

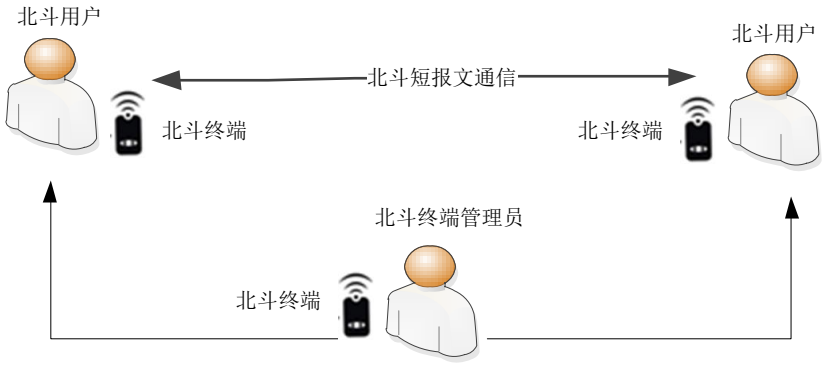


图 4-1　北斗短报文通信业务模型图

北斗终端：利用北斗卫星导航系统进行定位及导航的终端设备。如：北斗手持机（类似于手机）、北斗车载或机载终端。

北斗用户：使用北斗终端在发送端、接收端进行短报文通信的用户。按照应用场景，北斗用户短报文的通信类型包括：业务报文、管理报文、监测报文。

北斗终端管理员：对北斗终端、北斗用户等信息进行增、删、改、查等管理的人员。

4.2.2 北斗短报文通信安全需求

北斗短报文通信在北斗终端设备、数据传输过程等方面存在如下安全需求：

1) 北斗终端设备身份认证需求：北斗终端通过北斗卡号进行唯一标识，缺乏基于密码技术的身份标识。
2) 短报文数据传输的机密性需求：保障短报文传输过程中的安全，防止传输的敏感信息在传输过程中被非法窃取。
3) 短报文数据传输的完整性需求：保障短报文信息的完整性，确保发送端和接收端通信的短报文信息是完全一致的，防止被非法篡改。
4) 短报文数据传输真实性需求：确保发送端是真实用户、可被验证和信任。
5) 支持加密群组划分，满足短报文群内加密通信、临时跨群加密通信的安全需求。

4.3 加密通用模型

对北斗短报文通信加密分群内和跨群两种通信场景，加密模型如图 4-2 所示：

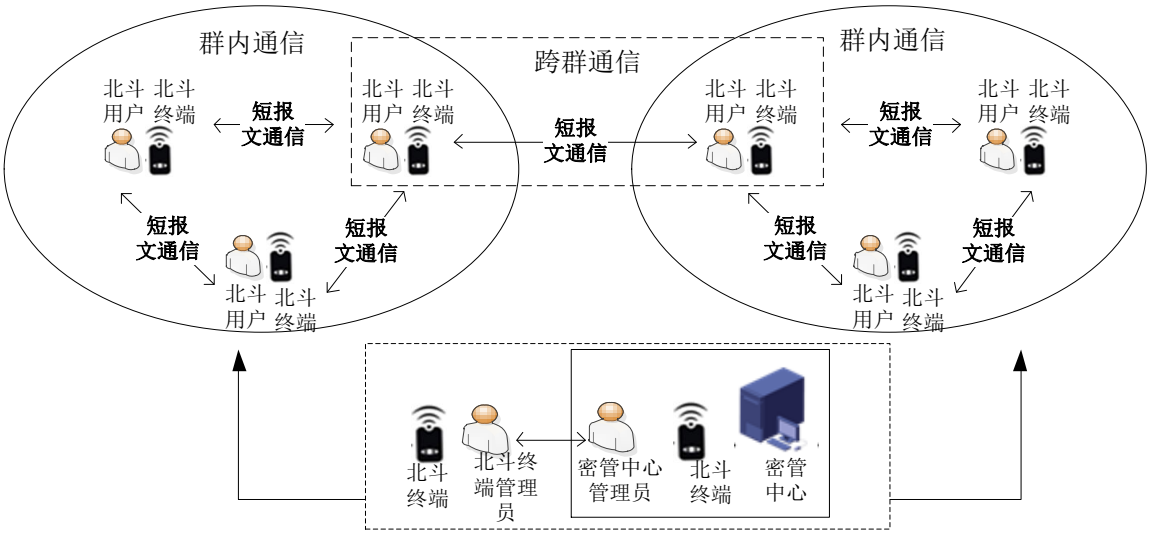


图 4-2 北斗短报文通信加密模型

北斗短报文通信加密模型，在原有业务的基础上，加强北斗短报文通信安全，进行加密群组划分，主要分为两种类型：同一组织机构中的北斗终端进行群内加密通信；不同群的用户临时组建的新的群组进行临时跨群加密通信。如果同一群内不同成员存在着独立的加密通信需求（如 P2P、TCT 等），可建立临时跨群加密机制。

建立密管中心，设置密管中心管理员。密管中心管理员：主要是对北斗终端设备信息及变更信息录入；对北斗终端设备密钥生命周期管理。

北斗终端管理员增加对群组新建、变更、撤销等管理工作。

北斗终端管理员与密管中管理员间的交互主要包括：北斗终端管理员上报北斗终端用户的信息变更、群组信息变更及新建群组密钥申请；密管中心管理员对北斗终端管理员上报信息的响应等工作。

在大规模的北斗短报文应用中，部署多套密管中心，实现密管的级联，对所有北斗终端进行统一管理。密管中心级联可采用两层架构，上层为密管总中心，下层为各个区域/行业的密管分中心。密管分中心之间建立安全通道，实现密钥的安全查询。密管总中心与密管分中心之间，可通过在线或离线的方式实现密钥的安全同步、

备份、归档等过程。如果密管分中心间存在密钥的同步、申请等需求时，密管分中心应当与密管总中心通信，由密管总中心负责全网密钥的管理。

4.4 密码应用技术框架

北斗短报文加、解密及群组管理等应用层的安全可通过北斗短报文密码应用技术框架提供密码支撑。北斗短报文密码应用技术框架示意图，如图 4-3 所示：

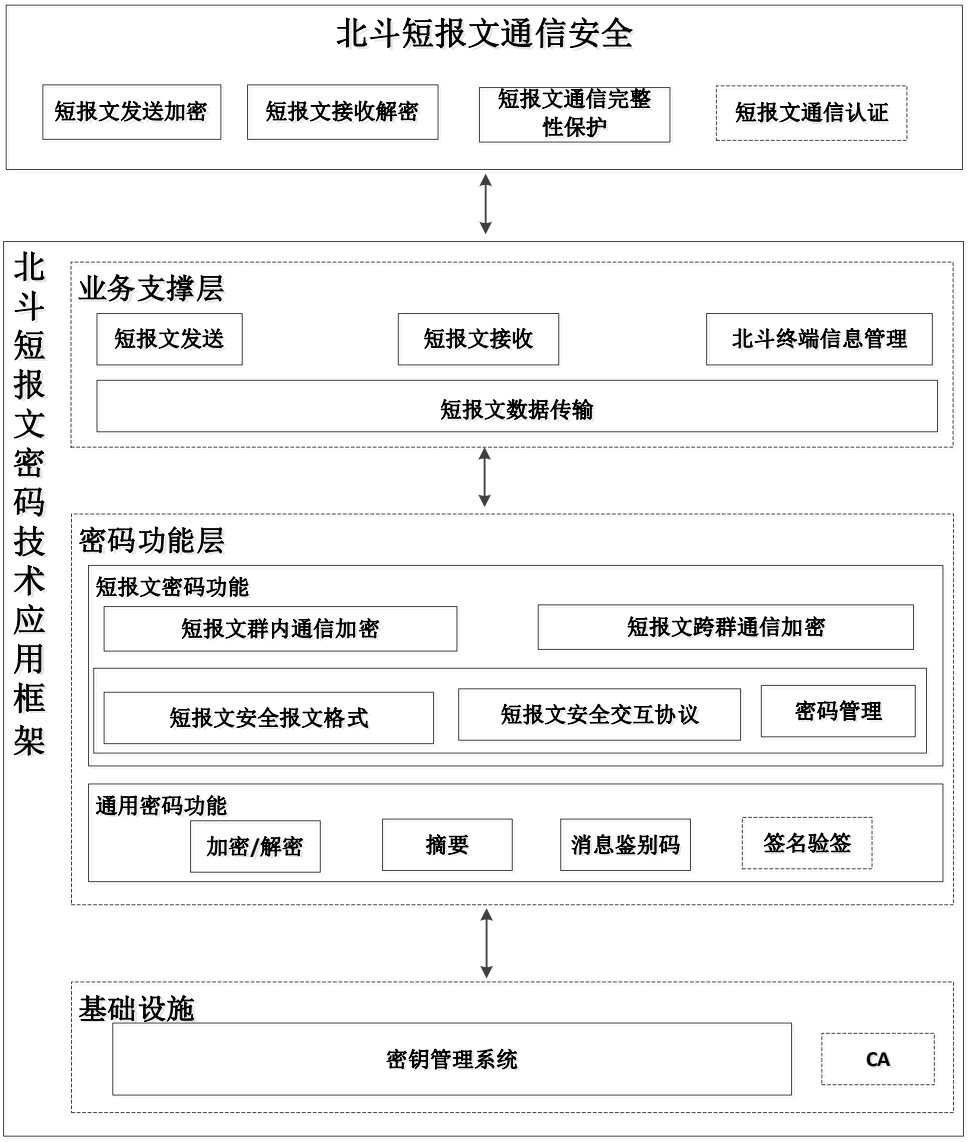


图4-3　短报文密码应用技术框架图

北斗短报文密码技术应用框架由业务支撑层、密码功能层和基础设施层构成。

业务支撑层：北斗短报文业务支撑层，涉及北斗短报文数据及主要管理过程，包括短报文发送、短报文接收及北斗终端信息管理等环节，通过调用密码功能层实现安全的发送和接收短报文管理。

