第35卷 第12期 计 算 机 工 程 2009年6月
Vol.35 No.12 Computer Engineering June 2009
·安全技术· 文章编号：1000—3428(2009)12—0125—03 文献标识码：A 中图分类号：TP393.08

# 基于CCSDS的空间网络跨层安全接入研究

钱雁斌，陈性元，杜学绘
（解放军信息工程大学电子技术学院，郑州 450004）

**摘 要：**针对高度开放、拓扑多变的空间网络容易受到各种类型的攻击，仅在某一单独层次实施安全防护不能满足空间网络高等级的安全需求的问题，在深入分析CCSDS尤其是数据链路层AOS协议特点的基础上，提出一种空间网络跨层安全接入机制，在网络层和数据链路层建立一体化防护体系，探讨CCSDS协议体系下的实现方式，当对已认证节点信任发生变化时能进行自动调整和恢复，有效提高空间网络移动接入的安全性、适应性及接入性能。

**关键词：**空间网络；跨层安全接入；高级在轨系统

# Research of Layered Secure Access for Space Network Based on CCSDS

QIAN Yan-bin, CHEN Xing-yuan, DU Xue-hui
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

**【Abstract】** Due to the open nature and the frequent network topology changes, space network is vulnerable to various attacks. It can not satisfy higher levels of security requirements of the space network that just implement protection in only one protocol layer. This paper analyzes thoroughly characteristic of CCSDS in particular in the data link layer Advanced Orbiting Systems(AOS) protocol, and proposes the layered secure accessmodel mechanism at the data link and network layers, expecting that it can establish integration access protection system. This paper also discusses the realization way under the CCSDS protocol system. When the trust to certain node that is authenticated changed, the mechanism proposed can automatic reaction in time, and enhance the security, the compatibility and performance of secure access.

**【Key words】** space network; layered secure access; Advanced Orbiting Systems(AOS)

## 1 概述

科技的发展和信息化时代对天地一体化的空间通信组网的需求越来越迫切。空间独特的环境特点使地面网络协议难以直接应用于空间网络，为此空间数据系统咨询委员会(CCSDS)发布了一系列的CCSDS建议，经过多次重构和扩充，逐渐形成了空间通信标准协议簇。目前较多国家和地区的空间组织和商业机构都采用CCSDS标准，如国际空间站、NASA哥达德飞行中心、NASA喷气推进实验室、ESA欧洲空间技术中心等。在国内，中国空间技术研究院、总装跟踪与通信技术研究所、中国航天标准化研究所等单位对CCSDS标准进行了长期的跟踪研究。实践-5号卫星、载人航天工程载人飞船系统、探月工程等也都采用CCSDS标准。

但空间网络具有高度开放、拓扑结构动态多变、无清晰的安全边界、通信方式不对称等特点，节点可能会频繁地加入与退出空间网络，空间信息安全问题十分突出。空间网络系统能否被普遍应用，不仅与相关技术准备和设备研发相关，也与系统的安全保障能力有关。移动安全接入是空间网络信息安全防护的第1道防线，对保护整个空间网络的安全具有十分重要的意义。地面网络现有的安全接入机制并不能满足空间网络的需求，同时CCSDS建议在网络层指定了SCPS-SP协议来保护端到端安全，但明确指出空间数据链路协议并不是安全协议[1]，而在单一层次实施安全防护无法满足高等级安全需求[2]，尤其对于无线接入而言，数据链路层防护是不可缺少的一环。

## 2 CCSDS网络层和数据链路层安全

### 2.1 网络层安全

SCPS-NP是CCSDS建议提出的空间通信网络层协议，同时CCSDS也支持IPv4、IPv6协议。为提供端到端安全服务，CCSDS提出SCPS-SP协议，其概念来自于安全数据网络系统(SDNS)的安全协议3(SP3)、ISO的网络层安全协议(NLSP)、IPV6的加密安全载荷(ESP)和综合网络安全协议(INLSP)等。其中，SCPS-SP追求最优比特效率，以最小的通信开销，在空间任务通信中提供数据保护。SCPS-SP能提供有效的端到端机密性、完整性、鉴别服务或上述服务的组合。

在SCPS-SP中，网络层的地址信息必须以明文形式存在且允许协议数据单元进行路由。因为地址信息是不加密的，而SCPS-SP不提供对流量分析及干扰防护，所以必须在链路层提供对流量分析的保护，在物理层提供抗干扰机制。同时，SCPS-SP也不提供对重放攻击的防护，而是假定由传输层协议如SCPS-TP采用加密算法或序列号以抵御重放攻击。

