空间信息网络安全协议综述

廖 勇[1,2] 樊卓宸[3] 赵 明[1]
(重庆大学飞行器测控与通信教育部重点实验室 重庆 400044)[1]
(西安电子科技大学陕西省网络与系统安全重点实验室 西安 710071)[2]
(重庆大学通信工程学院 重庆 400044)[3]

摘 要 针对空间信息网络安全协议展开综述。首先介绍了建设空间信息网络安全的意义,其次论述了国内外对空间信息网络安全协议的研究现状,然后重点对空间通信协议规范-安全协议(SCPS-SP)的核心关键技术——认证及加密算法进行详细分析。在此基础上,指出SCPS-SP在应用过程中遇到的挑战,并给出解决的思路和相关的建议。

关键词 空间信息网络,网络安全,空间通信协议规范-安全协议,认证,加密
中图法分类号 TN918 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.04.044

Survey on Security Protocol of Space Information Networks

LIAO Yong[1,2] FAN Zhuo-chen[3] ZHAO Ming[1]
(Key Laboratory of Aerocraft TT&C and Communication, Ministry of Education, Chongqing University, Chongqing 400044, China)[1]
(Shaanxi Key Laboratory of Network and System Security, Xidian University, Xi'an 710071, China)[2]
(College of Communication Engineering, Chongqing University, Chongqing 400044, China)[3]

Abstract This paper summarized the space information network security protocol. Firstly, we introduced the significance of construction of space information network security. Secondly, we discussed the research status at home and aboard of the space information network security protocol. Then we analyzed authentication and encryption algorithms in detail, which are the key technologies of space communication protocol specification-security protocol (SCPS-SP). On this basis, we indicated the challenges which SCPS-SP faced in the application, and gave some ideas and suggestions for solution.

Keywords Space information network, Network security, Space communications protocol specification-security protocol (SCPS-SP), Authentication, Encryption

1 引言

空间信息网络(SIN)是由具有空间通信能力的航天器(如卫星、深空探测器、载人飞船、空间站、航天飞机)和地面站共同组成的,以通过航天器的转发或反射来实现航天器之间、地面站之间以及航天器和地面站之间的互联互通功能的网络信息系统,它能把卫星、深空探测器、载人飞船、空间站、航天飞机和地面系统联系起来。SIN主要以航天器和地面站为网络节点,以立体动态的空间链路进行信息交互,航天器本身具有较强的综合处理功能[1]。SIN集成了各种空间信息获取、传输、处理、分发和应用系统,能够实现快速智能的信息共享和综合利用,极大地促进了制信息权的优势的获得,是未来信息化战争的核心技术支撑[2]。

空间信息网络安全技术针对SIN中拓扑、节点和无线链路的特性,研究并设计各种安全方案以提高空间网络的抗攻击能力并确保传输数据的安全性[3]。可以说,空间网络安全技术是SIN的一项极为重要的关键性技术。一方面,与地面通信系统相比,空间通信系统的覆盖范围更广,拓扑结构变化更加频繁,数据在传输过程中更容易受到攻击,而且系统的计算资源和功率有限,链路带宽比较窄,缓存空间及处理能力有限,传统的地面通信因特网安全协议(IPSec)并不适用于空间通信系统;另一方面,空间网络由于可能采用现有的标准网络协议或改进协议,仍然面临已有的甚至更大的网络安全威胁[2]。

发展SIN是未来航天器活动的必然要求[3],然而空间信息网络安全体系结构和安全机制是SIN研究、设计、部署、应用中至关重要的基础性、关键性问题。SIN在军事国防方面具有非常重要的意义,对安全性有更高的要求,所以避免类似

到稿日期:2016-03-02 返修日期:2016-05-11 本文受国家自然科学基金重大研究计划培育项目(91438104),国家自然科学基金项目(61571069),陕西省网络与系统安全重点实验室开放基金(NSSOF1500101),重庆大学中央高校基本科研业务费重点项目(CDJZR165505)资助。
廖 勇(1982—),男,博士,副研究员,CCF高级会员,主要研究方向为宽带无线通信与网络,E-mail:liaoy@cqu.edu.cn;樊卓宸(1993—),男,主要研究方向为宽带无线通信,E-mail:chaselfan@outlook.com(通信作者);赵 明(1994—),女,主要研究方向为宽带无线通信。