密码功能层：包括通用密码功能和短报文密码功能两部分。

通用密码功能：基于密码基础设施及设备，提供通用密码功能，如下：

1） 加密/解密：用于信息加密保护；
2） 摘要：实现信息的完整性保护；
3） 消息鉴别码：鉴别消息的完整性；
4） 签名验签：保证操作行为的不可否认性，数据真实性、完整性。

短报文密码功能：基于通用密码功能，提供短报文通信的加密的能力。

1） 短报文群内通信加密：同一群组的北斗短报文终端通信加密；
2） 短报文跨群通信加密：不同群的北斗短报文终端通信加密；
3） 短报文安全报文格式：在北斗短报文的报文格式中添加安全设置的字段，形成短报文安全报文格式；
4） 短报文安全交互协议：在短报文的报文格式中添加密钥安全通道等协议；
5） 密钥管理：实现密钥的生成、分发、更新、销毁等的生命周期安全管理。

基础设施层：密钥管理系统，对密钥生命周期进行管理； CA（可选），当系统需要数字证书时，对证书进行签发及管理。

4.4.1 短报文通信过程中的密码应用要求

4.4.1.1 初始化

采用主密钥标识短报文终端身份，采用会话密钥对短报文通信数据进行安全保护。

从安全角度考虑，主密钥（MK）采用离线预置的方式；根据北斗短报文应用实际业务场景情况，会话密钥（SK）可采用在线或离线的方式。离线和在线密钥注入的方式如下：

离线方式：

包括两种模式：当系统规模适中或较小的时候，可以采用密管中统一注入密钥的方式；当系统规模较大或系统分散的情况时，可以采用密管中心授权北斗终端厂商由它生产的过程中实现密钥的注入。

在线方式：

北斗终端出厂后，由密管中心通过主密钥加密会话密钥的方式实现会话密钥的安全在线分发。

4.4.1.2 群内通信

密管中心管理员按照不同单位的北斗终端设备建立不同群组后，群内通信应满足以下要求：

1） 检查群内的终端设备，能否进行加密通信；
2） 应使用加密保护措施实现传输中短报文信息的机密性；
3） 应使用MAC验证方式实现传输中短报文信息的完整性；
4） 应使用带密钥的MAC运算等身份鉴别方式来确保数据来源的真实性。

4.4.1.3 跨群通信

跨群通信，应满足以下要求：

1） 北斗终端管理员上报临时跨群终端信息及新密钥申请，密管中心管理员根据上报信息进行响应；
2） 检查新群内的终端设备，能否进行加密通信；
3） 应使用加密保护措施实现传输中短报文信息的机密性；
4） 应使用MAC验证方式实现传输中短报文信息的完整性；

5） 应使用带密钥的MAC运算等身份鉴别方式手段确保数据来源的真实性。

4.4.1.4 系统管理

在北斗短报文通信过程中，**北斗终端管理员对北斗终端管理，**要求如下：

1） 北斗终端基本信息管理：新增、更改、查询、删除；
2） 群组管理：新建、变更、撤销；
3） 跨群群组管理：新建、变更、撤销。

在北斗短报文通信过程中，**密管中心对于北斗终端管理，**要求如下：

1） 密管中心管理员将北斗终端信息准确无误的录入到密管中心管理系统中，若后期终端信息、群组信息发生变化，北斗终端管理员应及时上报密管中心管理员进行更新；
2） 密管中心下发通知出现通讯异常时，在北斗终端基本信息中找到相应的北斗终端管理员联系方式，进行联系并处理。

在北斗短报文通信过程中，**密管中心对于密钥管理**，要求如下：

1） 对终端密钥的初始化；
2） 密钥临期的更新；
3） 密钥到期的销毁；
4） 临时会话密钥的生成、分发、更新、销毁等密钥生命周期管理。

4.4.2 短报文密码技术要求

4.4.2.1 密码算法要求

北斗短报文中使用的密码算法，应采用国家密码管理主管部门批准的算法。杂凑算法应采用SM3算法，遵循GB/T32905。数据加解密应采用SM4分组算法、ZUC序列密码算法或SM7分组算法，其中SM4分组算法遵循GB/T 32907、ZUC序列密码算法遵循GB/T 33133.1-2016。消息鉴别码应遵循GB/T15852。

4.4.2.2 密码设备要求

北斗短报文中使用的密码设备，如：密码机、安全芯片、软模块等，应遵循相关密码国家标准和行业标准，并通过商用密码检测认证机构的认证。

4.4.2.3 密钥管理

每个北斗终端中的主密钥是唯一的，由密管中心生成，出厂时预置到北斗终端中。密管中心生成会话密钥，密管中心安全地向北斗终端分发会话密钥。北斗终端安全使用密钥。所有密钥，所有密钥应使用通过商用密码检测认证机构认证的密码设备对密钥的生成、分发、更新、销毁等环节实现安全管理。

4.4.2.4 协议交互

在北斗短报文有效载荷内，设置数据传输通道提供时间或序列号等协议数据，防止重放攻击。技术上采用对称加密算法，杂凑算法生成消息鉴别码，确保北斗终端间短报文数据传输过程中的机密性、完整性和真实性。

在北斗短报文有效载荷内，设置密钥管理通道，提供时间或序列号等协议数据，防止重放攻击，实现密管中心与北斗终端间的安全通信，实现密钥分发、更新、销毁等密钥生命周期进行管理，所用密码算法，应遵循相关密码国家标准和行业标准。

协议交互参考附录A.4。

4.5 安全性分析

4.5.1 初始化安全分析

北斗终端在生产时，已配置具备安全功能的密码模块（符合要求的密码软模块或硬件密码模块）；对密码模块进行功性能测试，保证密码功能的正确性、安全性、合规性；对密码模块进行清零设置，避免无效密钥、数据信息残留。

主密钥通过离线的方式实现安全注入，会话密钥通过离线或在线的方式实现安全注入。北斗终端出厂后，由北斗终端管理员将其安全地配送到密管中心，并交由专门的密管中心管理员对北斗终端进行初始化。密管中心管理员严格遵守管理章程，根据实际需求，分别向不同北斗终端灌装不同的密钥，相应密钥被安全地存储于北斗终端的密码模块内部。密管中心对厂商授权，由厂商在生产北斗终端的过程中，进行密钥的安全注入。此外，还可以考虑建立安全通道安全传输密钥、使用安全代理安全分发密钥等方式，在线注入密钥实现北斗终端密钥的初始化。

整个密钥初始化的过程严格遵循国家密码相关管理规范，密钥应使用通过商用密码检测认证机构认证的密码设备产生，并被安全地灌装到北斗终端内部。通过对初始化过程的安全管理，可以确保整个初始化的安全。

4.5.2 密钥生命周期安全分析

采用技术与管理相结合的方式，确保密钥从生成、分发、更新、销毁等整个生命周期的安全。一方面，建立符合要求的密管中心，使用通过商用密码检测认证机构认证的密码设备产生和管理密钥，从技术层面确保密钥的安全。另一方面，通过对密钥管理过程进行安全控制、监督，保证密钥管理操作行为的安全。

系统遵循“专钥专用”原则，在安全实用的原则下来控制密钥的使用权限，保证密钥安全使用。

4.5.3 分组建群安全性分析

对短报文通信场景进行抽象，梳理出群内通信和跨群通信两类模型。

群组划分的依据可以是同一组织机构、同一应用领域、同一身份属性的用户。同一个群组，使用相同的密钥及安全策略。群组外的成员没有群组的通信密钥，即时通信数据被其非法截获，也无法解开通信内容，有效保证群组内部短报文通信的安全。

在某些情况下，不同群组的用户存在短报文临时通信需求。此时，管理员为此类终端用户建立临时通信群，并分配临时密钥，保证短报文临时通信的安全。一旦通信结束，临时群解散，密钥失效。通过临时群生命周期的管理，有效防止临时密钥长期使用带来的安全风险，同时也可以避免非法的跨群通信。

使用密钥对不同群组的通信进行区分和隔离，能够有效防止短报文通信信息被泄露，保障通信过程的安全。

4.5.4 协议交互安全性分析

设置数据传输通道和密钥管理通道，分别承载数据面和管理面的信息。通过通道区分的方式，确保不同平面信息的隔离性，降低安全风险跨信息平面蔓延和传播的可能。

建立数据传输通道，使用符合商用密码标准要求的对称加密算法、杂凑算法，

对短报文数据进行机密性、完整性、真实性保护，有效防止对短报文通信数据的泄露及恶意篡改。通过 SM4 算法对北斗短报文消息载荷进行加密，实现对短报文消息载荷的机密性保护；在短报文消息内增加时间戳/序号、设备 ID 等字段并对所有数据 SM3_HMAC 运算实现短报文数据完整性保护，并实现隐式真实性保护；随着规模变大，还可以采用非对称的签名的方式，进行身份认证，实现数据的真实性保护；此外，通过密钥的安全管理确保密钥的使用是安全的。

建立密钥管理通道，对北斗终端与密管中心间的密钥通信进行安全保护，保证密钥通信的保密性、完整性、真实性，有效防止针对密钥信息的中间人攻击、重放攻击和非法监听。密钥是短报文加密的关键所在，通过对密钥的传输保护，实现密钥的安全分发，进而确保短报文端到端加密的安全性。

使用主密钥标识设备身份及身份认证，使用会话密钥实现短报文数据的安全保护。主密钥出厂时根据应用规模预置进北斗终端中，会话密钥采用在线和离线的分发方式，从密钥初始化、密钥分发直到密钥销毁结束整个密钥生命周期的管理。使用国家密码管理局批准的基于商用密码算法建立的密码协议，建立密钥中心与北斗终端建立密钥管理通道。密管中心收到北斗终端的密钥申请指令后对北斗终端进行身份验证，通过验证后，密管中心向北斗终端安全分发会话密钥。直到请求密钥下发完成，此流程结束。添加 ID、时间戳，密钥传输过程中遭受攻击，保证密钥通信的保密性、完整性、真实性，有效防止针对密钥信息的中间人攻击、重放攻击和非法监听。密钥是短报文加密的关键所在，通过对密钥的传输保护，实现密钥的安全分发，进而确保短报文端到端加密的安全性。

