基于CCSDS空间数据链路安全协议的星载遥控认证保护

唐利锋[1],崔　阳[2],刘晓瑞[1],刘希红[1]
(1.上海航天电子有限公司,上海 201821;2.中国科学院 微小卫星创新研究院,上海 201210)

摘　要: 在国际空间数据系统咨询委员会(CCSDS)规定的空间遥控系统数据传输体制下,对星载遥控认证保护进行了研究。选择了遥控数据认证保护层次,并设计了认证保护数据范围。针对上行遥控的认证保护机制与国际空间数据系统咨询委员会的空间遥控链路命令操作过程(COP-1)之间存在的"闭锁"风险,设计了重传请求保护机制。基于空间数据链路安全(SDLS)协议体制,提出了一种遥控认证帧结构模型。在该模型中,通过插入随机序列码段,使相同指令/数据帧经认证算法计算后,其结果的非线性度扩大;通过插入毫秒级精度的时间序列码段,抵御重放攻击,并极好地适应不同地面控制中心对航天器的并行控制。提出一种针对遥控认证保护的,涉及"常态"和"应急态"的安全关联(SA)周期管理的方法、密钥生存周期管理的方法,有效实现各虚拟信道的独立保护及密钥的科学管理。同时,提出一种开展星载遥控认证保护业务的算法设计方法。

关键词: 国际空间数据系统咨询委员会(CCSDS);空间数据链路安全协议(SDLS);通信操作程序;COP-1;密钥;MD5

中图分类号: TP 309;TP 872　　**文献标志码:** A　　**DOI:** 10.19328/j.cnki.2096-8655.2021.04.016

Satellite-Borne Transmission Control Authentication Protection Based on CCSDS Space Data Link Security Protocol

TANG Lifeng[1], CUI Yang[2], LIU Xiaorui[1], LIU Xihong[1]
(1.Shanghai Aerospace Electronics Co., Ltd., Shanghai 201821, China;
2.Innovation Academy for Microsatellites, Chinese Academy of Sciences, Shanghai 201210, China)

Abstract: The satellite-borne transmission control (TC) authentication protection is studied under the hierarchy of the TC data transmission system specified by Consultative Committee for Space Data Systems (CCSDS). The data link sub-layer used for authentication protection is selected, and the scope of protected data is designed. Due to the "lock-up" risk between the authentication protection mechanism of the uplink TC and the COP-1 command operation process of CCSDS, a retransmission request protection mechanism is designed. Based on the space data link security (SDLS) protocol system, a TC authentication frame structure model is proposed. In this model, the non-linearity of the same instruction/data frame is enlarged after the calculation with the authentication algorithm by inserting random sequence code segments. By inserting the time sequence code segments with millisecond-level precision, it resists the replay attacks and well adapts the parallel control of spacecraft by multiple satellite control centers. A security association (SA) cycle management model and a key life cycle management model involving "normal state" and "emergency state" for TC authentication protection are designed to realize the independent protection of each virtual channel and the scientific management of the key effectively. At the same time, an algorithm design method for satellite-borne TC authentication protection services is proposed.

Key words: Consultative Committee for Space Data Systems (CCSDS); space data link security (SDLS) protocol; communication operation procedure; COP-1; key; message digest-5 (MD5)

收稿日期:2020-10-18;**修回日期:**2021-02-01

基金项目:上海市科学技术委员会全球多媒体卫星系统项目(17DZ1100700)

作者简介:唐利锋(1986—),男,硕士,高级工程师,主要研究方向为空间数据信息保护、卫星综合电子系统、星载遥控系统等。

0　引言

在进行航天器的遥控系统设计以及任务实施过程中，星地通信链路安全保护尤为关键。由于空间链路具有开放传输网络属性，空间数据系统广泛存在被侦听、重传、伪造数据信息的安全隐患。为应对空间任务的安全需求，国际空间数据系统咨询委员会（Consultative Committee for Space Data Systems，CCSDS）提出了各类型航天任务的安全保证体系框架，开发定制了系列空间数据系统数据标准化文件[1-4]。

在实际应用中，军用航天任务执行过程一般包含高战略价值敏感信息的数据传输，安全需求等级较高。保护的措施包括：遥控数据加密、完整性判别、认证数据来源和授权访问。而对于民用航天任务，如商业通信卫星、气象卫星、遥感卫星等，一般只需要进行遥控数据完整性判别、数据来源认定。近年来，基于CCSDS体制，发展了将不同密码学算法应用于分包遥控的加密认证的研究方向[5-8]，但均停留在安全框架设计及算法性能分析与相互结果比较上，无法指导系统的工程设计。且对于单认证体制下的分包遥控系统详尽实施策略研究鲜有论文涉及。

本文针对单认证体制的分包遥控[9-10]，对系统处理数据的流程进行分析。基于空间数据链路安全（Space Data Link Security，SDLS）协议，确定了的认证保护实施的范围，并对遥控数据传输控制进行了设计。考虑民商用航天器通信的安全需求以及认证算法的功能，设计运用了集成密码结构的增强型（Message Digest-5，MD5）算法对星载遥控通信进行认证保护，通过设计安全关联（Security Association，SA）管理机制，保证星载遥控认证保护工作的有效运行。