的地面信息网络受到安全威胁甚至是攻击就显得非常必要。

空间网络安全技术是应对空间网络安全威胁和保障空间信息系统安全的技术基础。从攻击发起者的角度，安全威胁可能来自无线链路、核心网络实体或用户终端；从网络协议层次的角度，安全威胁可能来自物理层、链路层、网络层、传输层和应用层中的任意一个或多个层次。只有充分考虑各种可能的威胁来源和攻击方式，在每个协议层次均采用适当的安全机制和安全策略，制定合理高效的总体安全解决方案，才能抵御各种可能的网络攻击。

网络安全技术与空间组网的其他关键技术具有不可分割的关系，如路由技术和移动性管理技术。在研究空间组网中的各项关键技术时，必须与网络安全技术的研究综合起来考虑。

然而地面有线和无线网络中的安全技术并不完全适合空间网络，必须针对空间网络的异构性、层次性、链路时延长、拓扑变化快、误码率高等特点，充分考虑其对安全方案带来的不利影响，设计合理、高效的安全机制和安全解决方案[2]。

综上，针对目前国内对 SIN 的日益重视且 SIN 安全协议研究存在的不足，本文对其安全协议进行了较为全面的综述，主要工作如下：首先阐述了研究 SIN 安全协议的重要性；其次针对目前安全协议中研究最为广泛的空间通信协议规范-安全协议(SCPS-SP)，分析了其关键技术，并重点对其中的认证加密算法进行了分析、对比和小结；最后总结了 SCPS-SP 在研究和应用过程中面临的挑战，给出了对应的建议，并对未来的研究进行了展望。

2　研究现状

目前，空间信息网络安全标准的国内外研究现状如表 1 所列。

表 1　空间信息网络安全的研究现状

参考文献	组织或国家(地区)	采用的空间安全标准
文献[4-5]	CCSDS	SCPS-SP
文献[6]	欧洲	ECSS-E-ST-50-xxC
文献[7]	美国	NASA-STD-28xx EA-STD-xx EA-SOP-00xx
文献[8]	中国	SCPS-SP

(1)CCSDS

国际上有多个组织和公司专门针对空间通信的特点设计了各种开源和商业的空间通信协议栈，而在众多的空间通信协议栈中，最成功、最有名的就是由国际空间数据系统咨询委员会(CCSDS)[4]制定的空间通信协议规范(SCPS)[5]。

CCSDS 于 1999 年提出了 SCPS 协议，即 CCSDS 以 IP 协议为基础，进行适当的修改和扩充，提出了 SCPS 协议。SCPS 以地面网络普遍应用的 TCP/IP 4 层分层结构为模型[5]，针对空间传输环境特性，修改和扩展了 TCP/IP 协议栈，制定了网络协议(SCPS-NP)、安全协议(SCPS-SP)、传输协议(SCPS-TP)和文件协议(SCPS-FP)。

(2)欧洲和美国

1)安全标准

欧洲和美国都分别构建了空间安全防护的顶层设计，并且相关的法律和制度建设比较完善。欧空局(ESA)以欧洲航天标准化合作组织(ECSS)官方网站为平台，建立和发布包含安全标准在内的各种标准[6]。其中，ECSS-E-ST-50-xxC 系列标准为 ESA 空间通信和保密的标准，并且 ECSS 标准广泛参考和引用了 CCSDS 标准里提供的关于空间数据系统安全架构的实践建议等。

美国国家航空航天局(NASA)也先后建立了标准共享平台、标准和技术援助资源平台。NASA 安全标准主要有 NASA-STD-28xx 系列、EA-STD-xx 系列以及 EA-SOP-00xx 系列。这些标准吸收了部分军用、国家、国际标准和 CCSDS 标准[7]，航天器网络安全域则根据任务需要依照文献[6]及其他相关的 CCSDS 文档进行实施。

2)系统安全技术

ESA 和 NASA 采用的安全技术来源广泛，充分利用了安全技术发展的成果和国家公共资源，特别是在密码技术方面，美国数据加密标准[9](DES)就是一个曾经使用很普遍的常规对称加密算法。目前 ESA 和 NASA 广泛使用的是高级加密标准(AES)，在公钥加密和消息认证范围则为 RSA(Rivest Shamir Adlemen)等[10]。