4.5.5 系统管理安全性分析

对北斗终端管理员、密管中心管理员进行严格的培训、管理、考核，要求管理人员遵守密码相关法律法规，正确使用密码相关的产品及技术。对管理员进入工作区进行身份认证，保证管理人员身份的真实性。通过人员安全管理，避免非法人员伪冒管理者进行破坏行为，也可以防止管理人员错误操作带来的安全风险。

5. 北斗短报文密码应用案例

通过对北斗短报文通信应用的研究，分析通信中的安全现状和需求，基于商用密码，建立通用加密模型，形成北斗短报文密码技术，提供数据的机密性、完整性，防止北斗应用数据传输过程中的泄露、篡改、身份仿冒等危害，解决北斗短报文通信过程中的安全问题。将此研究成果应用到交通运输、远洋渔业、电力抄表等各行各业，可以起到保卫国家安全、人民生命，降低财产经济损失的重要作用。下述为基于本研究所提方法的北斗短报文加密应用案例。

5.1 交通运输部课题研究应用

2017 年 10 月 27 日，交通运输部发布《关于 2018 年度交通运输战略规划政策项目承担单位公开遴选的公告》，中电科网络安全科技股份有限公司组建了专门团队，围绕“北斗卫星导航系统交通运输行业数据传输加密和应用安全防护的研究”。根据项目的研究要点以及北斗系统在交通运输行业的应用特点，提出“商密+北斗”服务交通行业的总体研究思路，并提交了申报材料。2017 年 11 月 30 日，交通运输部发布公告，项目正式立项并确定电科网安为项目承担单位。在北斗卫星导航系统交通运输行业数据传输加密和应用安全防护的研究，主要包括三个部分的研究要点：

1) **卫星数据安全**：研究北斗系统卫星数据安全传输关键技术，以及在车载/终端卫星定位装置、密钥管理系统、安全网关等产品中的可靠应用。
2) **短报文通信安全**：研究北斗系统短报文功能，针对存在的安全问题提出解决方案，增强北斗系统通信安全性。
3) **业务系统安全**：研究北斗系统服务交通运输行业重要业务系统（等保 3 级以上系统）数据安全防护的商用密码技术应用标准。

通过对北斗短报文通信加密应用方案的设计，为后期交通运输行业特别是在“两客一危”中，提供了理论支撑，解决了北斗短报文通信过程中的安全隐患，降低了风险，保障应用顺利投入使用。在“两客一危”的场景中，以不过多增加北斗短报文通信应用的负担及应用性能为前提，对北斗设备终端中加入密码模块，实现端到端的加密；通过密管中心，实现密钥管理。具体的应用设计场景如图 5-1 所示。

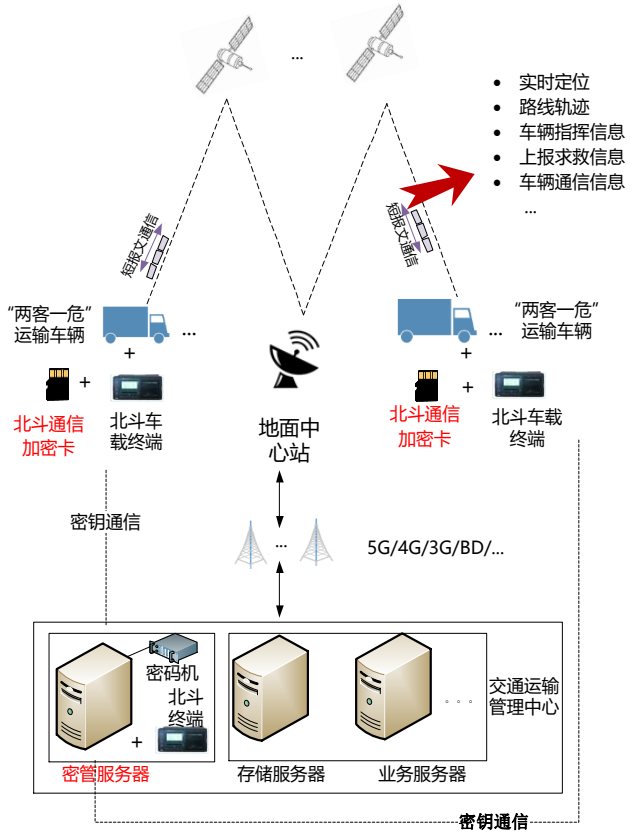


图 5-1　短报文密码应用技术框架图

本项目为试点研究项目，涉及的终端规模并不大。项目采用了第四章介绍的模型和方法，并对其进行了适当的简化，以适应项目的具体需求。项目的成功实施进一步验证了所提方法在实际中的有效性和指导价值。项目的主要方法包括：

1）初始化：采用离线的方式预置主密钥 MK 和会话密钥 SK。会话密钥以密码本的形式一次性预置 12 个。

2）群内通信：项目设置 1 个群组，对群组内短报文通信数据进行机密性保护和完整性校验，方法参考附录 A.2.2。

3）跨群通信：不涉及。

4）系统管理：项目规模较小，简化管理员操作。

5）密码算法：使用 SM4、SM3、HMAC 算法，实现短报文的加密及完整性保护，未采用 ZUC 算法。

6）密码设备：北斗通信加密卡以硬件芯片的形式固定在北斗终端上，以 SDK 的形式对外提供密码服务。为北斗终端提供统一的安全服务接口，支持 Android 系统和 IOS 系统。

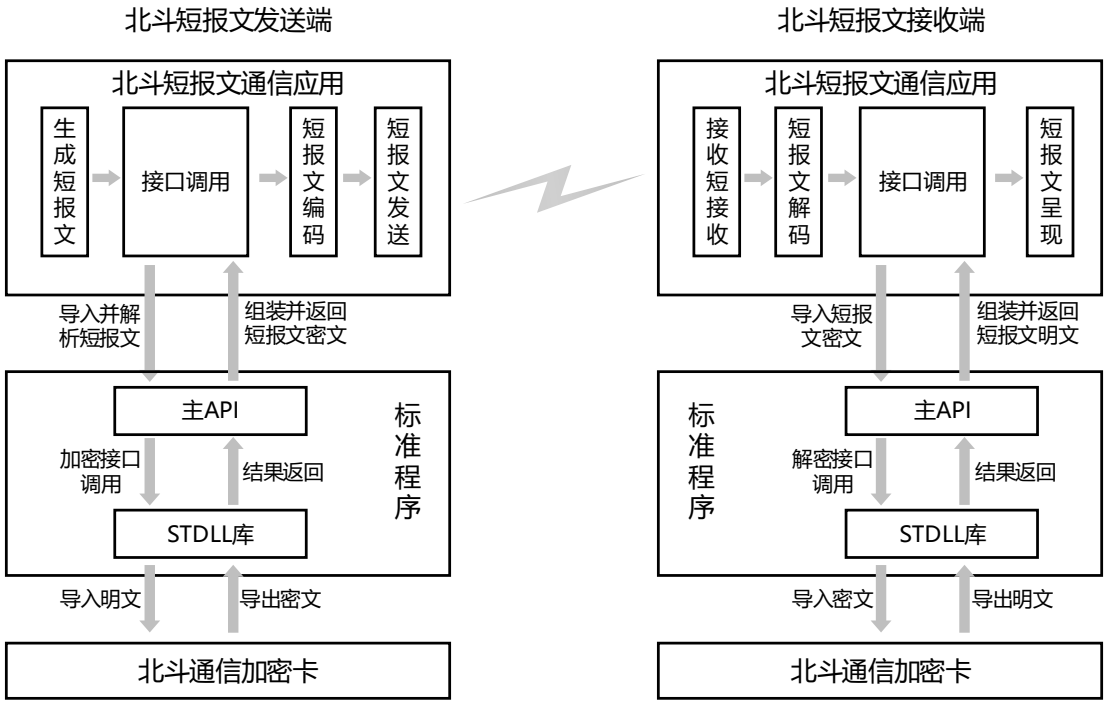


图 5-2　北斗短报文通信安全防护流程

7）密钥管理：使用附录 A.3 中的三层密钥体系。对于密钥管理的设计，根据场景安全性级别的要求，设置密管中心，建立三层密钥管理体系，负责对北斗设备的密钥的生成、分发、存储、更新、销毁等整个生命周期的管理。密钥体系分为三层，包含：本地主密钥 MK、分发保护密钥 KEK 和会话密钥 SK。

a）本地主密钥MK出厂时预置进北斗终端设备中，同时在密管中心备份，标识设备身份及对分发密钥进行保护；

b）分发保护密钥KEK属于临时密钥，在分发会话密钥时使用，不进行长期存储；

c）会话密钥SK存储在密管中心和北斗终端设备中，对短报文的通信数据进行保护。

5.2　北斗短报文加密方案推广应用

中电科网络安全科技股份有限公司联合北斗设备厂商，基于北斗手持机进行短报文通信加密应用系统原型开发，设计一套加密方案，面向特定行业用户进行推广应用。目前，交通运输、电力行业、水利行业、远洋渔业等部分行业用户表示对北斗短报文加密有明确的需求，同时也希望在行业场景中试点应用相关加密方案及产品。下面是基于北斗手持机进行北斗短报文加密应用原型设计的 APP，部分用户正在试用中。

在北斗设备出厂时，将密码软模块添加到北斗手持机中，在密管中心通过离线的方式将密钥预置进北斗手持机中，使北斗短报文能够进行加密通信。北斗手持机加密通信 APP 如图 5-3 所示：

图 5-3　北斗短报文加密通信 APP 新建短信界面

不加密的短报文通信，直接点击“发送”按钮；加密短报文通信，点击“加密发送”发送的短报文内容，短报文被加密以后发送出去。“收件箱”里存放收到的短报文信息如图 5-4 所示：

图 5-4　北斗短报文加密通信 APP 收件箱界面

已发送的报文将存入到“发件箱”中，如图 5-5 所示：

图 5-5　北斗短报文加密通信 APP 发件箱界面

登记北斗卡号的“通讯录”如图 5-6 所示：

图 5-6　北斗短报文加密通信 APP 通讯录界面

6. 标准化研究

北斗短报文密码技术应用研究的路线总体方向为：“推进密码标准应用，兼容国际密码标准，制定需求缺失标准，研究前沿技术标准”。根据北斗系统短报文通信的研究，制定如下的研究线路。

