天地一体化信息网络发展与拟态技术应用构想

梁浩*, 陈福才, 季新生, 吕平, 高彦钊

国家数字交换系统工程技术研究中心, 郑州 450002

* 通信作者. E-mail: lhmailhappy@163.com

收稿日期: 2019-01-02; 修回日期: 2019-03-27; 接受日期: 2019-04-12; 网络出版日期: 2019-07-16

国家自然科学基金创新研究群体 (批准号: 61521003)、国家重点研发计划 (批准号: 2016YFB0800100, 2016YFB0800101)、国家自然科学基金 (批准号: 61602509)、河南省科技攻关计划 (批准号: 172102210615) 和信息工程大学新兴方向培育基金 (批准号: 2016610708) 资助项目

摘要 天地一体化信息网络是国家面向 2030 的重大科技工程, 现有的基础架构及由此构建的技术体系在其节点高性能处理、网络高效互联、一体化安全防护等方面面临诸多挑战. 本文从拟态技术应用的角度出发, 在分析天地一体化信息网络面临的技术挑战和现有技术思路的基础上, 提出将拟态计算、拟态防御和软件定义互连技术应用到天地网络架构、关键信息系统中的设计思路与应用构想, 相关技术思路和设计可为高速、高效、灵活、安全的天地一体化信息网络建设提供参考.

关键词 天地一体化信息网络, 拟态防御, 拟态计算, 软件定义互连

1 引言

天地一体化信息网络是维护和拓展国家核心安全利益, 实现全球互联互通的重大信息基础设施, 是以天基网络为主体, 地面网络为基础, 可支持陆、海、空、天各类用户随遇接入、按需服务的信息网络. 随着星上处理和运算能力的加强, 以及各国在太空探索方面活动的深入开展, 天地一体化网络受到了越来越多的关注.

我国对卫星网络开展了大量的研究和实践工作, 但目前现有的卫星通信系统仍未实现星间组网; 同时由于天基信息系统在轨信息处理能力较差, 其运行模式仍然是传统的数据中继, 数据的交换与路由均需要经过指定的地面站处理, 其实时性和传输效率很低, 无法满足高时敏、多任务协同等多样性信息服务要求; 此外, 与地面网络相对稳定的物理环境不同, 空间网络具有传输距离远、节点高动态、链路时空尺度变化大等特点, 且目前大多数卫星通信系统依赖加密和接入认证机制保障信息安全, 缺乏完善的安全保障体系, 以及信息安全防护能力, 现有互联网基础架构、组网模式和由此构建的安全防护技术体系已无法有效适应. 因此, 如何有效地将空、地网络安全高效地融合互联, 形成空天地一体化的信息网络面临着众多的难点和挑战.

引用格式: 梁浩, 陈福才, 季新生, 等. 天地一体化信息网络发展与拟态技术应用构想. 中国科学: 信息科学, 2019, 49: 799–818, doi: 10.1360/N112019-00002

Liang H, Chen F C, Ji X S, et al. Development status and applied research on mimic technologies for space-ground integration information network (in Chinese). Sci Sin Inform, 2019, 49: 799–818, doi: 10.1360/N112019-00002

近年来, 基于开放架构的软件定义网络^[1,2] (software-defined networking, SDN) 和网络功能虚拟化^[3,4] (network function virtualization, NFV) 等技术的蓬勃发展与不断成熟, 为智慧化、多元化、个性化、高鲁棒、高效能的新型网络技术^[5] 发展提供了开放环境和核心要素基础. 着眼网络空间安全面临的重大战略需求与现实发展需要, 受生物界“拟态现象”的启迪, 中国工程院邬江兴院士先后提出了“结构适应应用”的拟态计算技术^[6]、“结构适应安全”的拟态防御技术^[7], 以及以软件定义互连和软件定义节点为特征的新一代软件定义体系结构^[8] (为便于表述, 简称为“拟态技术”), 在普适性网络安全架构、高效能处理, 以及异构网络互联等方面从理论、技术和技术应用等方面均取得了突破性的进展. 拟态技术以融合先进性与可信性、安全性与开放性、高可靠与高效能为一体, 具备广义鲁棒控制能力的网络信息系统架构及方法机制为共同意愿, 按照“平台面向应用、组件面向功能、构件面向处理”的技术思想, 尝试通过变结构解决传统网络体系“能效”矛盾、硬件刚性互连束缚, 以及网络空间广义鲁棒控制问题, 实现高效能计算、内生式安全防御和异构灵活互联性能, 为构建高速、高效、灵活、安全的新型网络提供新的思路及技术方案.

本文从拟态技术应用的角度出发, 在综合天地一体化信息网络构建需求与面临技术挑战的基础上, 从天基节点处理、复杂异构网络互联, 以及一体化安全防护 3 方面对目前天地一体化信息网络技术发展的研究现状进行分析和总结, 并提出将拟态计算、拟态防御和软件定义互连技术应用到天地一体化信息网络架构、关键信息系统中的设计思路与应用构想, 相关技术思路和设计可为高速、高效、灵活、安全的天地一体化网络建设提供借鉴.

2 相关需求及技术挑战

天地一体化信息网络跨陆、海、空、天的多层级建设, 架构宏大、技术内涵丰富. 尤其是天基网络, 无论是部署模式、技术升级机制、运行维护体制、安全防护手段等都与地面网络有着本质的不同, 因此, 构建提供“全球覆盖、随遇接入、按需服务、安全可信”的网络与信息服务的一体化信息网络面临诸多方面的挑战.

挑战之一: 多样化、高效能的计算需求与当前天基节点处理能力有限、功能固化难以灵活拓展之间的矛盾.

受卫星载荷、能源供给、太空恶劣环境和设备维护、技术升级困难等影响, 天基节点计算能力、存储能力有限, 而这些限制使得在卫星网络上寻找路径时往往会造成死锁、冲突、消息拥塞等, 甚至导致卫星通信瘫痪. 面向全球提供多样化应用服务, 要求天地一体化信息网络能够根据应用场景和服务需求提供针对性的支撑, 随之而来的海量应用数据对卫星节点的数据计算、存储等处理能力提出新的需求. 表现在: 一是高效能处理能力. 全球化、多样化的应用服务必然产生或利用海量的应用数据, 需要强大的计算、存储、传送等处理能力支撑, 这些能力必须以尽可能低的载荷和功耗来实现. 二是高可靠、高鲁棒服务能力. 除适应太空恶劣环境这一基本要求外, 天基设备难以维修、难以实施软硬件更替, 即使部分设备发生异常、故障或损毁, 仍须保证正常提供信息处理服务能力. 三是可拓展、可重构的处理体系. 着眼“按需服务”的总体目标, 天基节点需要支持灵活适配多样化应用场景和不同功能域、不同安全域的计算特点, 提供可拓展、可重构、可定义的信息处理能力.

挑战之二: 高效能、无阻塞的复杂异构网络柔性互联需求与当前硬件固化的刚性互联体系结构之间的矛盾.

天地一体化网络由涵盖陆、海、空、天在内的多种异构网络互联融合而成, 节点类型、终端类型、接口类型、协议类型复杂多样, 且天基卫星节点始终处于高速运转状态; 同时现有互联体系结构大多

采用基于特定协议的网络互联模式,其内部工作模、交换拓扑结构,以及端口带宽分配方式均是固定的,硬件固化的刚性互联体系结构给一体化的网络融合提出了新的需求.主要表现在:一是无阻塞的稳定连通能力.全球提供多样化应用服务,要求天地一体化信息网络能够实现网络互联全域覆盖和稳定连通,随之而来的通信服务泛在保持对业务接通效率和稳定连通成功率带来挑战.二是异构网络融合互联能力.天地一体化网络涉及网络类型异构多样,特别是天基网络与地面网络运行环境存在较大差异,网络连接呈现连通间断性、时延方差大等特点,网络互联需要融合不同速率信道带宽、不同量级传输时延、链路连通间歇性,以及链路动态切换带来的影响.三是柔性适配能力.现有刚性互联体系结构造成系统组网的不灵活和扩容的不方便,需要柔性适配能力以实现系统灵活扩容、新协议的开放支持,以及系统运行的在线优化和扩展.

挑战之三:一体化高安全等级防护需求与当前依赖于攻击先验知识的外挂式、层次化防御技术之间的矛盾.