(3)中国

我国非常重视空间信息网络的研究，国家自然科学基金委分别于 2013 年－2016 年连续发布了“空间信息网络基础理论与关键技术”重大研究计划项目[11]。特别地，我国高度重视研究空间信息网络安全。文献[8]通过分析我国未来的航空航天任务需求，提出了适合我国国情的空天一体化网络架构，探讨了需要突破的关键技术，以及基于此体系架构的各种网络安全传输协议。但是，目前这些技术大部分还都处于理论论证和模拟实验阶段，并没有大规模的应用。目前在空间信息网络安全的不同层面，已经提出并成功实施了各种技术支撑协议，如高级在轨系统(AOS)协议[12]、增强的 IPSec 协议，特别地，还有 SCPS-SP 协议等，但都还处于局部研究和应用阶段。我国并没有像美国和欧洲那样大规模地研究和应用 SCPS-SP。如何从系统工程的角度完整地设计出一整套适合复杂、动态变化的空间网络系统运行的通信协议及安全保障措施还没有实质性进展。总体说来，目前我国在空间信息网络安全方面相对一些发达国家而言比较落后，还有待进行深入的研究和实际的应用。

3　SCPS-SP 认证加密算法

由第 2 节可知，目前空间信息网络安全领域研究的热点是空间通信安全协议，而在这一领域，研究热度较高和成果较多的是 SCPS-SP，本节重点阐述其中的关键技术之一——认证加密算法。

SCPS-SP 应用在空间通信系统的网络层和传输层之间，其作用就是将传输层协议数据单元(T-PDU)经过处理后封装成安全协议数据单元(S-PDU)，并且可以根据通信用户的不同安全需求对这些来自传输层的数据单元提供相应的安全性服务[13]，主要包括端到端的空间数据机密性、完整性和认证服务 3 个方面[14]。前两个方面主要通过设计安全高效的

加密策略来实现，第三个方面主要是依靠 SCPS-SP 定义的数据封装规则，通过封装通信双方的网络地址来实现。SCPS-SP 协议的主要特点表现为最小的通信开销和最佳比特率，这些优势在通信资源受到严重限制的空间通信系统中得到了较好体现[15]。

然而提高空间通信系统安全防护性能通常是以降低该系统的通信效率为代价的，而且不同的空间通信任务有着不同的安全防护需求，若对所有的空间通信任务采用同等级的安全防护措施则必然给通信系统性能和效率带来重大影响，对 SCPS-SP 的研究带来一些技术挑战[16]。目前，在 SCPS-SP 领域研究的关键技术有 SCPS-SP 与地面 IPSec 网关的转换技术[17]、针对 SCPS-SP 不能提供抗流量分析保护的缺陷而设计的具有流量分析保护功能的空间通信安全隧道协议[18]，以及下文将要提到的 SCPS-SP 认证加密等关键技术，其中认证加密算法是目前研究的热点，相对来说研究成果较多。

针对认证加密技术在 SCPS-SP 上的使用，文献[19]对 SCPS-SP 进行了改进，很大程度上推进了 SCPS-SP 的应用。原始的 SCPS-SP 只是将较为单一的加密算法应用于空间通信系统，并没有具体规定用于数据保护的加密算法。因此尽管 SCPS-SP 在一定程度上解决了空间数据加密开销较大的问题，却没能较好地解决传输数据的安全性问题。基于 SCPS-SP 的混合加密算法可以同时解决安全性与加密开销两个方面的难题。

文献[20]提出一种基于 GCM (Galois/Counter Mode)[21] 认证加密算法的具有多级别安全自适应的改进 SCPS-SP 协议，其目的是一定程度地提升 SCPS-SP 协议的安全性能。GCM 具有效率高、性能好、可证明安全等特点，是针对高传输速率的网络应用而提出的一种认证加密算法，并且 GCM 只需要用到 AES 的加密算法。针对 GCM 的上述优点，可以将其应用到改进的具有多级别安全自适应的 SCPS-SP 协议中。仿真实验结果表明，改进后的 SCPS-SP 协议能够满足空间通信系统对数据保护的要求，并且在安全性能方面有明显的提升。实验中，根据每个 GCM 状态所使用的存储空间字节数的差异，将其划分为 GCM(64k)，GCM(8k)，GCM(4k)和 GCM(256) 4 种，并且对处理器每 1000 时钟周期所能处理的数据量的性能进行比较分析，仿真结果如图 1 所示。