6.1 采标计划

由于国、内外暂无民用北斗短报文结合密码技术应用的相关规范标准，因此暂无采标计划。

6.2 标准研究思路

研究典型行业领域下的北斗短报文通信场景，分析北斗短报文通信过程中的安全风险和威胁隐患，基于《GB/T 32907-2016 信息安全技术 SM4 分组密码算法》、《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》、《GM/T 0050-2016 密码设备管理 设备管理技术规范》、《GM/T 0051-2016 密码设备管理 对称密钥管理技术规范》等标准，梳理北斗短报文通信商用密码应用技术要求，提出北斗短报文通信在安全通信机制、数据加密方法、密钥管理体系、身份认证、访问控制等方面的密码技术实现要求，建立北斗短报文通信密码应用技术框架，保障北斗短报文通信过程中的机密性、完整性、真实性。

6.3 标准化建议

北斗短报文密码技术目前处于研究阶段，缺乏正式发布的标准规范。尽管如此，北斗短报文已广泛应用于多个行业，特别是交通“两客一危”车辆运输等重要领域。目前尚未有统一的标准来规范商用密码算法的使用，以确保信息安全。

通过本课题研究，建议基于现有的商用密码算法、密码技术规范，围绕北斗短报文密码技术应用，制定总体技术规范、终端技术要求、交通/测绘等典型行业密码应用要求等系列标准，以体系化支撑商密技术在北斗短报文通信的应用，保障北斗短报文通信服务的安全。

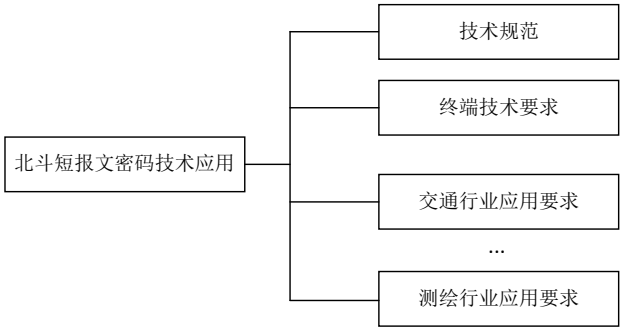


图 6-1　北斗短报文密码技术应用标准化建议

针对于总体技术规范、终端技术要求等技术维度的标准，将研究规定密码技术应用框架、密码应用机制、密码技术要求、安全协议规范等，适用于指导北斗短报

文密码应用系统的开发和使用。此类标准面临三个方面的挑战。其一，如何考虑短报文点对点通信、通播通信、平台通信等多种可能。其二，民用北斗卡中用户可使用的信息最长为 78 个字节，需针对短报文格式特点制定高效、实用的密码协议及安全报文格式，并同时兼顾北斗三号系统的拓展应用需求。其三，民用终端涵盖各种专用终端、大众消费型终端及指挥型终端，如何针对多源异构终端制定统一的密码应用框架，如何做好相关技术与北斗 SIM 卡等关键组件的关联和协调。

针对于测绘、交通等行业领域的应用维度标准，将研究结合行业通信场景的密码应用方法，满足不同行业、典型场景下差异化的密码应用需求。

7. 总结

本报告从北斗短报文通信民口应用体系出发，通过对北斗短报文通信在交通运输、电力数据传输、农业定位信息通信、远洋渔船通信、水文地质环境监测、应急救援及野外个人通信等多行业、多领域的应用场景的调研，进行信息收集和数据资产分析其中存在的安全威胁。选取现阶段民口应用最多的“两客一危”车辆运输、远洋渔船通信及应急救援三个领域，进行安全需求分析。根据当前北斗短报文通信现状，以商用密码为技术手段，构建合规的安全体系；以短报文通信为切入点，实现端到端的安全防护；提出基于商用密码的北斗短报文密码应用模型。该体系遵照安全标准体系和安全管理体系，以密码基础和密码产品为支撑，为北斗短报文通信提供机密性、完整性和真实性的密码服务，建立短报文密码应用的保障体系。通过综合多方面分析，提出一套基于商用密码的北斗短报文密码应用方案。密码算法使用对称密码算法，对短报文通信信息数据机密性保护，使用带密钥的 MAC 运算实现完整性及真实性保护，未来可以使用数字签名算法等方式实现对象的完整性保护。

本报告实现了密码与短报文协议融合，充分结合短报文特点，基于北斗短报文通信协议，设计密钥安全通道协议，进行密钥分发管理。通过多次试验验证北斗短报文密码应用方案，验证结果表明商用密码算法可以满足北斗短报文通信安全加密需求，且不会影响其通信效率。

北斗系统三代全球覆盖完成，对中国区域短报文通信服务，服务容量提高到字节1000万次/小时，单次通信能力1000汉字（14000比特）；北斗短报文通信民口应用从国内走向了国际，全球短报文服务，单次通信能力40汉字（560比特）。未来全面使用北斗三代系统后，短报文密码应用的将根据北斗短报文应用场景及业务安全性能需求，将通过多种密码技术的应用来保障短报文的应用安全。随着未来北斗应用领域更多，应用场景更加丰富，密码框架统一，应当制定一系列密码标准，通过标准化的方式进行规范应用。建议制定相关密码技术标准指导北斗短报文通信应用。

综上，此研究报告明确了以下问题：

1) 目前国内外都无北斗短报文密码技术应用标准，提出标准研究思路及建议；
2) 充分研究了北斗短报文通信的应用模式，抽象出了通用模型并对其进行加密模型、密码应用技术框架设计；
3) 应用案例：交通运输部课题研究应用和北斗短报文加密方案推广应用；
4) 提出《北斗短报文密码技术应用研究》报告。基于此研究报告，结合北斗短报文密码技术应用的国内外标准现状、应用案例的情况，建议后续开展标准制定工作。

参考文献

[1] 曹冲.卫星导航常用知识问答[M].北京:电子工业出版社,2010
[2] 帅平,曲广吉,向开恒.现代卫星导航系统技术的研究进展[J].中国空间科学技术,2004,24(03):45-53
[3] 唐金元,于潞,王思臣.北斗卫星导航定位系统应用现状分析[J].全球定位系统,2008,33(02):26-30
[4] 付朋侠.推进国产密码算法应用实现信息自主可控[J].科学家,2015,3(10):104-105
[5] 国家密码管理局.SM4 分组密码算法
[6] 《北斗卫星导航系统用户终端通用数据接口（2.1 协议）》
[7] 《北斗一号用户机数据接口要求（4.0 协议）》

附录 A　北斗短报文密码应用方案

A.1　系统框架

北斗短报文通信加密系统框架如图 A-1 所示：

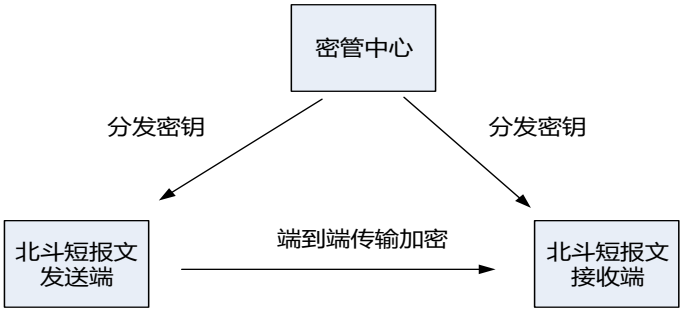
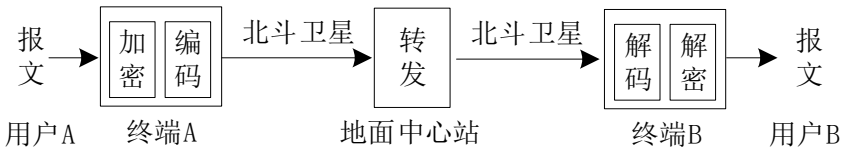


图 A-1　北斗短报文通信加密总体架构图

为保护短报文在传送过程中的安全，设计端到端的加密方案。在终端内部增加密码模块（如：使用硬件安全SE），使得报文在发送端先加密后再发送，经地面中心站转发后再传送至接收端，由接收端进行解密。北斗短报文加密通信示意图如图A-2所示。



图A-2　北斗短报文加密通信示意图

A.2　密码算法

A.2.1 算法配用

采用商用密码技术保护信息机密性、信息完整性和信息真实性。使用 SM4/ZUC 等对称密码算法，对短报文进行加密。使用基于 SM3 的 HMAC 算法实现对象的完整性、真实性保护。

表A-1　密码算法配用表

名称	密钥长度	类型	用途	备注
SM3	无	杂凑密码算法	信息摘要	使用基于

名称	密钥长度	类型	用途	备注
				SM3_HMAC 算法实现对象的完整性、真实性保护。
SM4	128	分组密码算法	加密信息	分组为 128 比特
ZUC	128	对称流密码	加密信息	

A.2.2 算法结构

密码算法主要应用在短报文加密、短报文完整性保护两个方面。对于短报文数据加密，系统既支持SM4的分组加密；也支持ZUC流密码加密。对于短报文完整性、真实性的保护，系统采用带密钥SM3_HMAC的方式。