作为融合陆、海、空、天多种异构网络,面向全域立体开放的信息通信基础设施,天地一体化信息网络容易受到源自所有网络,从链路层、数据层、网络层、控制层到应用层,从设备攻击、信号攻击、协议攻击、路由攻击、信息攻击到服务攻击的多层次全方位安全威胁.此外,由于自身的开放性、广域覆盖等特点,天地一体化信息网络还面临其特有的安全威胁及挑战,主要表现在:一是无边界网络,无法沿袭传统地面网络或移动网络在边界设防的常用措施,对所有网络节点实施网元级布防又面临成本高昂、难以管控等问题.二是天基节点设备难以维护、技术难以升级的特殊性,决定了基于先验知识的,“先亡羊、后补牢”式的传统防御方法难以适用,任何未知漏洞/后门引发的新威胁,以及新型攻击手段,都可能引发全网陷入“无险可守”的窘境.三是外挂式、层次化的传统防御机制不仅会降低网络服务性能,而且将进一步加剧天基节点的载荷、功耗问题.四是天基网络节点带宽及处理资源受限,拒绝服务等常规的网络攻击手段门槛低且容易奏效.五是军民共用、高保密通信与普惠服务共用,需提供不同等级安全保障机制和个性化的安全服务能力,安全等级与安全隔离设计复杂性高.

3 国内外研究现状分析

结合第2节天地一体化信息网络发展所面临的需求与挑战,本节从天基节点处理、复杂异构网络互联,以及一体化安全防护3方面对目前天地一体化信息网络的研究现状进行分析和总结.

3.1 天基节点信息处理

随着成像分辨率快速提升,遥感卫星载荷数据率、存储容量、对地传输数据率、中继传输数据率也快速增长.面对天基网络多样化应用场景和不同功能域灵活高效适配需求与节点计算能力/存储能力有限、扩展升级困难之间的矛盾,目前相关研究可以分为以下两个方面.

3.1.1 简化设计与性能优化

通过对现有协议、算法、密钥管理等不同层面的改良和优化,来降低对链路、带宽、存储、计算等节点资源和处理能力的需求和依赖,提高节点组网、通信、传输等处理效率.文献[9]提出一种采用双向认证方式的接入认证方案,在防护篡改、重放等攻击的同时,降低了身份认证的计算负载. Bayrakdar等^[10]采用时隙ALOHA技术随机接入空闲信道,提出一种基于认知无线电的时隙ALOHA方案,大幅提高了信道利用率.文献[11]提出一种基于认知无线电的信道接入策略,大幅提高低负载情况下卫

星网络吞吐率, 从而解决卫星网络信道固定分配导致利用率低下的问题. 文献 [12] 通过集中式认证来兼顾移动卫星通信系统用户接入安全和计算开销. 文献 [13] 通过设置切换次数和切换时间的阈值, 在保证网络切换可靠性和安全性的同时, 降低切换带来的计算开销. 文献 [14] 提出了一种新型安全切换认证协议, 仅需 MN (mobile node) 和 AP (access point) 间的握手操作; 同时采用批量签名验证方案, 实现单个 AP 对多个签名的同时验证, 有效降低了切换的计算和通信开销, 提高认证的安全性. 文献 [15] 通过对接收到的信号强度、终端的停留时间、所处位置与运行速度进行加权来动态调整切换频率, 有效降低系统负担、网络切换次数及切换时延. Rahman 等 [16] 利用不同无线信道最大化频谱效率的变化调整资源分配策略, 提出一种适用于 LEO 卫星网络的自适应切换方案. Wu 等 [17] 利用 GPS 和卫星的多样属性, 提出一种面向 LEO 卫星网络的实施切换算法, 有效减少卫星间切换次数. Sun 等 [18] 提出一种端对端 TFRC 协议, 在保证提高数据传输可靠性的同时, 显著提高瓶颈链路利用率. Hou 等 [19] 通过数据挖掘来预测路由节点间的动态变化, 有效降低总链路开销. 文献 [20] 提出的卫星多播安全传输协议, 采用分批密钥的生成方式, 有效地将密钥更新带来的影响局部化, 从而大幅降低了带宽消耗和计算、存储开销, 减轻了卫星节点的工作负载. 文献 [21] 通过对用户的访问能力进行分组, 并采用二叉树的方式合并管理数据密钥根节点中相同部分, 从而大幅减少了卫星节点的密钥存储和通信开销. 文献 [22] 提出一种适用于战术卫星的高性能组密钥管理算法, 该算法通过证书验证证书共享机制设计有效降低时间开销和节点计算开销. 文献 [23] 通过将空间网络中的元素按传输速率、可移动性、资源限制等条件进行分类, 基于各自网络的特性优化提出一种自适应的高效密钥管理方案, 实现各类网络密钥资源的按需分配.

3.1.2 平台构建与资源调度

另一种思路是通过平台构建与资源的调度, 对天基节点、网络进行专用化系统的升级改造. 文献 [24] 在分析了当前天基信息系统发展现状和特点的基础上, 提出了一种具备高性能在轨信息处理能力的天基信息节点——天基信息港概念, 及其基于高轨共位的模块化卫星组成的空间分布式系统的实现方案; 本质上, 天基信息港可视为一种“大”节点, 由一簇在同步轨道上共位的模块化卫星组成, 通过“池化”技术, 将各个卫星内部的计算、处理和存储资源统一起来, 形成空间上是分散的、逻辑上是统一的并行异构计算处理平台, 来增强天基节点各类数据/信息汇聚、处理、交换和分发等能力. 文献 [25] 针对天基系统星上处理能力不足、技术落后、无法实现多源数据在轨实时处理等难题, 提出一个应用于中低轨微小卫星的天基网络化通用服务平台的设计概念, 为现在的卫星技术发展提供新的硬件架构, 同时异构的体系结构既可以实现星上的独立运行, 又可以为星载计算机的数据处理提供硬件加速. 文献 [26] 针对如何实现资源的高效管理, 对天基资源网络的管理对象进行细粒度、多维度分析, 进一步提出动态天基资源虚拟化、调度方法与协同管理的设计, 来增强天基网络节点随时随遇接入、异构网络体系、不同类型资源协同管理等管理能力. 文献 [27] 针对天地联网中空间与地面网络节点的信息高效互通、交换及应用需求, 提出利用电子信息综合化技术实现高度综合化的多功能通用平台, 并结合 SDN 架构、网络协议与路由网关, 来解决网络中由于物理界限造成的信息阻隔, 实现物理资源与边界虚拟化、信息流程智能化的天地一体化天基信息系统, 提高天基信息资源利用率、信息按需定制及高效共享能力. 文献 [28] 通过开展分布式计算在可重构综合卫星平台中的应用研究, 提出一种可重构综合卫星平台的设计理念, 并围绕支持网络互联的可重构综合卫星平台的关键技术, 从安全控制协议、可扩展设计、分布计算与管理模型等方面进行详细设计, 提升在轨运行的稳定性、抗毁性, 以及可维护性, 实现平台功能的拓展和高效利用.

3.1.3 小结

从本质上看,“通用性(满足不同计算特点)+高性能+低功耗”是当前计算机体系结构设计面临的瓶颈性问题;冯·诺依曼(von Neumann)结构下的通用计算模式,面对大多数高密度计算、高通量传送的应用场景处理效能较低;专用计算机/处理设备又面临功能固化、难以适应需求变化进行灵活拓展的问题.在这种背景下,现有通过轻量化(构件、算法等)设计和改良优化的方案,与服务功能完备性、服务鲁棒性、服务安全性的需求存在互斥性,难以真正满足多样化应用的数据处理需求和实现服务质量与安全性能的兼顾.

3.2 复杂异构网络互联

天地一体化信息网络由天基骨干网、天基接入网、地基节点网、地面互联网、移动通信网等多种异构网络互联融合,尤其是天基卫星网络、星地互联协议作为网络互联、高效运行的关键,需要与具体网络环境、应用服务相适应.卫星通信网络与地面网络运行环境存在较大差异,天地一体化网络协议体系在设计时需要充分考虑到天基网络与地面网络的差异性.