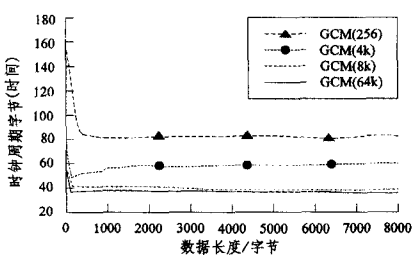

图 1 认证加密性能比较

由图 1 可知，随着数据长度的增加，GCM 算法处理数据的性能逐渐增加且趋于稳定，在数据长度为 1024byte 时，性能达到最高。测试在引入认证加密算法 GCM(64k)前后传输 1Mbyte 文件时的协议性能，仿真结果如图 2 所示。

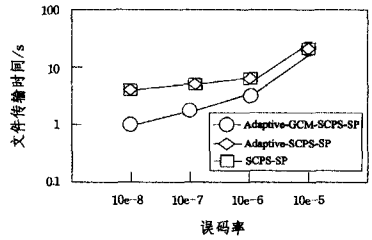

图 2 认证加密性能比较

图 2 中，Adaptive-SCPS-SP 即为改进的具有多级别安全的自适应 SCPS-SP[18]。与 SCPS-SP 相比，Adaptive-SCPS-SP 在 SCPS-SP 的 S-PDU 保护头中增加了安全选项标识域、安全级别标识域、抗重放数据域，从而提供了 SCPS-SP 中没有的自适应多级安全功能和抗重放服务。由以上仿真结果可知，在信道误码率较小的情况下，在 Adaptive-SCPS-SP 中引入 GCM 认证加密后的 Adaptive-GCM-SCPS-SP 能有效地减少文件传输的总时间，提高文件加密认证速度。但在信道的误码率较大的情况下，由于重传数据包往返的时间过大，因此该算法的高效性可能无法得到体现。

文献[22]研究了基于 SCPS-SP 的 DES 与 RSA 混合加密策略，该策略能很好地解决空间通信链路中存在的安全威胁问题。仿真实现时，每一个数据单元被接收方成功接收后都会显示传输时间，所有数据单元传输完毕后会得到传输所耗费的总时间及传输速率。实验通过测试传输不同数据量大小的文件信息得出数据量大小与信道传输时间及速率之间的关系，并将其作为依据来评价加密策略的性能。信道传输时间与传输速率随数据量大小的变化趋势如图 3 所示。

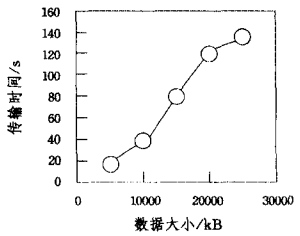

图 3 数据大小与传输时间和速率之间的关系

如图 3 所示，传输时间会随着数据量的增大而呈近似线性的增长，并且传输速率也会随数据量的增大而逐渐增大，增加到一定程度时，增长幅度会逐渐变小，最后趋近于一个数值。由于 RSA 加密算法的速度比 DES 算法慢很多，这个过程消耗的时间会相对比较多，因此若一次传输的数据较少，则建立安全通道所消耗的时间占整个数据传输时间的比值较大，传输速度就会偏低。数据量逐渐增大时，若 DES 密钥的长度并没有发生改变，则耗费时间的 RSA 算法处理的数据量占总体数据量的比重就会变小，加密速率就会得到一定的提高。

此外，文献[23]针对被加密的数据可能被非法利用以及 SCPS-SP 定义了安全等级的概念而没有给出具体的使用标准这两点不足，分别做出了以下两点改进：1)具体化 SCPS-SP 中的分等级保护概念，分为 A,B,C 三等，用户可根据需要选择不同的加密(DES/3DES/AES)和认证(SHA-1/MD2/MD5)组合；2)在 SCPS-SP 现有的服务上增加抗重放功能，即