术语和定义

比特bit：二进制字符0或1称之为比特。

字节byte：由8个比特组成的比特串称之为字节。

SM4：SM4分组密码算法。

ZUC：祖冲之序列密码算法。

密钥SK：短报文收发双端共享的会话密钥，密钥长度为128比特。

密钥K_{auth}：由密钥SK派生得到的认证密钥，用于完整性保护。

密钥K_{enc}：由密钥SK派生得到的加密密钥，用于数据加密。

初始向量IV： SM4/ZUC算法所使用的初始向量。

密钥流Keystream：ZUC算法根据密钥及初始向量产生的伪随机比特串，密钥流的长度根据加解密需要而选取。

时间T：北斗收、发当前时间，由北斗系统保证时间同步，以毫秒为单位。

符号和缩略语

⊕或XOR：按比特位逐位异或运算。

‖：表示串联，如$x_0 \| x_1 = x_0x_1$，$010 \| 110 = 010110$。

Trunr(A,B)：表示将字符串A截断为长度为B的字符串。

KDF(KEY,X)：密钥派生函数，根据密钥KEY，参数X，派生得到新密钥。实际应用中，可以采用SM3杂凑函数来实现。

短报文加密

设需要加密的数据为*M*，共享的会话密钥为*SK*，当前时间为*T*，发送端的ID为ID_A，接收端的ID为ID_B。

如果收、发双端采用的加密算法为SM4，发送端加密的过程如下：

1) $Input\ M, SK, ID_A, ID_B, T$

2) *K_enc=KDF(SK,0X0001)"*

3) $K_{enc} = KDF(SK,\ 0X0001)$

4) $IV' = SM_3(ID_A \,||ID_B \,||\, T)$

5) $IV = Trunr(IV', L_{IV})$

6) $C = SM4.Enc(M, K_{enc},\ IV)$

7) *Output* C

接收端解密的过程如下：

1) $Input\ C, SK, ID_A, ID_B, T$

2) $K_{enc} = KDF(SK,\ 0X0001)$

3) $IV' = SM_3(ID_A\ ||ID_B\ ||\ T)$

4) $IV = Trunr(IV', L_{IV})$

5) $M = SM4.Dec(, K_{enc},\ IV)$

6) *Output* M

如果收、发双端采用的加密算法为ZUC，发送端加密的过程如下：

1) $Input\ M, SK, ID_A, ID_B, T$

2) $K_{enc} = KDF(SK,\ 0X0001)$

3) $IV' = SM_3(ID_A\ ||ID_B\ ||\ T)$

4) $IV = Trunr(IV', L_{IV})$

5) $Keystream = ZUC(Key, IV)$，*注，只截取与* M *等长的比特*

6) $C = M \oplus Keystream$

7) *Output* C

接收端解密的过程如下：

1) $Input\ C, SK, ID_A, ID_B, T$

2) $K_{enc} = KDF(SK,\ 0X0001)$

3) $IV' = SM_3(ID_A\ ||ID_B\ ||\ T)$

4) $IV = Trunr(IV', L_{IV})$

5) $Keystream = ZUC(Key, IV)$，*注，只截取与* C *等长的比特*

6) $M = C \oplus Keystream$

7) *Output* M

短报文完整性、真实性保护

设需要保护的信息为M，共享的会话密钥为SK，当前时间为T，发送端的ID为ID_A，接收端的ID为ID_B，发送端完整性、真实性保护的过程如下：

1) $Input\ M, SK, ID_A, ID_B, T$

2) $K_{auth} = KDF(SK,\ 0X0002)$

3) $MAC' = SM_3\_HMAC(M\ ||\ ID_A\ ||ID_B\ ||\ T, K_{auth})$

4) $MAC = Trunr(MAC', L_{MAC})$

5) $Output\ MAC$

接收端完整性、真实性验证的过程如下：

1) $\mathrm{Input\ M, SK, ID_A, ID_B, T,\ MAC}$

2) $\mathrm{K_{auth} = KDF(SK, 0X0002)}$

3) $\mathrm{MAC' = SM_3\_HMAC(M \,||\, ID_A \,||ID_B \,||\, T, K_{auth})}$

4) $\mathrm{IF\ Trunr(MAC', L_{MAC}) == MAC}$

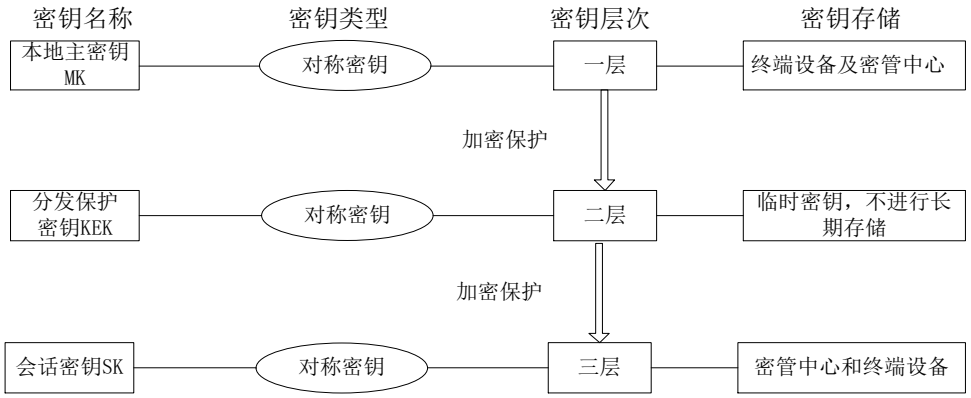
$Output\ M$

$ELSE$

$Output\ ERROR!$

A.3 密钥体系

A.3.1 密钥种类



图A-3 密钥体系图

密钥体系分为三层，包含：本地主密钥MK、分发保护密钥KEK和会话密钥SK。

1) 本地主密钥MK出厂时预置进北斗终端设备中，同时在密管中心备份；
2) 分发保护密钥KEK属于临时密钥，在分发会话密钥时使用，不进行长期存储；
3) 会话密钥SK存储在密管中心和北斗终端设备中。

A.3.2 密钥管理

1) 主密钥 MK

生成/分发：由密管中心生成，出厂时预置到北斗终端中。

存储：MK 被终端和密管中心共享，存储在北斗终端的密码设备内。

更新：MK 与北斗卡唯一绑定，不同的卡绑定不同的主密钥 MK，三年更新一次。

归档：无。

撤销：密管中心应在终端设备持有者对设备报失后，对相应终端密钥进行撤销。

备份：MK 除了在终端设备存储外，在密管中心存有备份。

恢复：当 MK 丢失时，需要向密管中心提起恢复申请，经审核通过后从密管中心的备份终端密钥数据中恢复。

销毁：无需销毁。

2）分发保护密钥 **KEK**

生成：当密管中心需要向北斗终端分发会话密钥时，密管中心生成 KEK。

分发：密管中心使用 MK 加密 KEK，将其安全分发给北斗终端。

存储：KEK 属于临时密钥，不进行长期存储。

更新：无。

归档：无。

撤销：无。

备份：无。

恢复：无。

销毁：通信结束后对 KEK 进行销毁。

3）会话密钥 SK

生成：密管中心生成。

分发：密管中心使用 KEK 加密 SK，将其安全分发给北斗终端。

存储：以密文的形式存储在北斗终端上。

更新：由会话密钥 SK 组成的密码本一年更新一次。每个月对应一个会话密钥 SK，一年 12 个月对应 12 个 SK，将这 12 个 SK 存储在一个密码本中一年更新一次。当更新周期达到时，需由密管中心产生新密码本安全发送给北斗终端进行更新。当怀疑泄露时，需对 SK 进行更新。

归档：无。

撤销：若密钥泄露时被撤销。

备份：密管中心进行存储备份。

恢复：当 SK 丢失时，可以从密管中心进行恢复。

销毁：当 SK 使用有效期失效时，对其进行销毁。

A.4　密码协议设计

A.4.1 短报文格式设计

北斗短报文通信涉及到两个协议，分别是 4.0 协议和 2.1 协议。

4.0 协议的全称是《北斗一号用户机数据接口要求》，版本 4.0，2006 年 11 月发布，简称 4.0 协议。4.0 协议为二进制格式，接口数据传输基本格式示例如下：

表 A-2　短报文 4.0 协议格式示例

指令	长度	用户地址	信息内容					校验和
通信申请 $TXSQ	16 bit	24 bit	信息类别 8bit	用户地址 24bit	电文长度 16bit	是否应答 8bit	电文内容最长 1680bit	8 bit

内容	长度	用户地址	信息内容							检验和
通信信息 $TXXX	16 bit	24 bit	信息类别 8bit	发信方地 24bit	发信时间 H 8bit	发信时间 M 8bit	电文长度 16bit	电文内容最长 1680bit	CRC 标志 8bit	8 bit

目前民用北斗卡中，用户可输入的信息最长为 78 个字节。

2.1 协议的全称是《北斗卫星导航系统用户终端通用数据接口（预）》，版本 2.1，2014 年 8 月发布，简称 2.1 协议。2.1 协议为文本格式，接口数据传输格式以语句的方式定义，以通信信息输出语句 TXR 为例，语句格式如下：

$--TXR,xxxxxxxx,x,hhmm,c--c*hh<CR><LF>

其中，“$”表示一条语句的开始，“hh”表示和校验字段，对“$”到“*”之间的字符执行 XOR（异或）运算所得。通信的电文内容在“c--c”位置，内容必须以有效的 ASCII 字符表示，除去一些预留字符，能在电文内容出现的有效字符范围大小为 89 个。目前民用北斗卡中，用户可输入的信息最长也为 78 个字节。

短报文可用长度为 78 个字节，考虑到日常发送的汉字、数字、字母等的 ASCI 码字均以字节为单位，所以短报文消息 PDU 的长度应设计为整数字节。由于消息 PDU 长度可变，需要由 PDU 长度字段进行标识，分配 1 字节为 PDU 长度字段，可标识 0-255 字节长度的 PDU，能够满足实际需求，同时也尽量减少了空间的浪费。使用通道类型字段区分短报文数据传输通信和密钥管理通信，使用指令类型区分数据加密策略及密钥管理指令。目前，通道类型及指令类型种类有限，两个字段可以共用 1 个字节。但是考虑到未来指令的扩展性，可以将通道类型字段设为 1 字节，指令类型字段设为 1 字节。