3.2.1 面向网络互联的协议体系

天基卫星网络经过近半世纪的发展,逐渐产生了多种网络协议体系结构,典型的包括TCP/IP协议体系¹⁾、CCSDS(consultative committee for space data systems)协议体系^[29]、DTN(delay-tolerant networking)协议体系和SDN协议体系等.卫星网络拓扑的动态性导致地面的TCP/IP协议体系不能直接应用于卫星网络,目前相关研究主要集中在针对卫星网络特点的TCP/IP协议改进和扩展^[30~36]上,一定程度缓解了延迟大、网络拓扑快速变化、链路时断时续、信道误码率高的复杂异构网络环境带来的网络拥塞、链路过载、数据包丢失、吞吐率下降等互联问题,但其只考虑了端到端的情况,并未考虑整个网络的行为特性,缺乏针对整体网络的优化.CCSDS协议体系是针对空间通信特点制定的空间通信协议标准,其基于TCP/IP协议体系的思想,主要是针对空间数据传输系统存在的传输距离远、节点动态性高、链路时延变化大、链路不对称、间歇性的链路连接等特点进行优化和扩展,目前已被较多的航天机构采纳和应用,并且已经过了多次航天任务考验.因此,面向天地一体化网络的互联应用,CCSDS协议体系具有方案可行性,但其无法与地面网直接互操作,需要进行协议转换,存在协议兼容的问题;同时动态路由支持能力弱,开发、测试、维护费用相对TCP/IP较高,一体化的网络互联面临路由、传输等方面的优化与设计,以及协议转换、安全防护方面的研究^[37].DTN协议体系采用持久存储、寻机转发的思想,是专门针对宇宙空间中星际通信的特点而提出的,用于解决大时空尺度和恶劣环境下多系统组网通信问题,以Bundle协议为核心构建的,且兼容CCSDS及TCP/IP协议体系,采取了新的分组丢失重传控制机制,大幅降低了数据传输所需重传频率,使DTN协议体系下的传输协议更适合于延迟很高、链路通断频繁、链路质量变化较快的深空通信网络;引入了Bundle层作为处理不同类型网络协议的覆盖层,一定程度上解决了不同协议间的兼容问题,但是该协议体系还未形成完善的路由选择、密钥管理保证机制,且协议开销较大.SDN协议体系是一种新型网络技术,能够在异构多域网络环境下对全网设备和多租户多应用服务进行全局优化的统一管理和动态配置,实现灵活高效的资源分配和协同;将SDN/NFV技术应用到天地一体化网络中,可以极大地提升天地一体化网络的管理能力、协同水平和服务质量,增强控制层的智能边缘转发能力、骨干网络的高效承载能力,以及网络能力的开放和协同;目前该方面的研究主要集中在接入认证架构^[38]、多功能载荷平台等

1) Space communications protocol standards (SCPS). [2017-08-08]. <http://www.scps.org>.

方面,但其多域的组网,以及大量转发设备的控制算法非常复杂,相关研究大多处于理论阶段,且没有形成统一标准,实际部署实现难度大。

上述典型的网络协议体系均属于层次化协议体系的范畴,各层之间相互独立,具有结构灵活性好、易于维护和设计等优势;然而各层的单独设计使得协议体系各层间存在功能冗余,缺乏整体性能的规划与优化,以及安全性的考虑。为更好地实现天地异构网络的互联互通,文献 [39] 根据航天器与地面站数据传输的特点,提出了一种航天器 IP 网络协议体系结构,设计了适合于天地间通信的网关协议和速率控制策略,实现了航天器与地面站网络的一体化通信,并已在货运飞船上成功应用。文献 [40] 提出 2 级网络架构的构建思路,采用标准的分层体系,融合常见的网络互联协议栈和天基骨干网专用协议(如 BTP, BNP, BRP, 以及宽带接入协议、安全认证协议等),并能够根据传输需求进行优化,降低了天基网络路由传输和接入的复杂度,提升信息传输效率。文献 [41] 提出了一种基于天地一体化网络体系架构的临近空间接入网,并基于分层自治域网络模型从实际应用出发,对网络层、数据链路层和物理层进行了一体化设计协议设计,保证了不同业务的 QoS 需求。文献 [42] 借鉴国内外空间信息网络协议体系的最新研究成果,结合我国天基网络特点,提出了适用于我国天地一体化网络的增强空间融合协议体系,该协议体系基于地面网的 TCP/IP 分层协议模型并兼容 CCSDS 协议体系、DTN 协议体系和卫星移动协议体系,并结合天基网络特点对每一层进行协议空间增强设计,实现天基网络与地面互联网和移动通信网络的互联互通、信息服务共享。

3.2.2 面向网络互联的路由交换

路由是网络互联的核心,路由协议直接决定着网络互联与数据传输性能。天地一体化信息网络由涵盖陆、海、空、天在内的多种异构网络互联融合而成,网络拓扑高度动态变化,以及空间环境对硬件技术的限制导致路由设计更加困难,对传统的路由的性能提出了新的需求。目前,面向网络互联的路由方案依据组成网络的卫星是否在同一轨道高度上可以分为单层卫星网络路由和多层卫星网络路由方案,从网络互联的角度,相关技术又可以分为面向连接和无连接的路由技术,而面向天地一体化网络互联的路由研究主要集中在针对空天通信环境的传统路由协议改进上,主要采用基于时间感知的预测、逻辑位置、信任机制等设计策略,目的在于实现异构互联网络中数据传输、转发处理等过程的路径最优,文献 [43~46] 在这方面做了较全面的研究和综述。

其中,面向连接的路由方案最早在单层卫星网络中被提出,主要是根据卫星运动的周期性来离散连接的时隙,将动态的卫星网络转化为多个静态拓扑下的路由连接;本质上是利用时间的周期性把卫星的移动特性隐藏起来,从而简化星座设计复杂度和路由的难度,卫星不需要实时计算,仅在时间分割点更新路由表,因此仅需要简单的查表操作,但是由于系统周期可能需要大量的路由表存储空间,同时由于星地通信并不是实时的,不能保证单位时间内拓扑的一致性,所以对通信流量变化、链路拥塞,以及故障等实时情况适应性较差。无连接的路由方案则主要基于虚拟节点策略,将真实的卫星网络进行虚拟化的逻辑抽象,本质上是利用卫星运动的空间周期性来隐藏卫星的移动性,与面向连接的方案相比,不需要预先大量的路由计算与信息上传,同时卫星节点也无需路由表维护,因此存储需求低,可根据流量负载、故障等情况实时选择路径,自适应性强;问题是该类路由通常要求拓扑结构规则、卫星数目较多的卫星系统;路由计算利用局部状态信息,分别对数据包进行局部最优转发,无法保障全局最优,并且对星上处理能力要求增强。

基于多层卫星网络路由方案,具有更大的空间自由度,相应的设计也更加灵活,近些年比单层卫星网络路由的研究更受关注;与单层卫星网络相比,具有满足多业务 QoS 需求、低链路拥塞、更高鲁棒性等优势。然而层次化的、基于快照的多层卫星网络路由算法一方面没有充分发挥 MEO 和 GEO 的

传输能力(只完成控制和管理, LEO 进行数据传输);基于快照的方式引入面向连接的路由方式,其拓扑更新大大增加了信令开销,无法保障高时延链路条件下及时更新每颗卫星的拓扑信息,同时也没有考虑上层卫星失效可能导致的大片下层卫星无法工作等问题.另一方面目前相关研究也大多存在于理想拓扑环境下的仿真设计,未考虑卫星运行时的实际情况,如天线对准时延、链路带宽占用率和误码率等情况,实际可参考性低.

DTN 是对一类具有大延时、链路间歇性中断的网络的抽象,天地一体化网络作为 DTN 的一个典型代表,DTN 的相关研究可以为其路由协议的设计提供参考.传统的 DTN 大多都是泛洪路由来存储转发的,造成网络通信双方可能找不到可持续通信的路由拓扑链路,基于泛洪的路由方式由于中间节点的缓存占用得不到及时的释放,容易产生拥塞,导致数据传输效率低下;同时由于没有利用网络先验知识,转发数据分组时,具有极大的盲目性,网络中传输并缓存着大量重复分组,极易造成网络拥塞及带宽和存储资源不足.因此,对运动节点的位置预测在 DTN 网络中具有很高的实用价值,如果能够提前掌握路由节点将会出现的位置信息,采用准确的数据包投递方式,就可以有效地降低缓存占用、设计出高效的路由机制;此外,也有文献研究从限制重复传送的副本数量^[47]、最佳能量感知的传染路由策略^[48]等方面进行优化,以减少网络资源的消耗及浪费.

3.2.3 小结

从现有的技术思路来看,多层级异构网络、异构协议互连,必须统筹考虑不同速率信道带宽、不同量级传输时延、链路连通间歇性,以及链路动态切换带来的影响并进行综合优化,才能保证业务接通效率和稳定连通成功率.同时,天地一体化网络全域覆盖、随遇接入和动态变化的特性,对异构网络交换节点的接口适配、协议适配等资源要求很高,这些资源的配置容量又跟系统载荷、功耗紧密相关,只有打破端口“硬件化”定义属性,对任意交换连接端口实现接口类型、接口带宽、协议方式的自定义,网络协议体系具备动态可重构特性,才能形成高效能、无阻塞的异构网络柔性互联能力.

3.3 一体化网络安全防护

安全防护保障作为天地一体化信息网络可靠运维的重要支撑,涉及系统工程的方方面面,需要体系化的安全防护设计.传统的互联网组网模式和安全防护技术已无法有效适应空间网络,为了能够应对来自不同方面和层次的网络安全威胁,如何安全有效地融合空间网络、临近空间网络和地面互联网,形成空天地一体化的信息网络,面临着众多的难点和挑战.