1　SDLS协议

在CCSDS分层模型中的数据链路协议层中，设计有一个额外的安全子层，作为一个功能实体，实现SDLS协议，如图1所示。SDLS协议结合了相应的数据结构，在空间数据链路协议传送帧中，为基于字节的用户数据提供了认证/加密认证服务的标准方法。该协议可作为各型号航天任务空间链路数据通信的标准，减少了安全解决方案的重复设计，有助于通用商业化的开发实现。

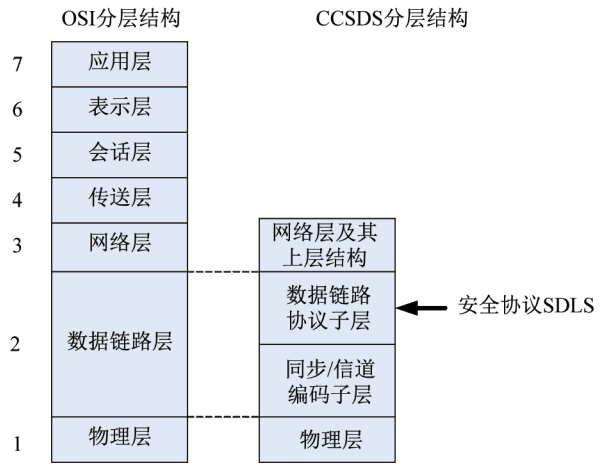

图1　CCSDS分层模型与SDLS所处位置

Fig.1　Location of SDLS in CCSDS layered model

1.1　SA的定义

当进行星地链路通信时，需要发送方与接收方统一数据保护模式、密码通信参数。SA定义了单向信息传递、数据认证算法体制、数据完整性确认、重放攻击识别的服务。地面测控中心与航天器在进行安全通信前，预先确定SA，使SA关联特定密钥及使用该密钥的虚拟信道（Virtual Channel，VC），并切换SA状态至运行状态，实现SA星地同步。VC是一种按数据特性和传输要求使多数据源分享同一物理信道的传输控制及动态调度机制，通过帧头识别码进行标识。SA一旦被定义，则用于认证的算法、参数及操作方式在SA生存周期内保持不变。

1.2　SDLS协议数据结构

SDLS协议在“安全导头（Security Header）”和“安全尾部（Trailer）”之间封装传送帧的应用数据，“安全导头”和“尾部”包含了接收端用于消息验证的必要参数。“安全导头”和“安全尾部”的格式定义如图2所示。其中，“安全导头”包含安全参数标志（Security Parameter Index，SPI）、初向量（Initialisation Vector，IV）、防重放序列号（Serial Number，SN）和填充块。“尾部”为验证码（Message Authentication Code，MAC）。除SPI外，SDLS中其他数据域为变长可选，其长度取决于SA所设定的算法和功能。SPI长度为2 byte，用于唯一标识传送帧所采用的SA。

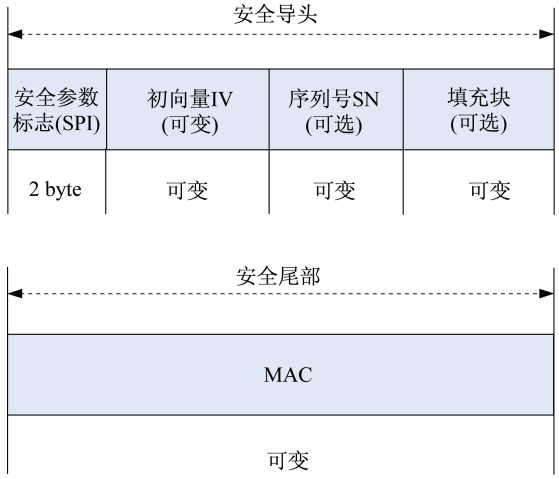

图 2 SDLS 协议中“安全导头”和“安全尾部”

Fig.2 Security header and trailer in SDLS protocol

1.3 基于 SDLS 协议的遥控认证保护范围设计与数据传输控制设计

为了保证遥控数据的可靠传送,CCSDS 设计了遥控通信操作程序(Communication Operation Procedure,COP)规约,实现发送端和接收端同步操作的闭环。其中在发送端执行的帧操作步骤称为帧操作程序(Frame Operation Procedure,FOP),其组织遥控帧发送队列;在接收端执行的帧接收及汇报机制称为帧接收和汇报机制(Frame Acceptance and Reporting Mechanism,FARM),FARM 识别接收到的数据帧结构中的“帧序列号”,是否匹配星上更新的帧序列计数,如果匹配,则接受并处理该数据帧,否则不予接收。同时 FARM 经由星地遥测下行链路,定时通过命令链路控制字(Command Link Control Word,CLCW)[10]反馈接收状态信息。FOP 识别 CLCW 结构数据信息,若有遥控数据帧未被接受,则从 FARM 所更新的帧序列号开始重新启动发送操作[11],上述过程形成一个完整的闭环,COP 闭环操作过程如图 3 所示。COP 机制保证了遥控数据准确并且按序在有噪信道中传输。