在用户可输入的 78 个字节内定义北斗短报文格式如图 A-4。

1字节	1字节	1字节	max75字节
通道类型	指令类型	PDU长度	PDU

图 A-4　北斗短报文格式

其中：

通道类型：00，数据传输通道。行业用户的数据（如：监测统计数据、业务应用数据、业务管理数据），都属于短报文数据平面的数据，处理方法和帧格式是相同的，不进行区分。

通道类型：01，密钥管理通道。不同方式的业务密钥（如：群密钥、跨群密钥）都是通过此通道传递。

通道类型：10，数据控制通道。

通道类型：11，保留通道。

具体通道类型描述如图 A-5 所示：

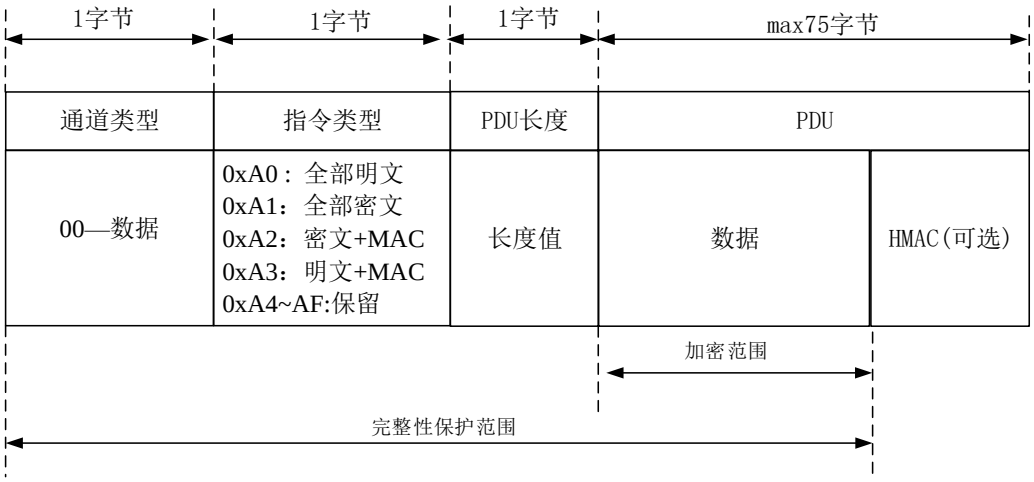


图 A-5　数据通道格式

注：

对PDU数据加密。对所有字段进行完整性验证。

HMAC：本方案中为可变字节长度，默认为16字节，后期短报文通信内容容量扩展，可能达到32字节。根据北斗短报文通信场景中的实际情况，可将HMAC长度截短为11字节，这样PDU最大传输75字节，减去MAC的11字节，等于64字节，正好是SM4分组加密分组长度16字节的整数倍，可以最大限度增加密文长度。

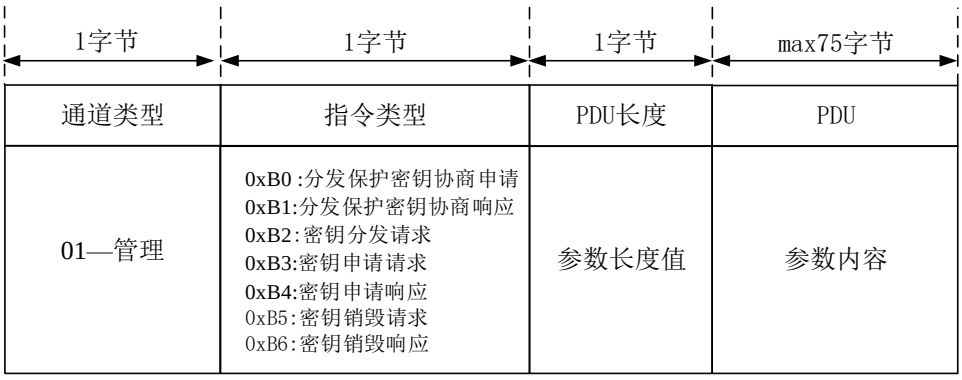


图 A-6　管理通道格式

对于01管理通道中，命令代码含义如表A-3所示：

表A-3　命令代码含义

命令类型	命令代码	代码含义
密管中心下发指令及其响应	0xB0	分发保护密钥协商请求
	0xB1	分发保护密钥协商响应
	0xB2	密钥分发请求
	0xB5	密钥销毁请求

命令类型	命令代码	代码含义
	0xB6	密钥销毁响应
北斗终端上报指令及其响应	0xB3	密钥申请请求
	0xB4	密钥申请响应
其他		可扩展命令，如密钥查询、密钥恢复、密钥启用等等

注：密钥分发请求由密管中心下发，北斗终端接收到后对应执行的响应指令为密钥申请请求 0xB3，在此不重复设置指令。

A.4.2 密钥安全通道协议

1) 密钥初始化协议

密钥初始化协议流程（出厂流程）采用离线方式，由密管中心将密钥初始化注入到终端。在北斗终端出厂时，将北斗终端带到密管中心，密管中心管理员对北斗终端进行初始化。初始化过程应满足以下要求。

a) 北斗终端信息录入：北斗终端管理员将一批北斗终端建群后带到密管中心，首先，在密管中心填写北斗终端基本信息表，密管中心管理员对表中信息进行录入；北斗终端管理员确认录入信息的准确性，在北斗终端基本信息表上签字报备。

b) 密钥注入：密管中心管理员根据北斗终端基本信息表中北斗卡号作为唯一标识，对应将密钥注入进北斗终端中。每个北斗终端注入不同的主密钥；同一群组的北斗终端注入同样的会话密钥。不同群组中的北斗终端注入不同会话密钥，确保群内密钥使用安全。

北斗终端设备出厂时，主密钥 MK 直接预置进北斗终端的密码设备中。北斗设备出厂时，会话密钥 SK 以密码本的形式预置进北斗终端中。SK 与 MK 分开存放，降低风险，提高安全性。

密码本预置策略：

a) 密码本中每个 SK 被 MK 加密后，以密文的形式存在；

b) 设计密码本中存放 SK 的个数公式：假设出厂时间为 x 月份，那么将由（12-x+1）个 SK 存放在密码本中。如：5 月出厂，则为：12-5+1=8,8 个 SK 存放在密码本中；

c) 由于每个北斗终端设备出厂时间不一致，因此密码本中的 SK 个数不一样，但是每个北斗设备对应月份的 SK 保持一致。如图 A-7 所示：

	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
1月	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10	SK11	SK12
	2月	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10	SK11	SK12
		3月	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10	SK11	SK12
			4月	SK4	SK5	SK6	SK7	SK8	SK9	SK10	SK11	SK12
				5月	SK5	SK6	SK7	SK8	SK9	SK10	SK11	SK12
					6月	SK6	SK7	SK8	SK9	SK10	SK11	SK12
						7月	SK7	SK8	SK9	SK10	SK11	SK12
							8月	SK8	SK9	SK10	SK11	SK12
								9月	SK9	SK10	SK11	SK12
									10月	SK10	SK11	SK12
										11月	SK11	SK12
											12月	SK12

图 A-7　密码本设计

如：1 月出厂的终端，密码本内存放 SK1，SK2…SK12 合计 12 个密钥，5 月出厂的终端，密码本内则存放 SK5，SK6…SK12 合计 8 个密钥。同一批次北斗终端每个月用的密钥一样。遇到月末、年末发送短报文时，接收端收到的报文信息跨月或跨年的情况，以发送时的时间使用对应的密钥。

考虑到北斗终端设备销售的一些情况，终端出厂到销售到用户手中会滞后一段时间，如：12 月份出厂的北斗终端设备，到达消费者手中可能是第二年的 1 月份以后，那么将导致无 SK 可用。因此，遇到这种比较特殊的情况出厂的北斗终端设备，当终端设备到达用户手中的时候，用户开机后，采用在线密钥申请的方式。

2) 密钥分发协议

会话密钥更新的周期为 1 年，每年的 12 月，密管中心向北斗终端下发第二年的密码本（12 个 SK），对北斗终端里的密钥进行更新。密钥更新的方式有两种，一种是密管中心主动启动密钥分发请求，北斗终端收到请求后，发出密钥申请请求，进行密钥更新，其协议流程如图中的 0-4 步骤所示；第二种是北斗终端直接向密管中心发送密钥申请请求，进行密钥更新，其协议流程如图中的 1-4 步骤所示。

密钥中心与北斗终端建立安全通道（直接使用北斗通信通道），在密钥即将到期更换的时候，北斗终端应当主动向密管中心发出 0xB3 密钥申请指令申请更换密钥。若北斗终端未向密管中心提出密钥申请请求，那么密管中心启用密钥分发请求 0xB0，北斗终端接收到请求后应响应该指令发出 0xB3 密钥申请指令。密管中心收到北斗终端的 0xB3 密钥申请指令后对北斗终端进行身份验证，通过验证后，密管中心向北斗终端发送分发保护密钥协商请求 0xB0，协商后续用于分发 SK 的加密密钥 KEK。北斗终端发起分发保护密钥协商响应 0xB1 指令，接收并确认密管中心向其发送的 KEK。密管中心向北斗终端发送若干条密钥申请响应 0xB4 指令，直到密码本中所有密钥下发完成，此流程结束。