3.3.1 协议栈安全

目前我国现有的卫星通信系统尚未实现星间组网,且大多数卫星通信系统依赖加密和接入认证机制保障信息安全,缺乏完善的安全保障体系,以及信息安全防护能力,卫星安全的相关研究主要集中在通信安全方面,涉及物理层、链路层,以及针对某些具体应用的安全技术,对于网络化,以及与地面网络融合方面的安全问题的研究不多;随着天地网络不断融合,针对空天网络的安全研究范围逐步拓展到了协议栈上层,在这方面英国 Surrey 大学的研究成果较为突出^[49~51].同时,鉴于 IPSec 是地面互联网中最有效且应用最为广泛的网络层安全协议,目前相关研究以 IPSec, SCPS-SP 等协议为基础进行扩展和改进,以解决 TCP 性能增强技术与 IPSec 的兼容性问题,实现卫星网络与地面互联网的融合互联,主要的思路有:采用传输层安全协议(SSL, TLS)替代 IPSec 的方案将暴露 TCP 报头,带来新的安全风险,同时 SSL 和 TLS 自身应用范围有限,无法有效支持 UDP 协议等其他传输层协议;

IPSec 嵌套 SSL/TLS 的思路, 会使得 TCP 载荷被 IPSec 和 SSL/TLS 两种安全协议分别处理, 造成主机与网关处理资源的浪费; 传输层友好的 ESP (TF-ESP) 协议方案则缺乏适合的完整性验证保护, 未加密的 TCP 状态信息容易被恶意中间节点所利用, 产生了易受攻击的脆弱性。除此之外, 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, 还应该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上的平衡。

结合天地一体化信息网络运行安全的实际需求, 目前相关防护技术研究主要集中在安全接入、安全路由、安全切换、安全传输等方面。文献 [52] 结合在安全路由、安全切换、安全传输等网络信息传输的不同阶段面临的严峻挑战, 提出了一体化网络安全防护未来发展亟待解决的关键技术。文献 [53] 基于通用开放、可重构的理念提出了一种天地一体化网络安全验证系统方案, 期望实现密钥管理、安全路由、安全切换、安全隔离、安全传输等安全保障技术的系统验证。此外, 网络安全切换的相关研究主要涉及网络、链路两个层面; 其中, 链路层切换主要基于卫星系统的通用虚拟拓扑和固定轨迹进行切换判断, 对有限的卫星网络资源实现有效分配。网络层切换主要采用基于用户位置信息或切换概率、基于频谱效率、基于上下文等设计策略, 目的在于降低由节点位置不固定、网络高度动态变化所带来的系统负担、切换次数及切换时延, 以保证网络拓扑的动态链接和节点间不间断通信。在安全接入方面, 主要采用数字签名、签密解密、拥塞控制等手段, 实现不同终端和用户之间的接入认证与访问控制。文献 [54] 基于信息安全模型, 重点从物理安全、运行安全、数据安全 3 个层面, 对抗毁技术、抗干扰技术、人工噪声、多波束通信等物理防护, 安全路由、安全接入、安全切换等网络运行保障, 以及安全传输、密钥管理等数据防护技术现状进行了全面系统的分析与阐述, 本文不再赘述。表 1 总结了天地一体化信息网络各个层面面临的安全威胁、相应的防护机制与技术以及存在的问题。这些问题存在的主要原因并不完全是技术自身的问题, 更多的是受其应用所在协议层的功能制约, 因此, 为了能够应对来自不同方面和层次的网络安全威胁, 必须打破层次化协议体系的限制, 将安全防护思想融合到空天地一体化网络的体系结构中。文献 [55] 基于可信网络连接架构提出一种可证明安全的可信网络连接协议模型 (TNC-PS)。文献 [56] 在分析天地一体化信息网络面临的安全威胁和现有防护技术手段的基础上, 探讨了内生式安全防御技术在天地网络架构、关键信息系统中的应用设想。这些都为突破传统层次化、外挂式防御技术缺陷, 构建内生式安全防护体系提供了思路 and 方向。

3.3.2 动态接入控制

访问控制的主要功能是允许合法用户访问和使用系统受保护的资源和服务, 并防止非法用户的访问和合法用户的非法访问。天地一体化网络环境具有设备动态接入、网络异构、众多和信息跨网流动频繁等特点, 网络动态接入的访问控制问题引起了重点关注。

考虑接入设备的动态性, 文献 [57~59] 基于访问控制列表提出基于 Capability 的访问控制模型, 实现对访问设备的细粒度管理。文献 [60] 基于可信的概念提出了终端到终端的安全交流和访问机制。针对天地一体化网络的接入动态性特点, 文献 [61] 结合基于角色、上下文的访问控制模型, 融合角色安全性和可用性、属性灵活性等优势提出一种分布式的访问控制框架, 通过将动态的偏好知识应用于用户授权与访问过程, 实现对用户的连续访问控制。文献 [62] 基于角色、上下文和动态的偏好知识, 结合 RBAC (role-based access control) 模型和 ABAC (attribute-based access control) 模型提出一种用户可连续访问的控制模型, 减少了角色和访问控制规则的数量, 降低了管理的复杂性。然而, 上述基于传统访问控制模型提出的方案很难解决天地一体化网络环境下信息流频繁的跨网问题。文献 [63] 提出了面向网络空间的访问控制机制 (cyberspace-oriented access control model, CoAC), 使用设备、接入点、时间、网络, 以及相关属性因素描述策略, 实现了网络空间对细粒度控制、策略跟随和策略语义一致性

表 1 面临的安全威胁、防护机制以及存在的问题总结

Table 1 Summary of security threats, protection mechanisms and existing problems

	Security threats	Protection mechanisms	Goal	Existing problems
Physical layer	Physical damage, deception interference and suppression interference caused by attacks such as congestion, tampering and eavesdropping	Anti-destructive technology, anti-deception jamming, anti-suppression jamming, artificial noise, multi-beam communication, etc.	Improve the survivability of network	Difficult to resist attacks within the system, and have complex synchronization and poor scalability
Link layer	Data leakage caused by attacks such as collision, denial of service, etc.	Security mechanisms such as error detection, transmission rate restriction, etc.	Improve the robustness of link communication	Without providing end-to-end network security
Network layer	Network attack such as sybil, replay, wormhole and so on; malicious behavior such as communication analysis, routing information manipulation, etc.	Security protocols such as IPSec, SatIPSec, SCPS-SP and security mechanisms such as digital signature, signcryption and decryption, congestion control, etc.	Improve the security of network access, connection and switching	Only suitable for IP-based networks and incompatible with satellite TCP performance enhancement technology
Transport layer	Data tampering and leaking threats caused by SYN attacks, man-in-middle attacks, forgery attacks, etc.	TLS, SSL, SCOKS and mechanisms to limit the number of links, customer problems, etc.	Improve the ability of network security transmission	Lack of support for UDP and multicast security methods
Application layer	Cloning attack, malicious code execution, privilege escalation and malicious use of privacy information, etc.	Security protocols such as SFTP, HTTPS, S/MIME, PGP, SSH and key management mechanisms	Provide the service security for different application requirements	Support user specific applications only

等访问控制需求. 文献 [64] 将 CoAC 进一步映射到天地一体化网络上, 提出了面向复杂网络环境的访问控制机制, 实现了对天地一体化网络环境信息流的跨网控制.

此外, 从服务保障的角度, 云计算已经成为未来天地一体化信息网络提供应用服务的主要承载形式, 目前云端访问控制的研究以多要素化为需求, 以时间、位置信任关系等不同的侧重点阐述了相关模型和机制, 文献 [65] 基于时态特性的 RBAC (temporal role-based access control, TRBAC) 模型及其扩展模型等, 将为天地一体化云环境下访问控制模型的构建提供参考. 文献 [66] 进一步细化了角色要素的描述, 提出 CARBAC 模型, 但要求数据所有者具有很强的计算能力, 与天地网络有限的资源相悖. 文献 [67] 将用户、环境、系统状态之间的信任关系作为重要的访问控制要素提出 SAT-RBAC 模型, 通过云环境的特征来划分信任关系. 文献 [68] 基于位置信息要素, 通过对云端存储位置的约束实现对数据的安全保护. 针对云环境下数据的安全性问题, 通常以数据所有者在使用云服务前会将数据进行加密处理, 因此, 针对密文数据的云端访问控制出现了基于角色加密^[69]、IBE、ABE 等机制^[70], 该类访问控制方案完全依赖用户自身进行数据密文的产生、密钥的产生、数据的解密等运算, 但为用户带来较高的资源和时间成本的同时, 也带来了大量密钥的管理问题. 随着代理重加密 (proxy re-encryption, PRE) 技术云端访问控制的不断应用, 在满足数据安全性需求的同时, 大大缓解了用户

在数据创建与访问时的运算量, 出现了基于身份与属性的代理重加密机制^[71, 72]、基于证书的代理重加密^[73]等; 代理重加密与云端访问控制的结合逐步面向多样化的访问控制条件, 出现了基于条件的代理重加密 (condition based PRE, CPRE)^[74]机制, 属性的多样化不仅增加了 ABE 加解密条件描述的难度, 更带来了访问者的密钥管理量和难度. 为了进一步减轻数据所有者的计算难度, 充分利用云服务端的计算能力, 文献 [75, 76] 提出一种多要素代理重加密机制; 文献 [77] 进一步结合代理重加密技术, 提出一种云端多要素访问控制方案 (PRE-MFAC), 实现在天地一体化复杂云环境下密文数据的多要素访问控制管理问题.