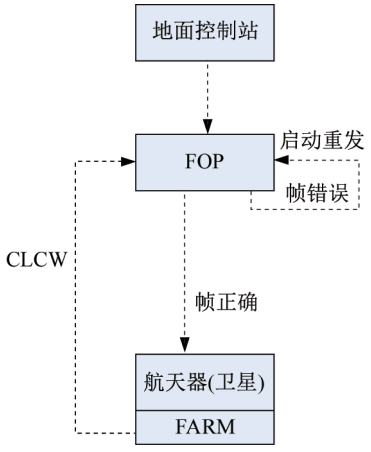

图 3 COP 过程

Fig.3 COP process

为了数据保护机制能保护命令操作步骤中的 COP 标志(AD 类型帧数据格式中的“通过标志”与“控制命令标志”),阻止敌方对上述标志发起攻击,引起服务拒绝,本文设计进行数据保护的范围如图 4 所示,对“帧头”域、“安全导头”域、“传送帧数据”域作为一个整体进行认证保护,认证输出的验证码填入“安全尾”域。

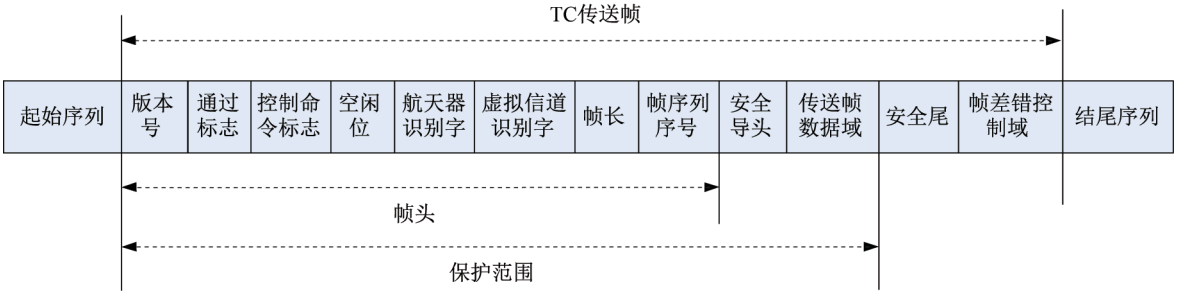

图 4 基于 SDLS 协议遥控传送帧及其保护范围

Fig.4 TC frame format based on SDLS protocol and its protection scope

由于分包遥控系统中的 COP 闭环机制与认证闭环机制之间相互独立,故在数据链路层开展认证操作时,认证重传循环内嵌 COP 重传循环,可能引起 COP 循环与认证循环发生冲突,造成通信的死锁[12-13]。所以本文在 VC 帧业务与 FARM 操作之间进行认证操作[14]。

地面控制侧,在数据链路层进行组帧,并按需求进行传输帧的认证,后输入至“FOP 帧传输控制

模块”进行数据帧的传输控制。“FOP帧传输控制模块”中建立遥控传输帧队列，并按照帧序列号进行先后排序。“FOP帧传输控制模块”同时接收星上下传的帧安全报告（Frame Safety Report，FSR）与CLCW，其中通过FSR判读星上传输帧的认证状态，而FSR被包装为均匀等间隔“源包”，当收到FSR时，按照帧序列号进行认证数据帧的重新传送。当收到定时CLCW，即判读星上帧接收状态，通过CLCW中包含的当前接收帧序列号删除地面侧FOP队列中已发送成功的帧。

星上侧，对接收到的遥控命令帧/数据帧进行认证后，通过FSR向地面控制端汇报帧认证信息，仅有认证通过后，才将遥控帧传送至“FARM帧传输控制模块”，“FARM帧传输控制模块”发出反馈CLCW，汇报航天器终端的遥控帧接收状态，该CLCW作为下行遥测帧的“操作控制域数据”，通过特定VC定时下传。上述设计避免循环冲突引发的进程死锁，传输控制流程设计如图5所示。

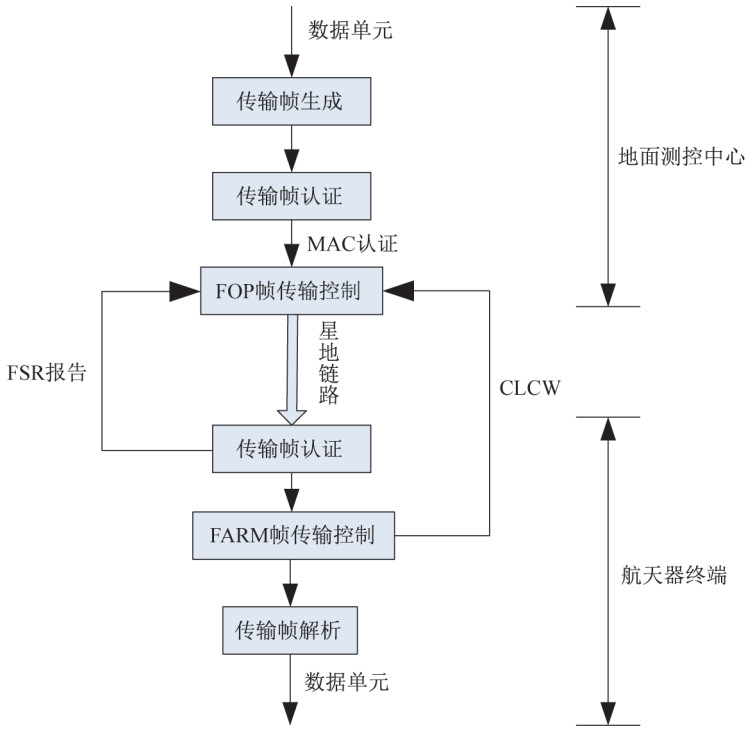

图5　传输控制流程设计

Fig.5　Design of transmission control flow

2　分包遥控认证应用方案

2.1　遥控认证帧格式设计

遥控认证指令、认证数据的帧数据格式见表1。为有效进行SA的管理，预防SA运行过程中的操作丢失，设计两层SPI结构见表2。

“IV”设计为地面测控中心生成的随机数注入，用以扩大认证计算结果的非线性度，避免星载遥控在生命周期内，由于相同指令码/数据多次重复发送而带来的攻击。“SN”设计为“时间序列码段”，为