密钥申请分发流程如图 A-8 所示：

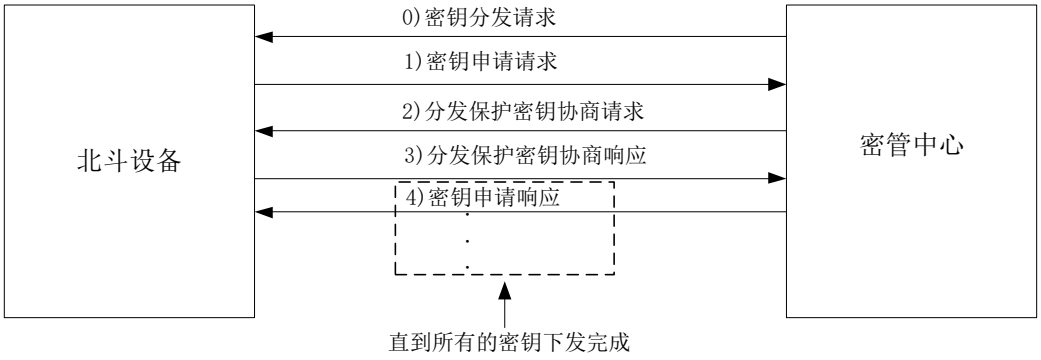


图 A-8　密钥申请分发流程

a)　密钥分发请求

用于密管中心向北斗设备发送密钥分发请求 0xB2 指令，该指令中下发的字段内容如图 A-9 所示：

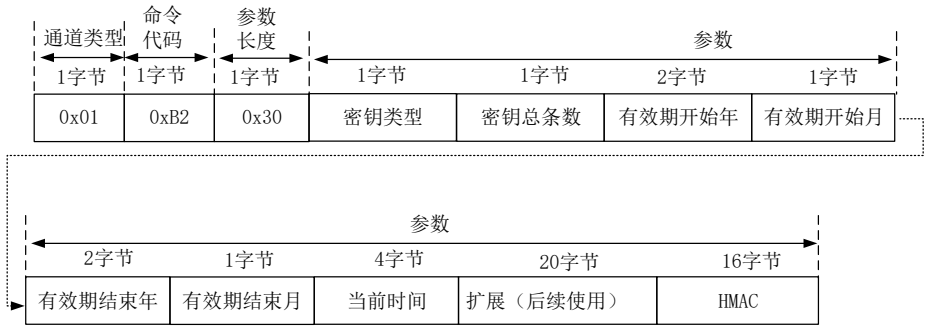


图 A-9　密钥分发请求

b)　密钥申请请求

北斗设备通过上报指令 0xB3，向密管中心提出密钥申请，格式如 A-10 所示：

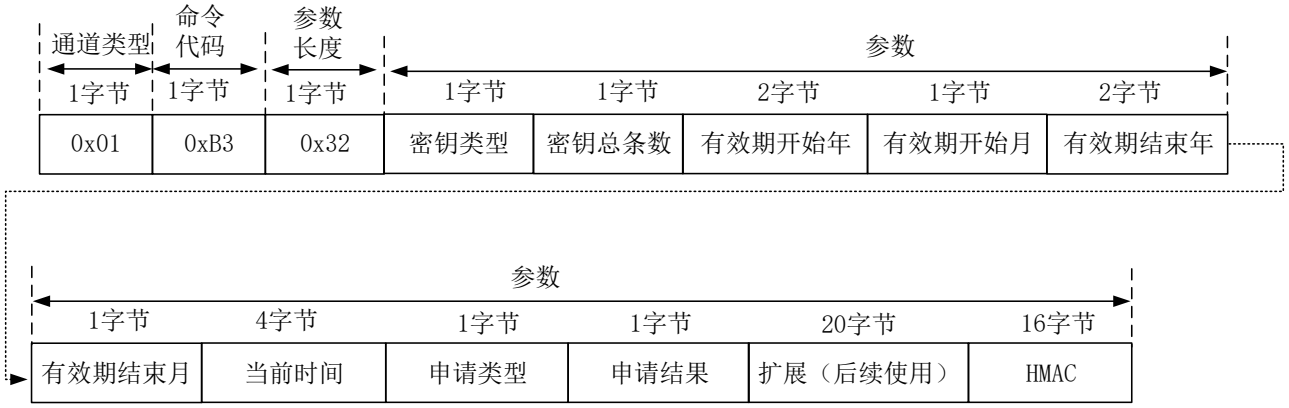


图 A-10　密钥申请请求

注：申请类型包括两种：0 为主动上报，1 为非主动上报；

申请结果：0 为成功，1 为失败。

HMAC:使用 MK 对其进行 HMAC 运算得到 MAC 值。

c) 分发保护密钥协商申请

密管中心接到北斗终端上报的 0xB3 指令后，向北斗设备下发分发保护密钥协商申请 0xB0 指令，格式如图 A-11 所示：

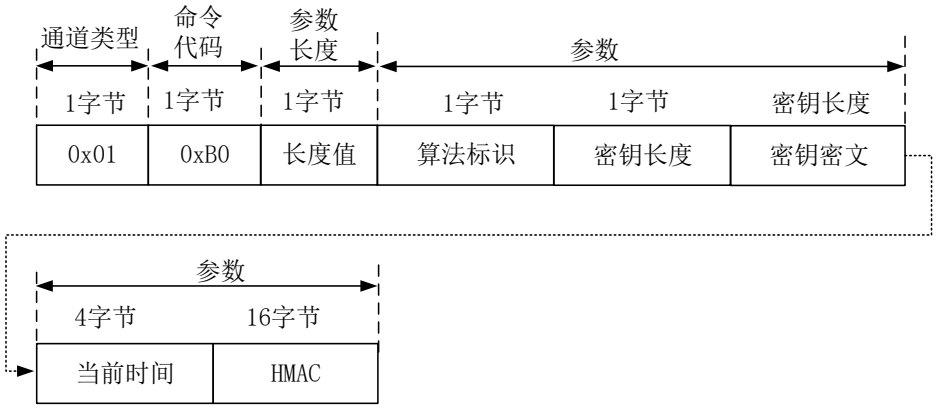


图 A-11　分发保护密钥协商申请

d) 分发保护密钥协商响应

密管中心向北斗终端下发分发保护密钥协商响应 0xB1 指令，格式如图 A-12 所示：

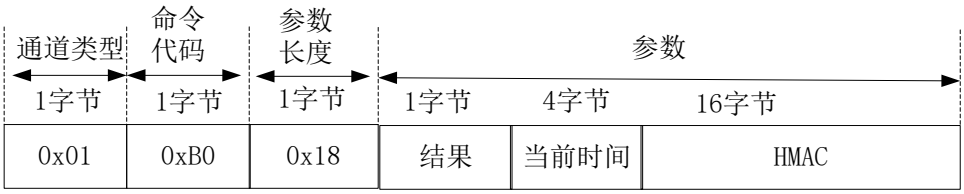


图 A-12　分发保护密钥协商响应

结果：为 0 分发成功，否则为错误码。

e) 密钥申请响应

北斗终端向密管中心发送密钥申请响应 0xB0，按照短报文传输字节数限制，无法一次传输完成，设计如下三段传输格式：

第一段密钥申请响应从接受第一个密钥开始，格式如图 A-13：

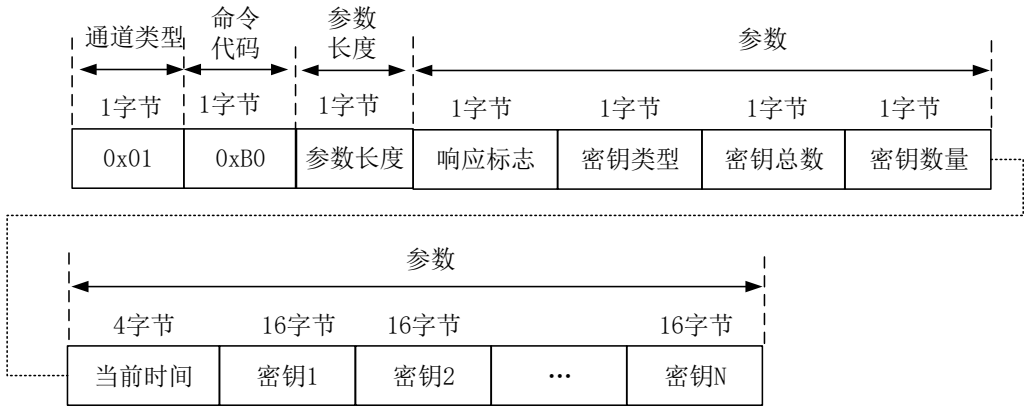


图 A-13　密钥申请响应 1

响应标志：设置 0x01，指从第一个密钥响应开始。

密钥类型：对称/非对称密钥。

密钥总数：密钥传输的总量。

密钥数量：此次传输的密钥数量。如：根据短报文长度限制，本次可以传 4 条密钥，即第 1 条密钥至第 4 条密钥。

第二段为中间的密钥响应，字段格式如图 A-14：

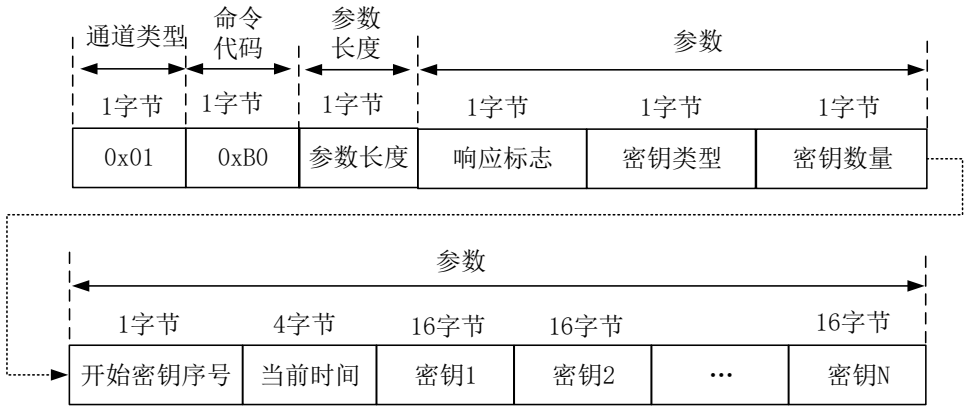


图 A-14　密钥申请响应 2

响应标志：设置 0x02，指从中间密钥响应开始。

开始密钥序号：标识本指令中密钥 1 的序号（如：从第 5 条密钥开始）。

根据密钥数量、开始密钥序号两个字段内容，可以得到本次传递的结束密钥序号。如：密钥数量为 4，开始密钥序号为 5，相应地结束密钥序号为 8。

最后一段的密钥响应，字段格式如图 A-15：

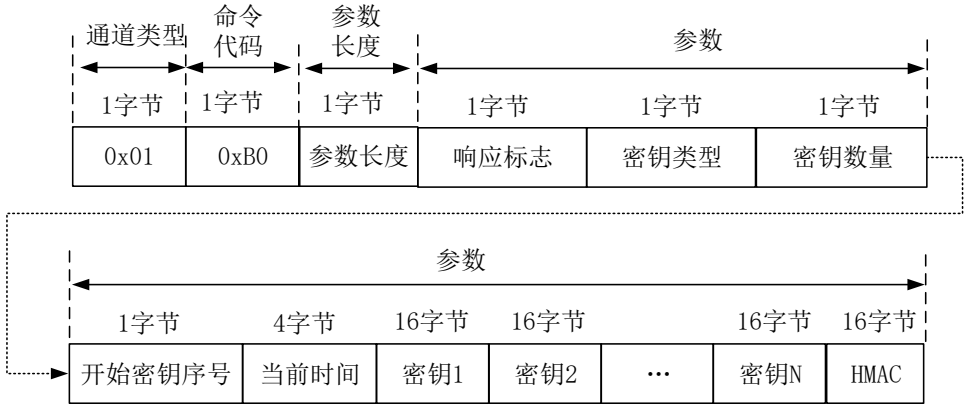


图 A-15　密钥申请响应 3

响应标志：设置 0x03，指最后一条密钥申请响应。

密钥数量：本指令中，密钥数量可能为 0，则此时开始密钥序号字段无意义，也不存在后续的密钥字段。

HMAC：对三段密钥申请响应中的所有内容计算 HMAC。

密码本使用过程中存在跨月，跨年的情况（如：3 月 31 日 23:59:00 发送，接收方可能在 4 月 1 日接收到），接收信息使用密钥以发送时期对应的密钥，进行解密。后期兼容北斗三号系统设计，北斗短报文通信内容容量变大，数据安全性需求更强，密钥更新策略进行调整（如：更新周期变短等）。