3.3.3 小结

从现有的安全防护技术来看, 目前大多仍局限于依赖于攻击先验知识 (如杀毒软件、防火墙等) 的被动式防御思路, 无法有效抵御基于系统软硬件未知漏洞和后门等的未知威胁 (如 0-day 攻击、APT 等); 同时静态、固化的部署模式无法主动适应一体化用户、网络和业务的快速变化, 难以满足不断扩展升级的安全需求、实现网络技术与安全的共生演进. 因此, 发展不依赖于先验知识、非基于边界的内生安全的主动防御技术成为天地一体化网络的安全防护新的技术方向与思路.

4 解决思路与应用构想

针对现有技术思路存在的不足, 本节提出将拟态计算、拟态防御和软件定义互连技术应用到天地一体化信息网络中的设计思路; 即在天基节点信息处理层面, 构建基于认知重构的天基节点计算体系, 形成面向不同应用场景, 满足不同计算需求, 支持在线重构和“函数化”调用的计算架构, 研发相应的芯片或算核, 实现通用化、高性能、低功耗的星载设备计算性能; 在复杂异构网络互联层面, 面向最基础的数据交换需求, 实现异构网络、异构协议转换适配资源的软件可定义, 简化网络互联部署及应用的复杂度, 提高互连接口及协议配置的灵活度, 支撑多网系融合的物理连接; 在一体化安全防护层面, 建立广义鲁棒控制的网络信息系统架构, 形成具备内生安全的天地网络安全防护体系, 实现对未知风险的内生式“主动免疫”.

4.1 基于认知重构的天基节点计算体系结构

拟态计算 (mimic calculation, MC) 的概念源于国家“863”计划重点项目“新概念高效能计算机体系结构研究与原理样机研制”提出的基于多维重构函数化结构与动态多变体运行机制的拟态计算体系. 本质上是通过动态的选择与使用多种功能等价、计算效能不同的软硬件变体或基础模块的多维动态重构函数化体系结构, 以达到计算效能最优化的目的. 其核心是基于认知的主动重构计算体系结构 (如图 1 所示), 物质基础是由不同软硬件计算单元 (构件) 组成的异构计算资源池, 比如宏观来讲可能由适合不同计算类型的 CPU, GPU, DSP, FPGA 构成计算资源池, 微观来讲可能是芯片上的各类算核. 拟态计算的核心机制就是在计算任务执行过程中, 通过基于主动认知的重构策略, 调度不同的计算资源构建最适于当前计算需求的处理结构, 达到“应用决定结构, 结构决定效能”的目的. 对应到天地一体化信息网络, 天基节点信息处理对计算的需求是既要满足不同计算特点需求, 又要满足处理的高效能, 拟态计算通过动态变结构, 可以契合这一需求.

如图 2 所示, 在实现机理上, 首先对于天基节点涉及的计算任务 (算法), 比如数据压缩、数据加解密、目标识别、图像解译等进行统一规划, 通过芯片或构件模式设计支持不同计算结构的异构资源池,

图 1 (网络版彩图) 拟态计算动态变结构示意图

Figure 1 (Color online) Dynamic variable structure diagram of mimic computing

图 2 基于认知重构的天基节点计算体系实现机理

Figure 2 Implementation mechanism of space-based node computing architecture based on cognitive reconstruction

然后对这些计算任务按一定颗粒度进行分解, 提取能与不同计算资源最佳映射的算核, 再利用这些算核对计算任务进行高效能应用编译, 实现计算结构在计算过程中能够主动认知计算需求并在线重构, 形成最优解的函数化计算结构, 达到高性能、低功耗计算目的. 具体来讲, 基于拟态计算原理, 可以面向天基节点信息处理应用设计拟态计算芯片, 也可以提供面向天基应用的软件可调用 IP.

4.2 基于软件定义的复杂异构网络柔性互联

软件定义互连可以在硬件层面实现互连协议、端口类型、拓扑结构、带宽分配、互连模式等关键参数的软件定义 (如图 3 所示), 支持不同协议、不同带宽、不同互连模式的数据交互通信需求^[8]. 将软件定义技术由服务层、网络层进一步下沉至最基础的物理连接层, 通过软件来定义物理层互连部件的接口类型、带宽、协议间转换和拓扑结构等主要参数, 可以极大简化天地一体化网络中不同谱系系统设备互联融合的复杂度, 提高设备形态可重组、可重构和通过现场定义快速适配应用场景变化的体系化支撑能力, 从而解决传统协议体系结构中的刚性互连问题.

软件定义互连的实现结构通常包括软件定义协议控制器、软件定义转发引擎和软件定义交换结构 3 个部分: 软件定义协议控制器可软件配置为支持不同频点、不同绑定模式、不同协议的协议控制

图 3 (网络版彩图) 软件定义互连
Figure 3 (Color online) Software defined interconnection

器; 软件定义转发引擎可软件配置为不同协议的解析与封装、不同协议的转换、不同协议的转发查表; 软件定义交换结构可软件配置为不同规模、不同结构的交换网络^[8]. 因此, 按照“平台面向应用、组件面向功能、构件面向处理”的技术思想, 面向天地一体化信息网络可以开展支撑多网系异构融合的软件定义互连交换芯片/交换部件研究, 针对不同接口、协议及连接需求一体化提供现场可定义的交换互连机制, 为不同网系或系统内不同模块灵活对接建立与接口及协议无关的异构互连能力. 在具体实现上, 可以通过对多种协议的处理机制进行分析, 根据协议特性关键字信息, 提取出协议处理的共性引擎集和专用处理引擎集, 对于共性引擎集通过专用电路予以实现, 对于专用引擎集通过软件定义的可编程逻辑予以实现, 形成针对多种异构协议的统一硬件架构和软件定义处理机制. 同时, 为了实现软件定义互连芯片的高效性, 可以在分析各种协议共性的基础上, 提取高速 PHY、协议解析、协议转换、动态缓存、路由寻址和动态拓扑等粗颗粒度硬核; 为了实现对不同异构协议支持的灵活性, 在硬核的实现中引入现场可编程和可重构的硬件可定义技术; 最终, 软件定义互连芯片既能实现高效互连与数据交换, 也能支持对不同异构协议的灵活可定义, 并基于指令流和配置流的融合实现用户的可定制计算和处理需求.

4.3 具备内生安全的天地网络安全防护体系

拟态防御的目标是转变传统外挂式安全防御的技术思路, 建立一种基于广义鲁棒控制构造的内生性安全理论及方法. 其基本原理是根据“相对正确”公理的等价表达机制, 自动感知“未知”安全威胁情况, 利用创新的动态异构冗余架构及其策略调度和多维动态重构负反馈机制, 形成具有“非配合条件下多元动态目标协同一致攻击难度”和“测不准效应”的防御场景, 使得目标系统能够有效抑制包括基于漏洞后门等“暗功能”攻击在内的广义不确定扰动, 在不依赖于攻击者先验知识和攻击行为特征信息情况下, 显著地提升系统功能的稳定鲁棒性和服务的品质鲁棒性.

将拟态防御技术应用到天地一体化信息网络中, 构建具备内生安全的安全防护体系, 其基本思路是: 在保持现有安全设计架构不变的基础上, 将拟态防御的内生安全机制叠加到网络和系统的层面, 从而形成内生安全的天地一体化网络安全防护架构, 如图 4 所示.