表1　遥控认证指令、认证数据帧格式

Tab.1　Authentication command and authentication data frame format of TC

帧主导头（5 byte）								帧数据域					差错控制域
版本号	通过标志	控制命令标志	空闲位	航天器识别字	VC识别字	帧长	帧序列序号	SPI	IV	SN	数据域	MAC	CRC
2 bit	1 bit	1 bit	2 bit	10 bit	6 bit	10 bit	8 bit	16 bit	96 bit	48 bit	偶数字节	16 byte	16 bit

表 2 层次 SPI 结构模型

Tab.2 Hierarchical structure model of SPI

层次	SPI实现功能	SPI相关联的密钥特征	SPI设计值
1	对SDLS协议数据单元进行传递	关联主密钥(协议数据单元(Protocol Data Unit,PDU)认证密钥)	0x0000H
2	对上注指令/数据进行认证	使用前需关联会话密钥,星上预存或者地面上注	0x0001H~0xFFFEH

防重放攻击所设计,由测控中心管理设备组织时间信息。格式见表3,星上判断每次上传的认证指令/数据帧中的“时间序列码段”,要求后一帧的“时间序列码段”必须大于前一帧的“时间序列码段”。如果后一帧的“时间序列码段”小于或者等于前一帧的“时间序列码段”,认为是重放攻击,遥控认证模块忽略该次遥控帧,并在下行遥测帧对应“重放”标识位中进行标示。

表 3 时间序列格式设计

Tab.3 Format of the time series bit

预留	年	月	日	时	分	秒	毫秒
4(0 000b)	12	4	5	5	6	6	6
48							

“MAC”为地面运控站使用认证算法计算输出的认证值,嵌入在传送帧中,传送给航天器。依据上节分析,认证运算区域设计为:帧主导头、安全导头、帧数据域、认证密钥。其中,“认证密钥”不参与传输,为星上预存。只有星上遥控认证软件计算的“MAC值”与上传数据帧的“MAC值”比对一致时,认证正确,该帧被接收。

2.2 SA管理设计

不同航天器任务复杂度不同,星上信宿(分系统或设备)对星地链路数据传输的保护形式和要求不一样,数据保护算法的挂钩密钥也可能随时进行变更。对于长生命周期的航天器而言,切换个别信宿的数据保护模式及参数、星地密钥传输的保护并可靠管理等是亟需解决的问题。SA管理机制的设计,可为解决上述问题提供了一套可靠方案。

设计通过将PDU[4]嵌入SDLS协议中的数据域中,实现数据保护,用以覆盖SA的管理要素,并且可以实现密钥管理的标识识别,地面站通过传递PDU至航天器终端来实现星载SA状态的动态切换。PDU传递帧格式如图6所示,其中,安全导头中SPI取值为表2“层次SPI结构模型”中的1层中数值,对SDLS协议数据单元进行传递。