### 2.2 数据链路层安全

由于空间和地面底层链路的差异，因此在链路层采用相同协议是不现实的[3]。CCDSD基于OSI参考模型中为空间网

**基金项目：**国家“863”计划基金资助项目(2006AA701416, 2007AA701309)

**作者简介：**钱雁斌(1981－)，男，博士研究生，主研方向：信息安全，空间网络；陈性元，教授、博士；杜学绘，副教授

**收稿日期：**2008-10-25 **E-mail：**qianyanbin@sina.com

络数据链路层定义了 2 个子层：数据链路协议子层和同步信道编码子层。数据链路协议子层定义了在空间链路上传输高层协议数据单元即数据帧的方法。同步信道编码子层定义了在空间链路上传输数据帖的同步和编码机制。CCSDS 为数据链路协议子层制定了 4 个协议：TM 协议，TC 协议，AOS 协议，Proximity-1 空间链路协议。其中，高级在轨系统(Advanced Orbiting Systems, AOS)协议是在常规在轨系统即分包遥测、分包遥控的基础上发展完善起来的空间网络数据链路层协议(属于 CCSDS 数据链路层的数据链路协议子层)。AOS 协议以标准化方式进行数据交换和处理，以更为经济有效的方式来满足不同空间节点和不同用户的业务需要，有效地提高了信道的效率和可靠性。因此，本文以 AOS 协议为基础来探讨空间网络数据链路层安全问题。

AOS 协议发送端的数据处理流程如图 1 所示[4]。

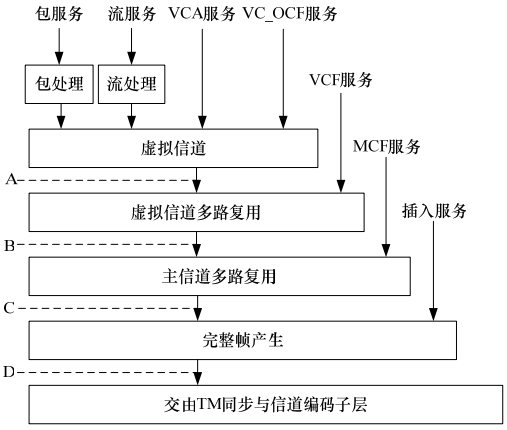


**图 1　AOS 协议发送端的数据处理流程**

接收端的数据处理流程与发送端正好相反。其中，虚拟信道产生功能用来建立基本的传输帧结构，产生传输帧头部，将包服务、流服务、VCA 服务中的 1 种协议数据单元放入传输帧数据域，并根据须填充虚拟信道运行控制域(可选)；虚拟信道复用功能则将同一主信道的多个虚拟信道以及 VCF 服务数据单元复用为一个传输帧；主信道复用功能是将同一物理信道的多个主信道以及 MCF 服务数据单元复用为一个传输帧，通常一个物理信道中仅存在一个主信道。完整帧产生功能是将最终完成传输帧的建立，并根据需要加入插入数据(可选)、加入帧头部错误控制和帧错误控制域编码。

AOS 协议本身没有提供任何的安全服务，须根据实际需要分析 AOS 的数据处理流程选择合适的服务、在合适的位置实施恰当的安全防护措施。

## 3　空间网络跨层的安全接入机制

通常的地面有线网络中，接入申请点直接通过位于受保护网络边界的网络接入点接入网络，而接入申请点与网络接入点之间的路由器、交换机等网络设备并不受保护，对来往数据流无条件转发。这对空间信息网络尤其是军事或其他高安全等级的应用是不可接受的。一方面，空间节点的资源有限，必须确保其只为合法有权限的用户服务，资源耗尽攻击、剥夺睡眠攻击正是针对空间节点这一特点的攻击形式。另一方面，采用自组网方式组建的空间网络，其信息节点既是通信中继节点也是信息处理节点。因此，必须将空间所有节点都纳入保护范围之内，无边界的空间网络意味着所有节点都是空间网络的边界，对接入申请点而言，每个节点都可以是网络接入点，只有当网络接入点认可接入申请点的身份和权限，才能为其开放网络服务、传递数据。同时，当前正在运行的许多空间节点，并没有组网功能，如部分在轨卫星仅仅支持物理层和数据链路层，通过链路密码机向特定地面接收站传输数据。考虑到空间网络的兼容性，应在支持端到端安全的同时支持这种链路直连通信的接入安全。

类似于其他无线通信网络，空间网络很容易受到各种被动、主动攻击，如窃听、复制、修改、删除等，针对空间网络还会引起的拥塞、传播不正确的路由信息，阻止服务正常的工作或完全关闭它们，针对空间节点的剥脱睡眠攻击、黑洞攻击等。仅在某一单独层次实施安全防护并不能满足高安全等级的空间自组织网络安全介入需求。而在多个协议层次上采用多重加密机制易产生重复敢应、引入安全缺陷、增加开发和操作成本[2,5]。因此，本文考虑结合数据链路层和网络层安全机制，建立一体化的跨层安全接入机制，在保证安全性的同时，避免多重加密，该机制如图 2 所示。