图 4 (网络版彩图) 内生安全防护体系

Figure 4 (Color online) Endogenous defense security architecture

图 5 (网络版彩图) 拟态天基路由器

Figure 5 (Color online) Mimic space-based router

在具体实现上, 将多维动态重构技术应用到云网架构层面, 形成动态路由、动态 IP、动态拓扑结构、动态异构协议等安全机制; 将动态异构冗余基因及其控制机制应用到软硬构件层面, 形成各类拟态化的芯片、部件及支撑软件; 应用到网络节点层面, 形成拟态化的网络控制器、路由器、DNS 服务器、云服务平台及威胁感知器等, 支撑构建高可靠、高可信、高可用“三位一体”、具备广义鲁棒控制能力的网络体系。下面以拟态天基路由器和拟态信息港云平台为例进行示例。

4.3.1 拟态天基路由器

传统路由器从功能上可以划分为 3 个平面: 配置管理平面、路由控制平面和数据转发平面。结合天基环境特点, 拟态化天基路由器构建的基本思路是基于既有的天基路由器运行平台 (需支持虚拟化功能) 和天基路由协议栈 (控制面) 进行拟态化改造。

如图 5 所示, 路由器主要分为数据平面和控制平面, 路由转发的核心在于控制平面, 以既有的路由器控制平台为基础, 通过多样化工具链 (虚拟化工具、多样化编译工具等), 形成若干异构控制平面,

图 6 (网络版彩图) 拟态云平台
Figure 6 (Color online) Mimic cloud platform

进而针对拟态调度、拟态裁决等设计标准化的拟态插件, 异构控制平面与拟态插件两者融合即形成具备动态异构冗余特性和多维动态重构机制的拟态控制平面, 再结合既有的天基转发单元, 即可形成路由设备及路由服务的内生安全效应。

4.3.2 拟态信息港云平台

随着全球网络信息基础设施的加速云化重构, 云计算已经成为未来天地一体化信息网络提供应用服务的主要承载形式, 同时云平台也是实现拟态机制的最佳平台, 其基于虚拟化技术实现应用的天然特性, 很容易构建异构化的资源池, 也就是拟态化的基础. 拟态云虚拟可信平台的基本思想是以既有云平台各类异构资源池为基础, 在保持上层应用调用接口不变的条件下, 将拟态防御的动态、异构、冗余技术应用到云服务平台的计算、存储和网络层面中, 通过在云平台的管理模块增加拟态调度器、裁决器、反馈控制器等管理插件, 构建支撑拟态机制的云平台, 赋予所调用的虚拟机异构冗余和动态变换的特性.

具体实现如图 6 所示, 利用云平台天然的虚拟化环境, 构建各类异构化和多样化的物理/虚拟资源, 如网络、计算、存储资源等; 进一步基于漏洞分型的软件异构化技术构建多样化的软硬件构件, 利用广义鲁棒控制的构造技术实现对异构的虚拟机、容器和存储等资源的拟态化封装, 建立多种虚拟资源实体的拟态结构, 包括拟态云主机、拟态容器和拟态存储等, 从而为任务执行层提供具备广义鲁棒特性的处理平台. 其处理流程是通过感知层实现威胁的度量和各种负载的安全防护需求, 进而通过任务执行层的解析与编排, 根据不同的防护任务需求和场景, 对异构资源进行拟态化封装, 构建与安全等级相适应的虚拟化执行空间, 并主动地动态适配与重构, 从而提高云服务平台应对利用未知漏洞和后门带来的不确定性威胁的能力.

5 结束语

本文从拟态技术应用的角度出发,在综合天地一体化信息网络构建需求与面临技术挑战的基础上,探讨了拟态计算、内生式安全防御和软件定义互连在天地网络架构、关键信息系统安全防护中的应用设想,提出了基于认知重构的天基节点计算体系结构设计、基于软件定义的复杂异构网络柔性互联和具备内生安全的天地一体化网络安全防护体系架构设计思路,并重点以拟态天基路由器和拟态信息港云平台为典型系统进行应用示例,相关技术思路和设计可为天地一体化信息网络高效能天基节点平台构建、复杂异构网络互联,以及一体化安全防护建设提供借鉴。

本文提出的拟态技术在天地一体化信息网络的应用思路与构想,无论是在理论研究还是工程实践上都有大量工作需要进一步研究:比如拟态计算应用方面,面向天基节点信息处理应用的异构资源池构建、有效载荷认知重构软硬件设计,以及卫星(特别是低轨)平台尺寸、重量和功率(SWaP)的限制等问题,都对拟态计算的认知重构能力,以及计算平台的整体设计提出了新的需求。软件定义互连应用方面,涉及到硬件软件定义、软件可重构、主动业务感知、最佳匹配映射、资源调度管理等系列关键技术;如何面向天基信息网络开展软件定义互连芯片设计,推出开发和应用所需的软硬件工具和支撑环境,是实现复杂异构网络柔性互联的关键。拟态防御应用方面,如何面向天基信息网络开展多维动态重构内生安全机制研究、可重构内生安全架构设计、拟态防御要地建模与脆弱性分析、关键网元设备的拟态化设计与防护、拟态防御有效性度量和测试评估方法,以及拟态防御代价等问题,都需要进一步结合天地一体化信息网络架构、组网模式,以及协议体系开展深入研究。

参考文献

- McKeown N, Anderson T, Balakrishnan H, et al. OpenFlow. *ACM SIGCOMM Comput Commun Rev*, 2008, 38: 69–74
- Hakiri A, Gokhale A, Berthou P, et al. Software-defined networking: challenges and research opportunities for future Internet. *Comput Netw*, 2014, 75: 453–471
- Han B, Gopalakrishnan V, Ji L S, et al. Network function virtualization: challenges and opportunities for innovations. *IEEE Commun Mag*, 2015, 53: 90–97
- Mijumbi R, Serrat J, Gorricho J L, et al. Management and orchestration challenges in network functions virtualization. *IEEE Commun Mag*, 2016, 54: 98–105
- Wu J X. Thoughts on the development of novel network technology. *Sci China Inf Sci*, 2018, 61: 101301 [邬江兴. 新型网络技术发展思考. *中国科学: 信息科学*, 2018, 48: 1102–1111]
- Wu J X. Meaning and vision of mimic computing and mimic security defense. *Telecommun Sci*, 2014, 30: 2–7 [邬江兴. 拟态计算与拟态安全防御的原意和愿景. *电信科学*, 2014, 30: 2–7]
- Wu J X. *Introduction to Cyberspace Mimic Defense*. Beijing: Science Press, 2017 [邬江兴. 网络空间拟态防御导论. 北京: 科学出版社, 2017]
- Lü P, Liu Q R, Wu J X, et al. New generation software-defined architecture. *Sci Sin Inform*, 2018, 48: 315–328 [吕平, 刘勤让, 邬江兴, 等. 新一代软件定义体系结构. *中国科学: 信息科学*, 2018, 48: 315–328]
- Zheng G, Ma H T, Cheng C, et al. Design and logical analysis on the access authentication scheme for satellite mobile communication networks. *IET Inf Secur*, 2012, 6: 6–13
- Bayrakdar M E, Atmaca S, Karahan A. A slotted Aloha based random access cognitive radio network and its performance evaluation. In: *Proceedings of the 20th International Conference on Software, Telecommunications and Computer Networks*. New York: IEEE, 2012. 1–5
- Xiao N, Liang J, Zhang H Y, et al. A channel access strategy based on cognitive radio for satellite communication