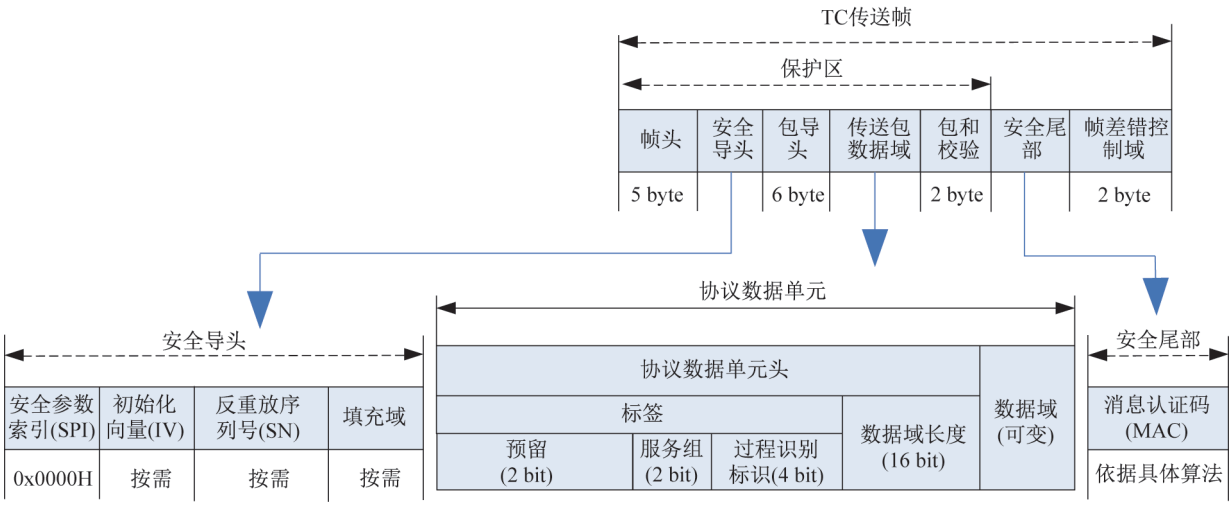

图 6 基于SDLS的PDU传递帧格式设计

Fig.6 Format of PDU transfer frame based on SDLS

常态下,航天器内部预加载SA及与其相关联密钥、数据保护认证算法(见表4),通过关联VC的SA启动命令以及SA停止命令实现遥控数据的握手传递。

由于认证保护算法的强度要求,而定期对SA挂钩密钥进行更迭时,可通过SA密钥关联/解关联

PDU命令予以实现，如图7所示。在应急态下，当需要实现星地密钥传递，以及之后的密钥关联变更等需求时，通过表4中的PDU指令对SA管理模式进行切换，如图8所示。

表4　SA管理PDU定义

Tab.4　PDU design for SA management

序号	服务组(Service Group，SE)(2 bit)		过程识别标志(Proc. Ident，PI)(4 bit)	数据域填充内容	意义解析
1	01	意义：从地面控制站传送PDU至航天器终端	0001	SPI序号＋认证状态标志＋(安全导头的IV长度＋安全导头的反重放SN长度＋安全尾部长度)＋(认证算法标识/认证模式标识)	SA生成。标识该生成的SA采用的保护方式、安全导头及安全尾的构成
2	01		0110	SPI序号＋新认证密钥ID号＋新反重放序列值＋新IV值	SA密钥关联。通过密钥ID号，标识该SA使用的具体密钥
3	01		1011	SPI序号＋VC号	在特定VC上启动SA
4	01		1110	SPI序号	停止对应序号的SA
5	01		1001	SPI序号	SA与当前密钥解关联。在解关联后，可以通过PDU指令将另一密钥与之相关联
6	01		0100	SPI序号	SA删除

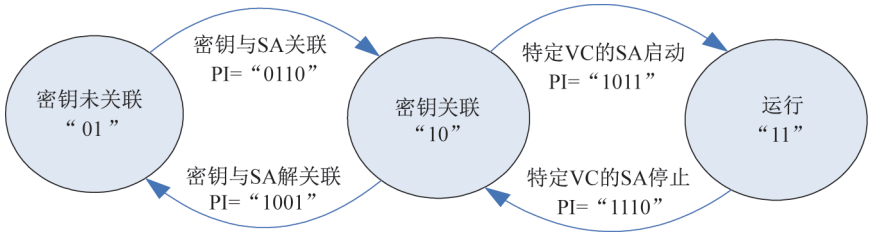

图7　SA管理常态状态模型

Fig.7　Normal state model of SA management

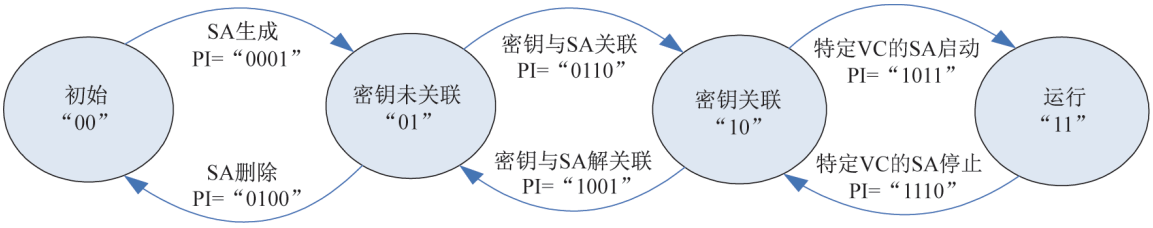

图8　SA管理应急状态模型

Fig.8　Emergency state model of SA management

2.3　密钥生存周期设计

对遥控数据保护控制的密钥结构进行两层设计，见表5。在航天器任务实施前，“主密钥”以及部分“会话密钥”预加载在星载可编程只读存储器(Programmable Read-Only Memory，PROM)中。常态下，考虑到认证算法保护强度要求，定期会对运行中的“会话密钥”进行“去活”处理，执行过程如图9所示。当处于应急状态时，星地需要实现会话密钥的传递，则PDU密钥上注指令、PDU密钥激活指令被执行，执行过程如图10所示，相关密钥管理PDU定义见表6。

表 5 密钥结构模型

Tab.5 Key structure model

序号	密钥设计分类		来源	意义
1	主密钥	PDU 认证密钥	星上预存	用于对 PDU 指令进行认证
		“会话密钥”加密密钥		用于对上注的“会话密钥”进行加密
2	会话密钥		1) 星上预存;2) 通过空间数据链路进行上注	用于上行指令/数据的来源合法性、数据完整性的认证