发送端将安全联盟中的序列号填充在 SCPS-SP 报文的抗重放域中随着数据报发送出去，而在接收端通过建立滑动窗口对接收到的数据进行取舍来实现抗重放服务。

由以上分析可知，认证加密算法作为重要的 SCPS-SP 关键技术，能够很好地解决空间数据安全传输问题，合理地搭配使用混合加密算法还能在一定程度上减少安全传输所需的时间。对 SCPS-SP 中的安全等级等内容进行改进，还可以在某种程度上提高通信服务质量。

4　挑战及建议

SCPS-SP 在实际的研究和应用推广中还存在诸多技术挑战，主要体现在以下几个方面。

(1)目前，卫星网络主要使用的传输协议为 CCSDS 的 SCPS 和空间 IP 及其改进协议。在安全传输方面，则以 IPSec 和 SCPS-SP 两种协议为基础。

然而，上述方案均为卫星网络协议栈中网络层的安全技术，传输层安全方面的研究涉及较少。安全的传输层协议不但需要考虑真实性、机密性、完整性等安全服务需求，还应降低协议的交互次数和传输的消息量，在安全和性能之间达到一定程度的平衡。

(2)SIN 涉及空间网络、临近空间网络和互联网、无线移动网络等多种异构网络，为端到端信息传输提供了多种可选途径，增大了传输容量，但由于不同网络在传输特性和性能等多方面存在巨大差异，使得端到端多网络一体化安全传输技术成为研究难点[24]。

(3)采用 CCSDS 标准是空间通信领域技术发展的必然方向[25]，而将不同的密码学算法应用到 CCSDS 空间通信系统的 SCPS-SP、实现对空间传输数据的保护，以及如何选择或设计更加适合空间信息网络数据通信的加密和认证安全协议已成为近年来的研究重点。因此，有必要继续为改进的协议引入高效的认证加密算法[20]。

(4)为了实现空间网络与地面网络的互联，网关协议在转换的同时还需要使用一些机制来提高网关的性能[26]。然而，这样不可避免地增加了系统的复杂性，降低了协议的效率，限制了 SCPS-SP 的更多应用。因此，调节好性能和效率之间的矛盾在以后的研究中也应值得注意。

(5)应进一步研究 SIN 系统被攻击之后的修复方法，深入研究这些修复方法并验证其可行性，最大程度地降低安全风险。

结束语　首先，本文介绍了空间信息网络特别是空间信息网络安全的概念和意义；其次，分别阐述了空间信息网络和其安全协议的国内外研究现状和进展；然后，介绍了空间通信安全协议 SCPS-SP 的关键技术，并重点针对其认证加密算法进行了深入分析；最后，分析了空间信息网络安全协议在研究和应用过程中面临的主要挑战，并给出了对应建议。

随着我国“十三五”规划中建设空间信息网络国家重大工程的逐步推进，未来此领域的研究将更多地集中在理论到实践的转化上。

参 考 文 献

[1] LIU X Y, MA J F, ZHONG Y T, et al. A new architecture of space information network security network[J]. Network Security, 2009(6): 13-15. (in Chinese)
刘小跃，马建峰，钟焰涛，等. 空间信息网安全组网新架构[J]. 网络安全技术与应用，2009(6)：13-15.

[2] PENG C Y. Research on key security technologies in space networks[D]. Changsha: National University of Defense Technology, 2010. (in Chinese)
彭长艳. 空间网络安全关键技术研究[D]. 长沙：国防科技大学，2010.

[3] SHEN R J. Some thoughts of Chinese integrated space-ground network system[J]. Engineering Science, 2006, 8(10): 19-30. (in Chinese)
沈荣骏. 我国天地一体化航天互联网构想[J]. 中国工程科学，2006，8(10)：19-30.

[4] CCSDS[OL]. [2016-03-18]. http://public.ccsds.org/default.aspx.

[5] CCSDS. Space Communications Protocol Specification (SCPS)-Security Protocol: CCSDS 713.5-B-1[S]. 1999.

[6] ECSS. ECSS-*Standards active and discontinued* [S/OL]. [2016-03-18]. http://www.ecss.nl/forums/ecss/templates/default.htm.