- network. *J Astronautics*, 2015, 36: 589–595 [肖楠, 梁俊, 张衡阳, 等. 一种基于认知无线电的卫星网络信道接入策略. *宇航学报*, 2015, 36: 589–595]
- 12 Hwang M S, Yang C C, Shiu C Y. An authentication scheme for mobile satellite communication systems. *SIGOPS Oper Syst Rev*, 2003, 37: 42–47
- 13 Xu G Y, Chen X Y, Du X H, et al. New near space security handoff scheme based on content transfer. *Comput Sci*, 2013, 40: 160–163 [徐国愚, 陈性元, 杜学绘. 一种新的基于上下文传递的临近空间安全切换机制. *计算机科学*, 2013, 40: 160–163]
- 14 He D, Chen C, Chan S, et al. Secure and efficient handover authentication based on bilinear pairing functions. *IEEE Trans Wirel Commun*, 2012, 11: 48–53
- 15 Deng Z, Long B, Lin W, et al. GEO satellite communications system soft handover algorithm based on residence time. In: *Proceedings of the 3rd International Conference on Computer Science and Network Technology (ICCSNT)*. New York: IEEE, 2013. 834–838
- 16 Rahman M, Walingo T, Takawira F. Adaptive handover scheme for LEO satellite communication system. In: *Proceedings of AFRICON*. New York: IEEE, 2015. 1–5
- 17 Wu Z F, Hu G Y, Younes S, et al. A simple real-time handover management in the mobile satellite communication networks. In: *Proceedings of the 17th Asia-Pacific Network Operations and Management Symposium (APNOMS)*. New York: IEEE, 2015. 175–179
- 18 Sun Y, Ji Z, Wang H. TFRC-Satellite: a TFRC variant with a loss differentiation algorithm for satellite networks. *IEEE Trans Aerosp Electron Syst*, 2013, 49: 716–725
- 19 Hou W, Xian B, Guo L, et al. Novel routing algorithms in space information networks based on timeliness-aware data mining and time-space graph. In: *Proceedings of International Conference on Wireless Communications & Signal Processing (WCSP)*. New York: IEEE, 2015. 1–5
- 20 Yavuz A A, Alagz F, Anarim E. SAT05-6: NAMEPS: n-tier satellite multicast security protocol based on signcryption schemes. In: *Proceedings of IEEE Globecom*, 2006. 1–6
- 21 Sun Y, Ma H. Satellite multi-group key management. In: *Proceedings of IEEE 3rd International Conference on Information Science and Technology (ICIST)*. New York: IEEE, 2013. 894–899
- 22 Elmasri M H, Megahed M H, Elazeem M H A. Design and software implementation of new high performance group key management algorithm for tactical satellite. In: *Proceedings of the 33rd National Radio Science Conference (NRSC)*. New York: IEEE, 2016. 149–158
- 23 Hu S M X. Classification and key management approaches for space networks security. In: *Proceedings of International Conference on Anti-counterfeiting, Security and Identification*, Guiyang, 2008. 127
- 24 Li B, Liu C Y, Zhang Y B, et al. Space-based information port and its multi-information fusion application. *J CAEIT*, 2017, 12: 251–256 [李斌, 刘乘源, 章宇兵, 等. 天基信息港及其多源信息融合应用. *中国电子科学研究院学报*, 2017, 12: 251–256]
- 25 Tian X, Ni M, Shi H J, et al. Hardware implementation of space-based network universal service platform. *Comput Syst Appl*, 2018, 27: 45–51 [田雪, 倪明, 施华君, 等. 天基网络化通用服务平台的硬件实现. *计算机系统应用*, 2018, 27: 45–51]
- 26 Wang R, Han X D, Wang C, et al. Resources scheduling and cooperative management of space-based information networks. *J Commun*, 2017, 38: 104–109 [王睿, 韩笑冬, 王超, 等. 天基信息网络资源调度与协同管理. *通信学报*, 2017, 38: 104–109]
- 27 Hu J P, Xu H Z, Li T, et al. Discussion on networked and integrated space-ground information system. *J Spacecr TT&C Tech*, 2016, 35: 241–252 [胡建平, 徐会忠, 李婷, 等. 网络化综合化的天地一体化信息系统探讨. *飞行器测控学报*, 2016, 35: 241–252]
- 28 Wang C, Han X D, Wang R, et al. Study of key technology for reconfigurable satellite platform supporting network

- interconnection. *J Commun*, 2017, 38: 83–87 [王超, 韩笑冬, 王睿, 等. 支持网络互连的可重构卫星平台关键技术研究. *通信学报*, 2017, 38: 83–87]
- 29 Cerf V, Burleigh S, Hooke A, et al. Delay-tolerant network-ing architecture: IETF RFC 4838, informational. Network Working Group, 2007
 - 30 Eggert L. Moving the Undeployed TCP Extensions RFC 1072, RFC 1106, RFC 1110, RFC 1145, RFC 1146, RFC 1379, RFC 1644, and RFC 1693 to Historic Status. HeiseZeitschriften-Verlag, 2011
 - 31 Akyildiz I F, Morabito G, Palazzo S. TCP-Peach: a new congestion control scheme for satellite IP networks. *IEEE/ACM Trans Netw*, 2001, 9: 307–321
 - 32 Akan O B, Fang J, Akyildiz I F. TP-planet: a reliable transport protocol for interplanetary Internet. *IEEE J Sel Areas Commun*, 2004, 22: 348–361
 - 33 Liu J, Cao Z G, Kahan M J. TP-satellite: a new transport protocol for satellite IP networks. *IEEE Trans Aerosp Electron Syst*, 2009, 45: 502–515
 - 34 Luglio M, Sanadidi M Y, Gerla M, et al. On-board satellite “Split TCP” proxy. *IEEE J Sel Areas Commun*, 2004, 22: 362–370
 - 35 Sundararajan J K, Shah D, Médard M. ARQ for network coding. 2008. ArXiv: 0802.1754
 - 36 Barros J, Costa R A, Munaretto D, et al. Effective delay control in online network coding. In: *Proceedings of INFOCOM 2009*. New York: IEEE, 2009. 208–216
 - 37 Chen H, Zhou N, Tong X J, et al. The research on security technology of CCSDS-TC Protocol. *J Nanjing Univ (Nat Sci)*, 2018, 54: 548–554 [陈红, 周钠, 佟晓筠, 等. CCSDS-TC 协议安全技术分析研究. *南京大学学报 (自然科学)*, 2018, 54: 548–554]
 - 38 Hu Z Y, Du X H, Cao L F. One access authentication architecture and method for software defined space-ground integration net-work. *Appl Res Comput*, 2019, 36: 240–244 [胡志言, 杜学绘, 曹利峰. 软件定义天地一体化网络接入认证架构与方法. *计算机应用研究*, 2019, 36: 240–244]
 - 39 Ding K, Chen S, Zhu K, et al. Spacecraft IP network design used in integrated space-ground network. *Spacecr Eng*, 2017, 26: 67–73 [丁凯, 陈淞, 朱珂, 等. 天地一体化网络中的航天器 IP 网络设计. *航天器工程*, 2017, 26: 67–73]
 - 40 Liu L X. Analysis of architecture and protocol of space-ground integrated information network. *J Chongqing Univ Posts Telecommun (Nat Sci Ed)*, 2018, 30: 9–21 [刘立祥. 天地一体化信息网络的体系结构与协议分析. *重庆邮电大学学报 (自然科学版)*, 2018, 30: 9–21]
 - 41 Liu Z F, Sun Z M, Jia Y P. Research and design of near-space access network protocol based on the space-ground integration information network. *J Nanjing Univ (Nat Sci)*, 2018, 54: 562–570 [刘志峰, 孙振明, 贾越普. 基于天地一体化网络架构的临近空间接入网协议设计与研究. *南京大学学报 (自然科学)*, 2018, 54: 562–570]
 - 42 Zhang Y S, Sun C H, Gu J J. Research on protocols of space-ground integrated network. *Radio Eng*, 2018, 48: 178–182 [张亚生, 孙晨华, 谷聚娟. 天地一体化网络协议研究. *无线电工程*, 2018, 48: 178–182]
 - 43 An J P, Jin S, Xu J, et al. Development and outlook of deep space communication network protocol. *J Commun*, 2016, 37: 50–61 [安建平, 靳松, 许军, 等. 深空通信网络协议的发展与展望. *通信学报*, 2016, 37: 50–61]
 - 44 Xu M W, Xia A Q, Yang Y, et al. Intra-domain routing protocol OSPF+ for inte-grated terrestrial and space networks. *J Tsinghua Univ (Sci Tech)*, 2017, 57: 12–17 [徐明伟, 夏安青, 杨荒, 等. 天地一体化网络域内路由协议 OSPF+. *清华大学学报 (自然科学版)*, 2017, 57: 12–17]
 - 45 Lu Y, Zhao Y J, Sun F C, et al. Routing techniques on satellite networks. *J Softw*, 2014, 25: 1085–1100 [卢勇, 赵有健, 孙富春, 等. 卫星网络路由技术. *软件学报*, 2014, 25: 1085–1100]
 - 46 Liu L X. *Space-Ground Integrated Network*. Beijing: Science Press, 2015 [刘立祥. 天地一体化网络. 北京: 科学出版社, 2015]
 - 47 Spyropoulos T, Psounis K, Raghavendra C S. Spray and wait: an efficient routing scheme for intermittently connected mobile networks. In: *Proceedings of ACM SIGCOMM Workshop on De-lay-Tolerant Networking*. New York: ACM,