图 9 密钥生存常态周期模型

Fig.9 Normal cycle model of key life

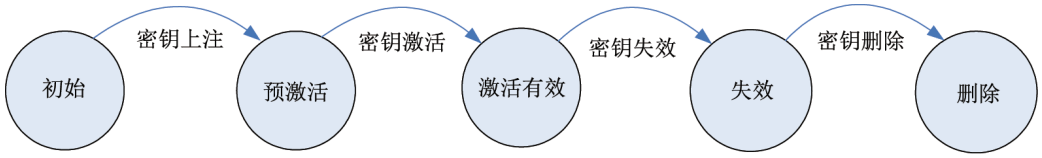

图 10 密钥生存应急周期模型

Fig.10 Emergency cycle model of key life

表 6 密钥管理 PDU 定义

Tab.6 PDU design for key management

序号	服务组 SE(2 bit)		过程识别标志 PI(4 bit)	数据域填充内容	意义解析
1	00	意义:密钥管理	0001	主密钥 ID+上注会话密钥 ID+上注会话密钥的具体值	会话密钥上注。执行该指令的 TC 传送帧中,利用主密钥 ID 对上注密钥进行加密以及认证
2	00		0010	待激活的会话密钥 ID	会话密钥激活,开始应用工作
3	00		0011	待失活的会话密钥 ID	会话密钥失活,应用工作结束
4	00		0110	待删除的会话密钥 ID	会话密钥删除

3 遥控认证保护算法设计

3.1 认证保护强度的确定

航天器任务的性质决定了测控系统对通信保护强度的需求,涉及任务自身的保密要求和开展任务的周期。

某航天器测控系统具有如下典型要求:任务期内,要求敌方穷举攻击的成功概率不大于 P_r,最小上行遥控帧的码长为 L(含认证尾码),上行遥控码速率为 C_r,任务周期为 T,遥控认证尾码长设为 N,则对所有遥控认证尾码完成一次穷举攻击所需时间为 $2^N \cdot L/C_r$。假设在任务周期内敌方持续对该航天器进行穷举攻击,要满足其攻击的成功概率 $T \cdot C_r/(2^N \cdot L) \leqslant P_r$,则消息认证尾码的长度应满足 $N \geqslant \log_2(T \cdot C_r/(P_r \cdot L))$[15]。当设计航天器寿命周期为 10 a,遥控上行码速率为 2 000 bit/s 时,最小遥控帧长为 440 bit。经理论计算,使其穷举攻击的成功概率 $\leqslant 10^{-28}$ 的消息认证码的长度设计至少为 124 bit。本文设计消息认证码的长度为 128 bit,穷举攻击的成功概率 $\leqslant 10^{-31}$。

需要注意的是,在工程实践中,普遍通过综合平衡任务的安全强度需求与为满足该需求所建立的系统软硬件开销,合理制定数据保护机制。事实上,由于星载遥控具有特定的协议格式,即便敌方对认证保护算法进行的穷举攻击,理论上能找到特

定的碰撞实例，也基本无法被航天器识别且动作。

3.2　算法设计

以Key作为输入密钥，长度320 bit，M为输入帧信息（遥控帧主导头＋安全导头＋帧数据域）。

1）在Key后面填充0，得到512 bit的Key1。

2）将Key1和掩码字符串（MASK1）进行异或运算得到Key_c1。其中，MASK1的构成：遥控帧安全导头中初向量IV前48 bit重复10次＋初向量IV前32 bit，共512 bit。

3）将M与Key_c1进行拼接，输入至MD5算法模块进行运算，输出散列值HV，长度128 bit。

4）将Key1和掩码字符串（MASK2）进行异或运算得到Key_c2。其中，MASK2的构成：遥控帧安全导头中初向量IV后48 bit重复10次＋初向量IV后32 bit，共512 bit。

5）把HV与Key_c2进行拼接，输入至MD5算法模块再进行运算，输出散列值HV1，长度128 bit，作为最终的遥控认证码。其中，MD5算法是一种密码散列函数，其主要步骤如下[16]：

步骤1　数据填充及长度扩展。首先对输入数据块进行填充补位，满足最终位数对512求模结果为448。实现过程为在数据块后填充长度为1 bit的“1”，其后全部填充“0”。之后继续填充表示原始数据长度的64 bit的长度值，至最终数据长度为512的整数倍。

步骤2　消息分组。以512 bit为单位，将输入数据进行划分，形成数据块$\mathrm{Block}_0,\cdots,\mathrm{Block}_N$。将每一个数据块划分为16个小组$M_0,\cdots,M_{15}$，每个小组32 bit。

步骤3　数据处理。将步骤2中每个Block数据块的处理过程划分为4轮，每轮16步，每步的执行如图11所示。其中a、b、c、d为32 bit链接变量并进行初值设置（初值记为A、B、C、D）；M_j为上述Block数据块中划分的数据小组，32 bit数据；t_i（$i=0,1,\cdots,16$）为设定的不同的常量；操作函数（Round1、Round2、Round3、Round4）分别由“与”“或”“非”逻辑组成的逻辑函数，第1轮采用Round1函数、第2轮采用Round2函数、第3轮采用Round3函数、第4轮采用Round4函数，$\ll k$为循环左移k位。

经过64步处理后的a、b、c、d链接变量再与初始设定值（A、B、C、D）进行逻辑加，最终得到新的链接变量值，该链接变量继续作为下一个Block数据块处理的初始链接变量，依次计算，当所有数据处理完成，将最终得到的链接变量进行顺序级联并输出，即为MD5计算模块的输出值。