[7] NASA Space Network Security Standard [S/OL]. [2016-03-18]. http://standards.gsfc.nasa.gov.

[8] TAN Y J, REN J S. Summarize on security technology development in space networks[J]. Microprocessor, 2014(6): 1-3. (in Chinese)
谭延军，任劲松. 空间网络安全技术发展综述[J]. 微处理机，2014(6)：1-3.

[9] COPPERSMITH D. Data encryption standard (DES) and its strength against attacks[J]. IBM Journal of Research and Development, 1994, 38(3): 243-250.

[10] GAO X L, WANG J, ZHANG Q. A study on the security architecture of TT&C networks[J]. Journal of Spacecraft TT&C Technology, 2013, 32(4): 294-301. (in Chinese)
郜晓亮，王剑，张权. 测控网安全防护体系研究[J]. 飞行器测控学报，2013，32(4)：294-301.

[11] 国家自然科学基金委空间信息网络基础理论与关键技术重大研究计划[EB/OL]. [2016-03-28]. http://www.nsfc.gov.cn.

[12] BAI Y F, CHEN X M, AN J S, et al. Introduction to CCSDS AOS Protocols and its Applications[J]. Journal of Spacecraft TT&C Technology, 2011, 30(Z1): 16-21. (in Chinese)
白云飞，陈晓敏，安军社，等. CCSDS 高级在轨系统协议及其应用介绍[J]. 飞行器测控学报，2011，30(Z1)：16-21.

[13] KENNY G, ACHILLEOS N, CARR E, et al. A testbed for simulating and exploring secure communications between terrestrial and space environments[EB/OL]. [2016-03-28]. http://citeseer.ist.psu.edu.

[14] CCSDS. The Application of CCSDS Protocols to Secure Systems: CCSDS. 350.0-G-2[S]. 2006.

[15] ZHANG D H, LI H X. Analysis of the advantage of the encryption policy for the air to air communication based on SCPS-SP [J]. China New Technologies and Products, 2011(22): 4-5. (in Chinese)
张德慧，李海霞. 基于 SCPS-SP 的空间通信加密策略优势分析[J]. 中国新技术新产品，2011(22)：4-5.

[16] LIU Y,DONG Y,LI Z H. Discussion of data security about space-earth all-in-one networking and analysis of CCSDS SCPS [J]. Chinese Space Science and Technology,2004,24(1):31-36. (in Chinese)
刘泳,董勇,李泽慧. 空间通信协议分析与一体化网络安全问题探讨[J]. 中国空间科学技术,2004,24(1):31-36.

[17] LI J Y. The design and implementation of SCPS-SP/IPSec protocol conversion[D]. Harbin: Heilongjiang University,2013. (in Chinese)
李敬媛. SCPS-SP/IPSec 协议转换的方案设计与实现[D]. 哈尔滨:黑龙江大学,2013.

[18] DUAN X F,AN H Z,XIE S M. Space communication security protocols[J]. Communications Technology,2009,42(12):101-103. (in Chinese)
段小芳,安红章,谢上明. 空间通信安全协议研究[J]. 通信技术,2009,42(12):101-103.

[19] CCSDS. Encryption Algorithm Trade Survey: CCSDS. 350. 2-G-1 [S]. 2008.

[20] YANG Y H. Research on the authenticated encryption technology in CCSDS[D]. Shenyang: Shenyang Aerospace University, 2011. (in Chinese)
杨亚辉. CCSDS 认证加密技术研究[D]. 沈阳:沈阳航空航天大学,2011.

[21] MCGREW D,VIEGA J. The security and performance of the galois/counter mode (GCM) of operation[J]. Lecture Notes in Computer Science,2004,3348:343-355.

[22] LI H X. Research on data encryption/decryption strategy of CCSDS space communication system[D]. Shenyang: Shenyang Ligong University,2011. (in Chinese)
李海霞. CCSDS 空间通信系统中数据加密/解密策略研究[D]. 沈阳:沈阳理工大学,2011.

[23] LIAO Y,GUO X Q. A design method of multi-level security and anti-replay function of SCPS-SP[P]. 2015. (in Chinese)
廖勇,郭修琼. 一种 SCPS-SP 多安全等级及抗重放功能的设计方法[P]. 2015.