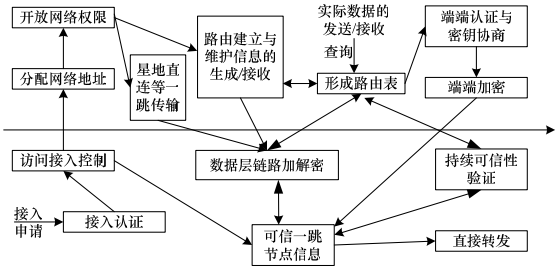


**图 2　空间网络跨层安全接入机制**

在空间节点新申请加入网络时，首先由数据链路层实施接入认证与访问接入控制，通过认证之前不开放所有的网络层以及更高层次服务。在通过接入认证确认节点的身份及入网权限后，开放网络层服务为其分配网络层地址(自动分配地址情况下)，可以参与路由的建立与维护，允许转发来自接入请求点的数据包。路由建立与维护过程中节点到节点的报文在数据链路层加密来确保数据传输的安全，同时以节点自身为发起/接收终端、一跳传输能到达目的终端的特殊通信数据(如星地链路直连)，也采用数据链路层加解密来保证机密性。当有实际报文的发送/接收时(多跳才能到达目的终端情况)，执行端到端的强认证与密钥协商，此时由端端密钥来保护端到端的安全，数据链路层不执行加密。

相邻节点(一跳)的可信性及与相邻节点的点到点网络控制信息(如路由)的安全由数据链路层提供，端到端安全则完全由网络层提供。为提高空间数据传输效率，实际数据传输在数据链路层并不加密(多跳情况下)，数据链路层在接入认证完成之后无法通过会话密钥维持这种可信性，因此，每个节点须维护自己相邻一跳可信节点信息，并定时对相邻节点进行持续可信性验证，可采用刷新认证等方式完成[6])，及时排除不可信节点(可信节点可能在遭受攻击后变为不可信节点、或攻击者冒充可信节点等)。任何途径节点数据链路层的数据，在数据链路层必须查询可信一跳节点信息，确保对方是可信节点方可发送。

一旦发现可能的恶意节点，在数据链路层将立即从可信节点信息中删除，并阻止数据向该节点发送，已传送到数据链路层的数据暂时缓存。网络层也同时阻止继续将数据发往该节点，对于转发数据应立即调整路由，通过其他路径传递给最终的接收端。网络层恢复之后，数据链路层将缓存的数据按新的路径转发出去。

## 4 基于CCSDS的空间网络跨层安全接入

### 4.1 链路层安全实施位置分析

AOS 协议的一个主要特征就是虚拟信道(VC)。VC 允许一个物理信道(MC)被多个高层数据流所共享，每一个 VC 可以有不同的服务需求。每一个通过 MC 传输的 AOS 传输帧都属于一个 MC 的一个 VC。AOS 向高层协议提供的服务从类型上说，包括异步、同步、周期，其包括数据包、流、虚拟信道访问、虚拟信道运行控制域、虚拟信道帧(Virtual Channel Frame, VCF)、主信道帧(Master Channel Frame, MCF)、插入等服务，见图 1。

文献[2, 5]讨论 AOS 协议安全实施位置时，都是基于加解密机制来分析的，很少考虑其他安全机制如接入认证、数据完整性、访问接入控制等。AOS 可实施的安全位置主要包括:

(1)位置 A，为各个虚拟信道单独选择安全机制和运行模式。若在位置 A 采取加密措施，仅 VCF、MCF、插入服务以及错误控制域支持相应交叉支撑业务，可利用 VCF 服务提供接入认证和访问接入控制服务。

(2)位置 B，为各个主信道单独选择安全机制和运行模式。采取加密机制将导致仅 MCF、插入服务以及错误控制域支持交叉支撑业务，可利用 MCF 服务提供接入认证和访问接入控制服务。

(3)位置 C，对插入域以外的完整的帧数据域进行保护。采取加密机制将导致仅插入服务和错误控制域支持交叉支撑业务，可采用插入服务提供接入认证和访问接入控制服务。

(4)位置 D，对完整的数据帧进行保护，在位置 D 进行加密将导致交叉支撑业务在数据链路层完全失效，帧头部错误控制和帧错误控制域因成为密文而无效，不能方便地提供接入认证和访问接入控制服务。

### 4.2 基于CCSDS的空间网络跨层安全接入设计

在空间网络跨层安全接入机制当中，数据链路层关注相邻一跳节点的可信性，而不对具体应用进行区分，针对发往某个空间节点的所有数据帧，对应于 AOS 协议来说就是对应于一个主信道，对应于图 1 的位置 B，多路虚拟信道复用为一个主信道之后。因此，接入认证和访问接入控制应该选择在位置 B。而对于加密机制来说，若针对高层的不同应用提供不同强度的安全服务，加密应该在位置 A 实施，否则可以同时在位置 B 实施，使安全服务形成一个清晰的安全层次。对 AOS 协议进行如下改进:

(1)在图 1 的位置 B 处，添加安全服务层，负责网络接入控制和链路加密，只有经过认证且权限允许接入的用户才能通过。

(2)对接入认证帧应作特殊标识，AOS 协议传输帧信号域的第 3 bit 和第 4 bit 为保留域[4]，不使用时应该被设置为“00”，因此，可定义这 2 个 bit 为“01”来标识特定 AOS 帧为接入认证帧，以提高接入认证效率。

(3)MCF 服务可以传输固定长度主信道中的 AOS 传输帧，同一主信道内只能存在一个 MCF 服务，这一特征也正好适合接入认证，因此可通过 MCF 服务来提供认证接口。

(4)在 AOS 建议中 SCPS-NP 等网络协议数据都通过包服务交由数据链路层处理，同时可以使用独立的协议实体通过多种服务(如流服务、VCA 服务、插入服务等等)传递到数据链路层，利用这一特性可设置一个跨网络层、数据链路层的独立协议实体来完成 SCPS-SP, SCPS-NP, AOS 的交互。

基于 CCSDS 的空间网络跨层安全接入的总体设计如图 3 所示。图中只列出了相关内容，省略了网络层以及数据链路层的包处理、流处理、VCA 服务等。

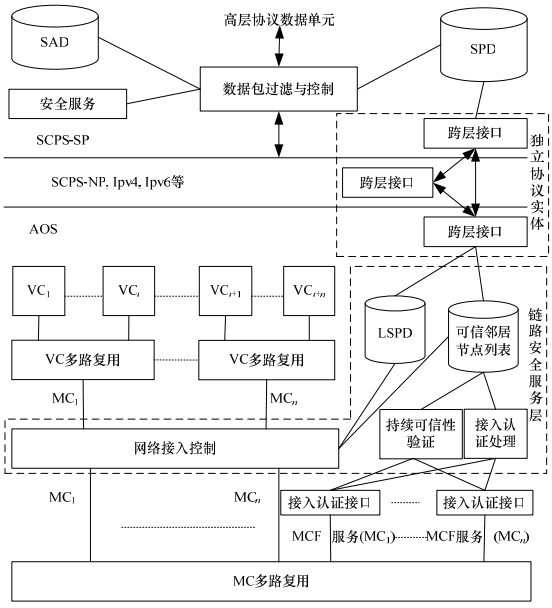


**图 3 基于 CCSDS 的空间网络跨层安全接入设计**

SCPS-SP 协议层次的数据包过滤与控制模块根据策略数据库 SPD，在 SAD 和安全服务模块的支持下，按 CCSDS 建议执行端到端安全防护。

链路层安全防护在 VC 多路复用与 MC 多路复用之间形成一个清晰的安全层，称为链路安全服务层。链路安全服务层主要由网络接入控制、接入认证管理、LSPD、可信邻居节点列表、持续可信性验证 5 个部分组成。网络接入控制负责过滤不同 MC 的数据，只允许经过认证且策略允许的 MC 数据通过;接入认证处理在每个主信道中以 MCF 服务提供一个接入认证接口作为认证代理，代理将数据传递到接入认证管理处统一处理所有的认证过程；可信邻居节点列表负责记录相邻的一跳可信节点信息，包括节点的地址、最近一次可信探测的时间、双方的密钥等等；LSPD 为数据链路层策略库，决定是否允许特点节点(主信道)访问、是否需要暂时阻止数据通过并缓存数据等，同时 LSPD 也可通过跨层接口与 SCPS-SP 的 SPD 交互并保持一致性，决定是否在数据链路层执行加解密操作;持续可信性验证也同样通过 MCF 服务提供一个接入认证接口，验证可信邻居节点列表中节点的可信性。

## 5 结束语

本文提出基于 CCSDS 的跨层安全接入方案，支持根据策略合理配置数据链路加密、网络层加密，在保证安全性的前提下，避免多层加密增加开发和操作成本。若安全需求远高于性能要求，跨层安全接入机制也支持在链路层和网络层同时加密，或只采用数据链路层加密，具有良好的兼容性与可扩展性。同时，当对已接入节点信任发生变化时，该方案能在数据链路层和网络层同时自动调整和恢复，继续安全的传递数据包，保证空间链路的可用性，提高了接入的安全性。

本文未指定任何具体的认证、密钥协商或加密算法，空间网络认证和密钥协商协议的设计应以减少计算开销、传输开销为目标，而加密算法则可采用现有的高效加密算法。文中提出的持续可信性验证问题，其参数设置的合理性将影响

(下转第 130 页)