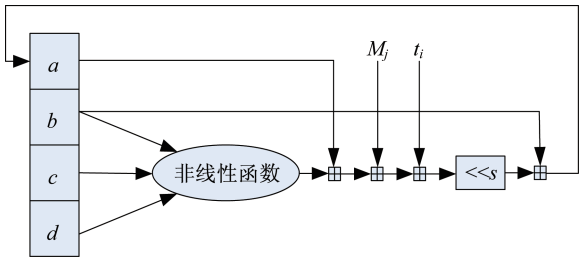

图11　MD5的一个执行过程

Fig.11　An execution process of MD5

4轮操作如下：

Round1(a,b,c,d,M_j,k,t_i)为

$$a=b+((a+(F(b,c,d)+M_j+t_i)\ll k) \quad (1)$$

Round2(a,b,c,d,M_j,k,t_i)为

$$a=b+((a+(G(b,c,d)+M_j+t_i)\ll k) \quad (2)$$

Round3(a,b,c,d,M_j,k,t_i)为

$$a=b+((a+(H(b,c,d)+M_j+t_i)\ll k) \quad (3)$$

Round4(a,b,c,d,M_j,k,t_i)为

$$a=b+((a+(I(b,c,d)+M_j+t_i)\ll k) \quad (4)$$

以下是每轮操作中用到的4个非线性函数（每轮1个）：

$$F(b,c,d)=(b\wedge c)V((-b)\wedge d) \quad (5)$$

$$G(b,c,d)=(b\wedge d)V(c\wedge(-d)) \quad (6)$$

$$H(b,c,d)=b\oplus c\oplus d \quad (7)$$

$$I(b,c,d)=c\oplus(bV(-d)) \quad (8)$$

式中：“$\oplus$”为“异或运算”；“V”为“或运算”；“$\wedge$”为“与运算”；“$-$”为“取反运算”。

4　遥控认证保护实现

某卫星综合电子的遥控认证系统采用上述方案，其地面侧基本认证业务流程如图12所示，星上侧流程相反。硬件平台基于反熔丝FPGA（现场可编程门阵列，使用AX2000）＋PROM（用于预存密钥）。实现了SA管理调度、密钥管理调度、遥控指令/数据的认证保护，具备重放鉴别、认证错误鉴别功能，程序算法的核心参数见表7，相关测试性能见表8。

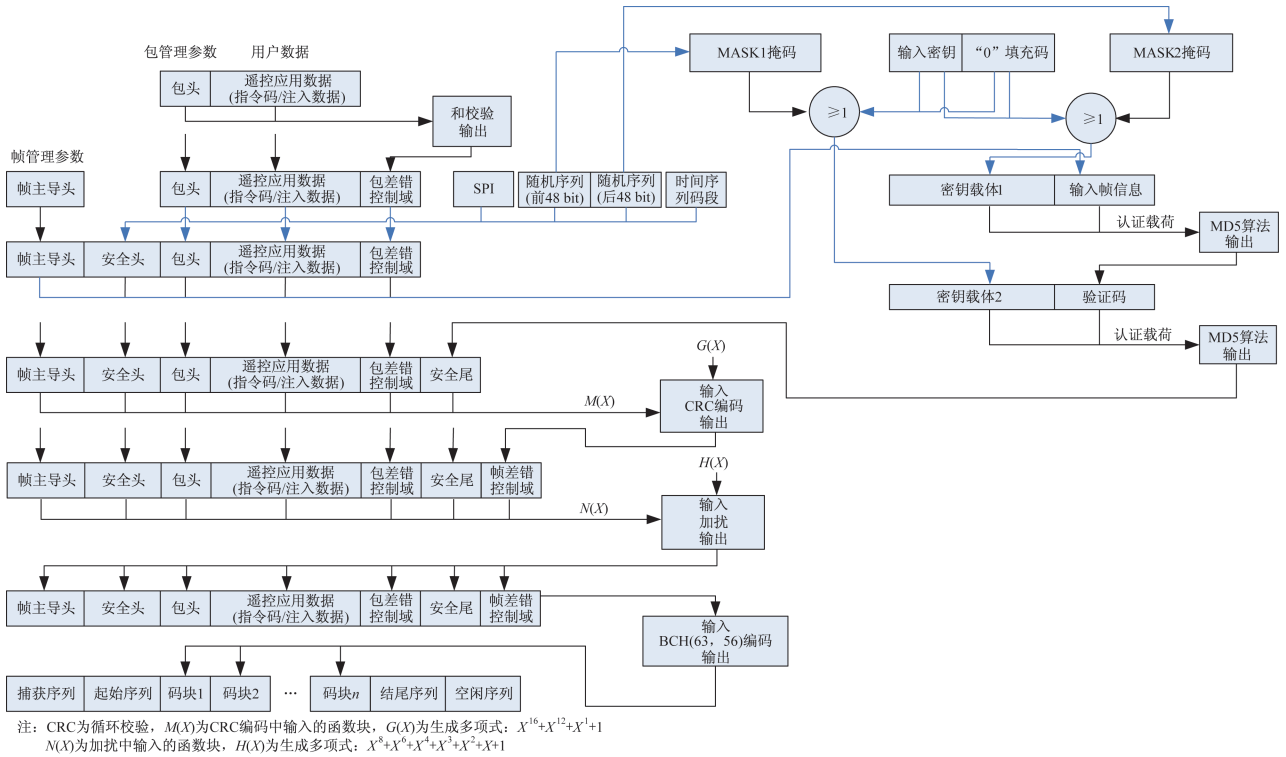

图 12 上行遥控认证业务流程

Fig.12 TC authentication business process

表 7 AX2000 平台算法核心参数

Tab.7 Core parameters of the algorithm running on the AX2000 platform

参数	数值
SEQUENTIAL/%	43.61
COMB/%	62.72
LOGIC/%	56.35
RAM/FIFO	6/64
频率/MHz	11.059 2