[24] LI H,FAN X X,MI J N,et al. Analysis of security technologies in integrated space-air-ground networks[J]. Journal of CAEIT, 2014,9(6):592-597. (in Chinese)
李华,范鑫鑫,秘建宁,等. 空天地一体化网络安全防护技术分析[J]. 中国电子科学研究院学报,2014,9(6):592-597.

[25] CCSDS. Next generation space internet (NGSI)-end-to-end security for space mission communications: CCSDS 733. 5-O-1[S]. 2003.

[26] LIANG L,LU S W. Design and implementation of gateway between CCSDS standard and TCP/IP protocols[J]. Computer Engineering,2006,32(4):134-136. (in Chinese)
梁莉,鲁士文. CCSDS 标准和 TCP/护协议间的网关设计与实现[J]. 计算机工程,2006,32(4):134-136.

(上接第 187 页)

[17] SARA S B,MATTHIEU D,PATEL S J,et al. An Adaptive Performance Modeling Tool for GPU Architectures[C]// Proceedings of the 2010 ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming. New York: Association for Computing Machinery,2010:105-114.

[18] HONG S,KIM H. An Analytical Model for a GPU Architecture with Memory-Level and Thread-Level Parallelism Awareness [C]// International Symposium on Computer Architecture. United States: Institute of Electrical and Electronics Engineers, 2009:152-163.

[19] KISHORE K,RISHABH M,REHMAN S M,et al. A Performance Prediction Model for the CUDA GPGPU Platform[C]// 16th International Conference on High Performance Computing. United States: IEEE Computer Society,2009:463-472.

[20] LIANG T. The Research on Optimizing Sparse Matrix Computation Based on GPU[D]. Wuhan: Huazhong University of Science and Technology,2012. (in Chinese)
梁添. 基于 GPU 的稀疏矩阵运算优化研究[D]. 武汉:华中科技大学,2012.

[21] BARRETT R,et al. Templates for the solution of Linear Systems: Building blocks for Iterative Methods[R]. Philadelphia: SIAM Press,1994.

[22] RUKHSANA S,ANILA U,CHUGTAI I R. Implementation and Evaluation of Parallel Sparse Matrix-Vector Products on Distributed Memory Parallel Computers[C]// IEEE International Conference on Cluster Computing. United States: Institute of Electrical and Electronics Engineers,2006.

[23] WANG Z W,CHENG L L,ZHAO W Q. Parallel Computer Performance Analysis Model Based on GPU[J]. Computer Science, 2014,41(1):31-38. (in Chinese)
王卓薇,程良伦,赵武清. 基于 GPU 的并行计算性能分析模型[J]. 计算机科学,2014,41(1):31-38.

[24] PING G,WANG L Q,CHEN P. A Performance Modeling and Optimization Analysis Tool for Sparse Matrix-Vector Multiplication on GPUs[J]. IEEE Transactions on Parallel And Distributed Systems,2014,25(5):1112-1123.

[25] DAVIS TIMOTHY A,HU Y F. The University of Florida Sparse Matrix Collection[J]. ACM Transactions on Mathematical Software,2011,38(1):1-28.

[26] SAMUEL W,LEONID O,RICHARD V,et al. Optimization of Sparse Matrix-Vector Multiplication on Emerging Multicore Platforms[J]. Parallel Computing,2009,35(3):178-194.

[27] VASILEIOS K,GOUMAS G,NECTARIOS K. Performance Models for Blocked Sparse Matrix-vector Multiplication Kernels[C]// 2009 International Conference on Parallel Processing. United States: IEEE,2009:356-364.

[28] FENG X W. Research on Key Technology of Similarity Calculation based on GPU[D]. Wuhan: Huazhong University of Science and Technology,2014. (in Chinese)
冯晓文. 基于 GPU 的相似度计算关键技术研究[D]. 武汉:华中科技大学,2014.

[29] CHEN R X. Parallelized XML Query Based on Functional Intermediate Language[J]. Journal of Chongqing Uiversity of Technology(Natural Science),2011,25(7):81-86. (in Chinese)
陈荣鑫. 基于函数式中间语言的 XML 查询并行化[J]. 重庆理工大学学报(自然科学),2011,25(7):81-86.