3) 密钥销毁

密码本中有 12 个密钥，每个月对应一个密码，每个月结束，当月的密钥就由北斗终端自动销毁。若密钥使用过程中出现紧急情况，如：密钥泄漏等。由密管中心通知北斗终端将密码本中的所有密钥进行销毁，流程如下，包含两部分：密钥销毁请求和响应。流程如图 A-16 所示：

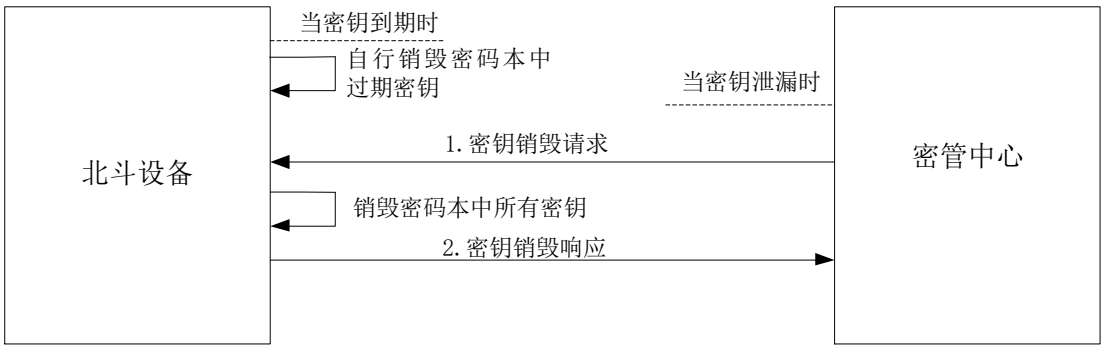


图 A-16　密钥销毁流程

密钥销毁请求，如图 A-17：

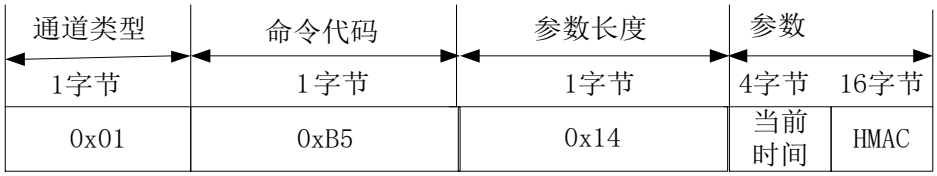


图 A-17　密钥销毁请求

密钥销毁响应，如图 A-18：

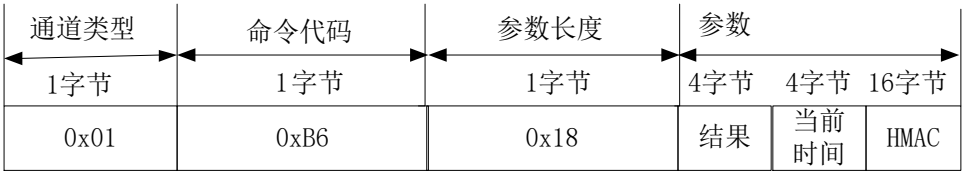


图 A-18　密钥销毁响应

其中，结果为 0 则销毁成功。当结果小于零为销毁失败错误码。

A.5　安全性分析

1)　算法应用安全性分析

方案采用的对称密码算法、杂凑算法、消息鉴别码算法符合法律、法规的规定和密码相关国家标准、行业标准的有关要求，算法应用合规。

方案采用 SM4 或 ZUC 算法对短报文进行加密，保护短报文的机密性。目前尚无对 SM4 或 ZUC 算法的有效攻击，从而能提供对报文机密性的有效保护。

方案采用 SM3 算法计算出来的 256 比特 MAC 值进行了截断，只选取了后L_{MAC}（如 128 比特）比特作为消息的 MAC 值，此在一定程度会降低完整性认证的安全性，但由于该 MAC 值综合考虑了密钥、时间、ID 等信息，在攻击者未掌握对称密钥时难以进行篡改、伪造消息。此外，还可以通过其他方式得到L_{MAC}的 MAC 值，如：对 256 比特 MAC 值再次计算 MAC 并进行截断，或者将 256 比特 MAC 值的前L_{MAC}与后L_{MAC}进行异或等等。另一方面，随着北斗三号系统的应用，可以根据实际应用情况调整 MAC 值长度（如继续保持为 256 比特），以满足完整性认证强度的需求。

2)　密钥管理安全性分析

方案建立密管中心，实现全网密钥的安全管理。系统如果遭遇突发事件，密管中心能够对密钥进行统一的恢复、更新、撤销等处理，保证系统可持续运转。

方案采用三层密钥体系，实现密钥层级保护。设备主密钥不出密码设备，大大降低主密钥泄漏的风险。采用一次一密的设计思想，使用临时的分发保护密钥加密会话密钥，实现会话密钥的安全分发。设计密钥派生函数，将会话密钥派生为加密

会话密钥和认证会话密钥，分别用于加密和完整性保护，体现专钥专用的思想，降低一钥多用带来的安全风险。

3) 数据传输协议安全性分析

参考《GM/T 0050-2016 密码设备管理 设备管理技术规范》，建立数据安全通道，实现短报文数据的安全传输。根据不同的安全需求，对短报文数据进行不同程度的安全保护。对于最低安全等级，进行短报文明文传输，此类场景适应于无安全需求的短报文通信，如日常测试性的通信。对于一般安全等级，进行短报文明文+MAC传输，对短报文进行完整性保护，此类场景适用于可防止信息篡改的短报文通信，如工业的控制指令等。对于较高安全等级，进行短报文密文传输，对短报文进行机密性保护，此类场景适用于防止信息泄露的短报文通信，如组织机构间的敏感通信。对于最高的安全等级，进行短报文密文+MAC 传输，对短报文进行机密性、完整性保护，此类场景适用于防止敏感信息篡改、泄露的短报文通信，如企业机构的核心商业秘密、重要敏感场所位置信息、金融数据等。

4) 密钥管理协议安全性分析

参考《GM/T 0050-2016 密码设备管理 设备管理技术规范》、《GM/T 0051-2016 密码设备管理 对称密钥管理技术规范》，建立密钥管理通道，用于对密钥分发、更新等生命周期管理。

采用密码本机制，一个密钥可使用一月，一年共十二个密钥。一年的密钥通过密码本的形式下发到北斗终端，能够有效解决密钥频繁传输带来的安全隐患，同时也能避免密钥使用周期过长带来的密钥破译风险。

每次密钥下发均需要经过密钥申请、分发保护密钥协商、密钥下发、密钥响应等完整的协议交互，一旦某一步协议通信失败，将终止整个过程，同时在密管中心进行异常记录，以此保证通信交互的正确性。

在密钥通信交互中，通过在报文中设置“当前时间”、计算报文的 HMAC 值等方式，能够有效防止针对密钥的重放攻击、中间人攻击、篡改和破坏行为。对于通信数据较长（如密码本的下发）的情况，发送方将通信数据截断为若干个连续的短报文，标识每个报文的排列顺序，并在最后一个报文上填充“当前时间”并计算整体的 HMAC 值；接收方接收到所有连续的短报文后，进行拼接和恢复，并进行时间验证和完整性验证，以此保证通信的安全性。

5) 报文格式密码应用安全性分析

对数据传输协议和密钥管理协议通信中的命令进行约定分类，制定规则（如通道类型规则，字节长度规则、命令代码规则等），规避错误通信。基于短报文的 78 字节通信内容设计报文格式，不影响短报文功能使用，并在此基础上实现应用层安全协议，保障短报文端到端传输安全。

A.6 典型方案部署

此方案的北斗短报文加密通信部署，如图A-19所示。

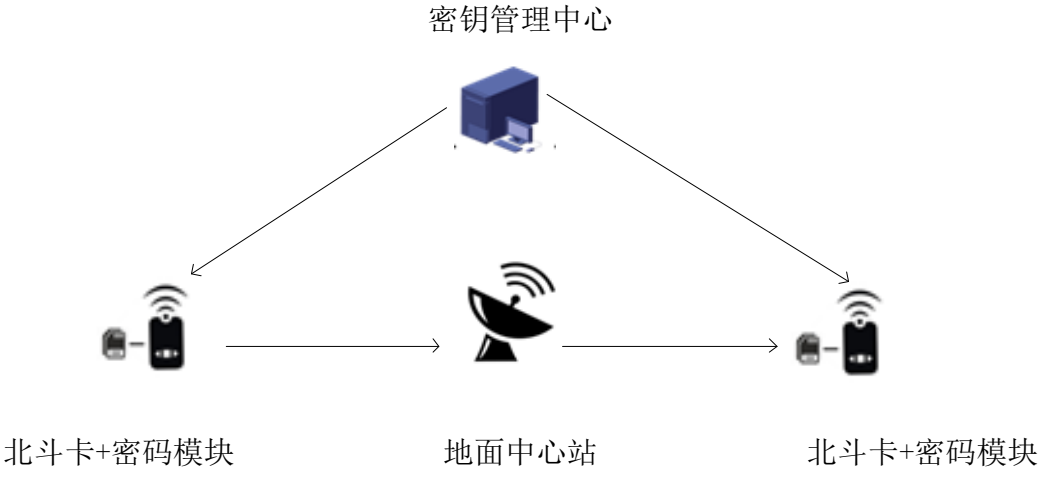


图 A-19　北斗短报文通信加密图

注：密码模块，推荐使用硬件安全 SE。