表 8 试验性能表

Tab.8 Test performance table

序号	试验项目	设计要求	测试结果
1	重放攻击保护	卫星生命周期内接收到相同的上行遥控帧,认证不予通过	上行注数(4种长度)、上行指令(32条)不响应。重放攻击计数+1,通过下行遥测返回
2	认证攻击保护	卫星接收到的上行遥控帧中,遥控数据被篡改或者认证码被篡改,认证不予通过	上行注数(4种长度)、上行指令(32条)不响应。认证错误计数+1,通过下行遥测返回
3	密钥攻击保护	卫星接收到的上行遥控帧所使用的保护密钥与星上使用保护密钥不一致,认证不予通过	动态随机生成保护密钥,在遥控码速率为2 000 bit/s条件下,持续利用非法密钥保护的遥控帧进行上注攻击,进行强度测试。上行注数、上行指令持续不响应。认证错误计数持续累加,通过下行遥测返回
4	SA管理调度	1) SA常态模式可切换 2) SA应急模式可切换	1) 实现认证保护挂钩密钥的切换,使用的密钥遍历了星上预存密钥库;2) 实现3路VC的SA启动;3) 实现了上行注数(4种长度)、上行指令(32条)的认证服务
5	密钥管理调度	1) 密钥生存常态模式可切换 2) 密钥生存应急模式可切换	1) 实现预存密钥"去活"处理。地面使用"去活"后的密钥进行数据保护的遥控帧进行测试,星上不响应,认证错误计数+1,通过下行遥测返回。2) 密钥上注成功、使用激活后的上注密钥开展认证服务成功,上注密钥"去活"功能、"删除"功能均有效。地面使用"去活"或"删除"后的密钥进行数据保护的遥控帧进行测试,星上不响应,认证错误计数+1,通过下行遥测返回

5 结束语

本文基于CCSDS分包遥控系统的层次结构、SDLS协议模式，设计了遥控认证帧格式结构、保护范围。同时，针对上行遥控的认证保护机制与CCSDS空间遥控链路COP-1传输控制协议之间存在“闭锁”风险，设计了COP传送控制流程。此外，对SA结构和运行管理机制进行了设计，对密钥结构和运行管理机制进行了设计，运用了集成密钥结构的增强型MD5算法对星载遥控认证保护进行了算法实现。上述方案具备遥控数据完整性鉴别、来源合法性鉴别、防“重放攻击”、防“流量分析”攻击等性能，可实现“认证算法的动态维护”“密钥生存控制”“认证参数的星地维护”等功能，满足民用航天器遥控单认证体制的任务需要。

参考文献

[1] CCSDS. Space data link security protocol-summary of concept and rationale: 350.5-G-1 [S]. National Aeronautics and Space Administration, 2018.

[2] CCSDS. CCSDS cryptographic algorithms: 352.0-B-1 [S]. National Aeronautics and Space Administration, 2012.

[3] CCSDS. CCSDS data link security protocol: 355.0-B-1 [S]. National Aeronautics and Space Administration, 2015.

[4] CCSDS. Space data link security protocol-extended procedures: 355.1-B-1 [S]. National Aeronautics and Space Administration, 2020.

[5] 陈红，周钠，佟晓筠，等.CCSDS-TC协议安全技术分析研究[J].南京大学学报(自然科学)，2018，54(3)：548-554.

[6] 刘兰，姚行中，王振宇，等.适用于CCSDS的“一帧一密”加/解密方案的FPGA实现[J].计算机工程与应用，2015，51(10)：84-88.

[7] 杨亚辉.CCSDS认证加密技术研究[D].沈阳：沈阳航空航天大学，2011.

[8] 张磊，周君，唐朝京.认证加密算法在CCSDS遥控协议中的应用研究[J].电子与信息学报，2009，31(2)：343-348.

[9] CCSDS. Telecommand summary of concept and rationale: 200.0-G-6 [S]. National Aeronautics and Space Administration, 1987.

[10] 张庆君，郭坚，董光亮.空间数据系统[M].北京：中国科学技术出版社，2016.

[11] 张磊，张权，唐朝京.COP-1协议参数确定方法及综合性能分析[C]//第十三届全国信号处理学术年会论文汇编.2007：408-413.

[12] FISCHER D, MERRI M, ENGEL T. Introducing a generic security extension for the packet TM/TC protocol stack [C]// 4th ESA International Workshop on Tracking, Telemetry and Command Systems for Space Applications. Washington D. C., USA: IEEE Press, 2007: 235-242.

[13] FISCHER D, ENGEL T, MERRI M. Approach of the integration of data security in the CCSDS packet TM/TC standards [C]// 9th International Conference on Space Operations (SpaceOps). Washington D. C., USA: IEEE Press, 2006: 524-531.

[14] 刘德波，王明华，张磊，等.CCSDS遥控协议数据认证保护研究[J].现代电子技术，2008，31(7)：76-79.

[15] 陈宜元.卫星无线电测控技术[M].北京：中国宇航出版社，2009.

[16] RIVEST R L. The MD5 message digest algorithm IETF [M]. Ganbridge, MA: IETF, 1992.