2005. 252–259
- 48 Khouzani M, Eshghi S, Sarkar S, et al. Optimal energy-aware epidemic routing in DTNs. *IEEE Trans Automat Contr*, 2015, 60: 1554–1569
- 49 Iyengar S, Cruickshank H, Pillai P, et al. Security requirements for IP over satellite DVB networks. In: *Proceedings of the 16th IST Mobile and Wireless Communications Summit*, 2007. 1–6
- 50 Cruickshank H, Iyengar S, Fan L, et al. Secure composite satel-lite IP multicast architecture for heterogeneous groups. In: *Proceedings of the 16th IST Mobile and Wireless Communications Summit*, 2007. 1–5
- 51 Liang L, Cruickshank H, Sun Z. TESLA with FLUTE over satel-lite networks. In: *Proceedings of IEEE International Conference on Communications*, 2008
- 52 Li H, Fan X X, Bi J N, et al. Analysis of security technologies in integrated space-air-ground networks. *J China Acad Electron Inform Tech*, 2014, 9: 592–597 [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. *中国电子科学研究院学报*, 2014, 9: 592–597]
- 53 Qin Z C, Zhang P, Fan X X, et al. Design of security verification platform for the integrated space-ground network. *Chin J Netw Inform Secur*, 2016, 2: 39–47 [秦智超, 张平, 范鑫鑫, 等. 面向天地一体化信息网络的安全验证平台设计. *网络与信息安全学报*, 2016, 2: 39–47]
- 54 Li F H, Yin L H, Wu W, et al. Research status and development trends of se-curity assurance for space-ground integration information net-work. *J Commun*, 2016, 37: 156–168 [李凤华, 殷丽华, 吴巍, 等. 天地一体化信息网络安全保障技术研究进展及发展趋势. *通信学报*, 2016, 37: 156–168]
- 55 Ma Z, Ma J F, Li X H, et al. Provable security model for trusted network connect protocol. *Chin J Comput*, 2011, 34: 1669–1678 [马卓, 马建峰, 李兴华, 等. 可证明安全的可信网络连接协议模型. *计算机学报*, 2011, 34: 1669–1678]
- 56 Ji X S, Liang H, Hu H C. New thoughts on security technologies for space-ground inte-gration information network. *Telecommun Sci*, 2017, 37: 24–35 [季新生, 梁浩, 扈红超. 天地一体化信息网络安全防护技术的新思考. *电信科学*, 2017, 37: 24–35]
- 57 Anggorojati B, Mahalle P, Prasao N R, et al. Capabil-ity-based access control delegation model on the federated IoT net-work. In: *Proceedings of Symposium on Wireless Personal Multimedia Communications*, 2012. 604–608
- 58 Gusmeroli S, Piccione S, Rotondi D. IoT access control issues: a capability based approach. In: *Proceedings of the IEEE International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 2012. 787–792
- 59 Gusmeroli S, Piccione S, Rotondi D. A capability-based security approach to manage access control in the Internet of things. *Math Comput Model*, 2013, 58: 1189–1205
- 60 Bernabe J B, Ramos J L H, Gomez A F S. TACIoT: multidimensional trust-aware access control system for the Internet of Things. *Soft Comput*, 2016, 20: 1763–1779
- 61 Feng X S, Liu D S, Yue J, et al. Exploration on access control tonear space in-formation resources. *Appl Res Comput*, 2008, 25: 3702–3704 [封孝生, 刘德生, 乐俊, 等. 临近空间信息资源访问控制策略初探. *计算机应用研究*, 2008, 25: 3702–3704]
- 62 Qi H, Ma H, Li J, et al. Access control model based on role and attribute and its applications on space-ground integra-tion networks. In: *Proceedings of the IEEE International Conference on Computer Science and Network Technology*, 2015. 1118–1122
- 63 Li F H, Wang Y C, Yin L H, et al. Novel cyberspace-oriented access control model. *J Commun*, 2016, 37: 9–20 [李凤华, 王彦超, 殷丽华, 等. 面向网络空间的访问控制模型. *通信学报*, 2016, 37: 9–20]
- 64 Li F H, Chen T Z, Wang Z, et al. Cross-network access control mechanism for complex network environment. *J Commun*, 2018, 39: 1–10 [李凤华, 陈天柱, 王震, 等. 复杂网络环境下跨网访问控制机制. *通信学报*, 2018, 39: 1–10]
- 65 Jha S, Sural S, Vaidya J, et al. Security analysis of temporal RBAC under an administrative model. *Comput Secur*, 2014, 46: 154–172
- 66 Yang L, Tang Z, Li R F, et al. Roles query algorithm in cloud computing environ-ment based on user require. *J*

- Commun, 2011, 32: 169–175 [杨柳, 唐卓, 李仁发, 等. 云计算环境中基于用户访问需求的角色查找算法. 通信学报, 2011, 32: 169–175]
- 67 Luo J, Wang H, Gong X, et al. A novel role-based access control model in cloud environments. *Int J Comput Intell Syst*, 2016, 9: 1–9
 - 68 Li J W, Squicciarini A, Lin D J, et al. SecLoc: securing location-sensitive storage in the cloud. In: *Proceedings of the 20th ACM Symposium on Access Control Models and Technologies*, 2015. 51–61
 - 69 Zhou L, Varadharajan V, Hitchens M. Trust enhanced cryptographic role-based access control for secure cloud data storage. *IEEE Trans Inform Forensic Secur*, 2015, 10: 2381–2395
 - 70 Zhou L, Varadharajan V, Gopinath K. A secure role-based cloud storage system for encrypted patient-centric health records. *Comput J*, 2016, 59: 1593–1611
 - 71 Xu P, Jiao T, Wu Q, et al. Conditional identity-based broadcast proxy re-encryption and its application to cloud email. *IEEE Trans Comput*, 2016, 65: 66–79
 - 72 Zhang Y, Li J, Chen X, et al. Anonymous attribute-based proxy re-encryption for access control in cloud computing. *Secur Commun Netw*, 2016, 9: 2397–2411
 - 73 Li J G, Zhao X X, Zhang Y C, et al. Provably secure certificate-based conditional proxy re-encryption. *J Inf Sci Eng*, 2016, 32: 813–830
 - 74 Yang Y, Lu H, Weng J, et al. Fine-grained conditional proxy re-encryption and application. In: *Proceedings of International Conference on Provable Security*, 2014. 206–222
 - 75 Su M, Shi G Z, Xie R N, et al. Multi-element based on proxy re-encryption scheme for mobile cloud computing. *J Commun*, 2015, 36: 73–79 [苏钺, 史国振, 谢绒娜, 等. 面向移动云计算的多要素代理重加密方案. 通信学报, 2015, 36: 73–79]
 - 76 Su M, Li F H, Shi G Z, et al. A user-centric data secure creation scheme in cloud computing. *Chin J Electron*, 2016, 25: 753–760
 - 77 Su M, Shi G Z, Fu A M, et al. Proxy re-encryption based multi-factor access control scheme in cloud. *J Commun*, 2018, 39: 96–104 [苏钺, 史国振, 付安民, 等. 基于代理重加密的云端多要素访问控制方案. 通信学报, 2018, 39: 96–104]

Development status and applied research on mimic technologies for space-ground integration information network

Hao LIANG*, Fucui CHEN, Xinsheng JI, Ping LÜ & Yanzhao GAO

National Digital Switching System Engineering and Technological Research Center, Zhengzhou 450002, China

* Corresponding author. E-mail: lhmailhappy@163.com

Abstract Space-ground integration information network is one of the national science and technology major projects aimed toward 2030. However, the existing network architecture and technical systems still face a series of challenges such as high-performance network node, efficient internetworking, and integrated security architecture. The main research objective of this study is the application of mimic technologies. Herein, according to the analysis of the technical challenges, the existing protection technologies, and the ideas of space-ground integrated information network, the application of mimic defense, mimic computing, and software-defined interconnection technology in the space-ground network architecture and key information system are proposed. Related technical ideas and the proposed design can be used to provide a reference for the building of space-ground integration information network with high-speed, efficiency, flexibility, and security.

Keywords space-ground integration information network, mimic defense, mimic computing, software-defined interconnection

Hao LIANG was born in 1987. He received his M.S. and Ph.D. degrees at the Electronics Engineering Institute (EEI), Hefei, China, in 2013 and 2016, respectively. He is currently a research associate at the China National Digital Switching System Engineering & Technological Research Center (NDSC). His research interests include mimic defense security, active defense, and cloud computing.

Fucai CHEN was born in 1974. He received his master's degree at the Information Engineering Institute, Zhengzhou, in 2002. He is currently a senior research fellow at the China National Digital Switching System Engineering & Technological Research Center (NDSC). His research interests include wireless mobile communication, network security, and active defense.

Xinsheng JI was born in 1968. He received his master's degree at the Information Engineering Institute, Zhengzhou, in 1991. He is currently a professor at the China National Digital Switching System Engineering & Technological Research Center (NDSC). His research interests include wireless mobile communication, network security, and novel network architecture.

Ping LÜ was born in 1977. She received her master's degree at the China National Digital Switching System Engineering & Technological Research Center (NDSC) in 2007. She is currently pursuing her Ph.D. degree at NDSC. Her research interests include new architectures and new generations of information communication technology.