



专题：天地一体化信息网络

天地一体化信息网络安全防护技术的新思考

季新生, 梁浩, 扈红超

(国家数字交换系统工程技术研究中心, 河南 郑州 450002)

摘要: 天地一体化信息网络是国家面向 2030 的重大科技工程, 安全防护是保障其运行的关键。由于能够主动适应用户、网络和业务的快速变化, 可以实现网络技术与安全的共生演进, 天地一体化信息网络成为近年来国内外学术界和产业界普遍关注的重要方向。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思路的基础上, 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, 相关技术思路和设计可为内生安全的天地一体化信息网络安全防护体系建设提供参考。

关键词: 天地一体化信息网络; 安全防护; 内生安全; 拟态防御

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2017335

New thoughts on security technologies for space-ground integration information network

Ji Xinsheng, LIANG Hao, HU Hongchao

National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China

Abstract: Space-ground integration information network is one of the national science and technology major projects toward 2030, and the key to its running stability is security protection. However, the defense technology which has intrinsic security without depending on priori knowledge and being based on boundary is able to adapt proactively to rapid changes in users, networks and requirements, therefore it has become a significant development direction of academic and industrial circles. Based on the analysis of the security threats and the existing protection technologies and ideas of the integrated information network, the application of endogenous security defense technology in the world network architecture and key information system was discussed. Related technical ideas and design proposed can be used to provide reference for building of security protection system on space-ground integration information network with intrinsic security.

Key words: space-ground integration information network, security protection, intrinsic security, mimic defense

收稿日期: 2017-11-10; 修回日期: 2017-12-11

通信作者: 梁浩, lhmailhappy@163.com

基金项目: 国家自然科学基金创新研究群体资助项目 (No.61521003); 国家重点研发计划基金资助项目 (No.2016YFB0800100, No.2016YFB0800101); 国家自然科学基金资助项目 (No.61602509); 河南省科技攻关计划基金资助项目 (No.172102210615); 信息工程大学新兴方向培育基金资助项目 (No.2016610708)

Foundation Items: Innovative Research Groups of the National Natural Science Foundation of China (No.61521003), The National Key R&D Program of China (No.2016YFB0800100, No.2016YFB0800101), The National Natural Science Foundation of China (No.61602509), The Science and Technology Research Project of Henan Province (No.172102210615), The Emerging Direction Nurturing Foundation in Information Engineering University (No.2016610708)

1 引言

天地一体化信息网络是国家面向2030的重大科技工程,其核心建设思路是以地面网络为依托、天基网络为拓展,采用统一的技术架构、统一的技术体制、统一的标准规范,由天基信息网、地面互联网和移动通信网互联互通而成^[1],对拓展国家利益、维护国土安全、保障国计民生、促进经济发展具有重大意义,是我国信息网络实现信息全球覆盖、宽带传输、军民融合、自由互联的必由之路^[2]。

安全防护保障作为天地一体化信息网络可靠运行的关键支撑,其重要性不言而喻。有别于传统网络,天地一体化信息网络节点分布广泛、体系结构复杂、信道开放透明、拓扑动态变化、大尺度传输链路以及面向全球提供服务保障的网络特征,使其数据传输、信息服务等本身就更易受到来自外部的自然干扰和恶意攻击,这对网络的路由、切换、传输、接入等方面的安全运行能力提出了更高要求。同时当前我国天基信息网、互联网、移动通信网的发展很不平衡,总体上仍呈现“天弱地强”的特征;具有自主知识产权的空天地一体化全球信息网络及关键技术的标准化提案相对较少,特别是基础网络和信息系统在核心技术、基础软件、关键芯片及设备等方面对外依存度还比较高,面向天地一体化信息网络的安全防护面临诸多挑战。

近年来学术界在天地一体化信息网络安全防护方面的研究^[3-11]不断深入,但技术途径大多停留在传统的基于精确感知的被动式静态防御思路上,难以满足用户、网络和业务等的动态化安全防护需求;尤其是以星载设备为代表的安全组件,其载荷、处理能力有限,后期设备更新升级难度大^[12,13],难以适应网络架构和技术的长期演进和攻击技术的快速变化,更无法有效抵御基于未知漏洞和隐蔽后门的未知网络攻击,难以感知信息

化战争条件下瞬息万变的安全威胁态势。本文针对现有防护思路存在的局限性,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思路的基础上,探讨了拟态防御技术在天地网络架构、关键信息系统中的应用设想,为内生安全的天地一体化网络安全防护体系建设提供思路和技术借鉴。

2 网络特征和安全威胁

2.1 网络特征

天地一体化信息网络联网节点覆盖范围广、数量庞大、种类丰富、资源能力各不相同,在体系结构、传输信道、拓扑连接以及运行服务等方面具备以下典型特征。

(1) 网络体系结构复杂化

天地一体化信息网络涉及卫星网络、近地空间网络、地面无线移动网络、互联网等多层异质网络融合,网络规模庞大,结构极为复杂,呈现出立体多维异构典型特征。同时,各网络采用不同的制式,基于不同形态的物理资源,工作在不同频段,在发射功率、覆盖范围、传输体制、控制开销、管理方式、运行维护等方面存在巨大差异。

(2) 网络通信信道开放化

相比传统网络,信道开放、透明的特征在天地一体化信息网络中更加明显,特别是高低轨卫星节点,长期运行在暴露的空间轨道上,星间、星地等无线通信链路很容易遭受来自恶劣自然环境和恶意用户的影响。

(3) 网络拓扑连接动态化

地球的自转与公转使得天地一体化信息网络节点动态变化,特别是中低轨卫星始终处于高速运转状态,存在频繁地接入或退出组网的情况,网络拓扑变化频繁,网络稳定连通性遇到较大挑战,甚至需要数据重传。

(4) 网络传输链路跨域化

天地一体化信息网络节点分布稀疏,陆、



海、空、天的全维度覆盖使得通信链路具备大时间/空间尺度跨域传输与组网的特征，超出传统地面网络传输控制协议适应范围的传输距离，使得数据传输存在往返时延高、信号抖动幅度大以及星地网络上下行链路传输带宽不对称等特点，增大了节点接收机的灵敏度和处理的复杂度。网络拓扑的动态化进一步减小了通信节点的信号覆盖范围，加剧了通信链路的间歇性和持续保持的难度。

（5）网络服务保障全球化

面向全球提供联合作战、公共安全、应急救援、抢险救援、交通物流、空中交通管理、海洋维权、智慧城市等多样化应用服务，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处理、有效载荷、安全可靠能力提出新的要求和挑战。

2.2 面临的主要安全威胁

典型的网络特征及面向军、民各类用户实现海量信息的融合及多样化应用服务的灵活定制需求，为高效随遇接入、安全可靠可信的天地一体化信息网络建设带来诸多威胁与挑战。

（1）未知“漏洞、后门”带来的不确定安全威胁

无处不在的“漏洞、后门”威胁造成不确定安全威胁和安全防护困境，主要体现在：一方面，网络和信息系统的软硬件设计缺陷客观存在、不可避免，而任何一个缺陷或错误都有可能引入安全漏洞并被网络攻击者利用；另一方面，产品设计、制造等各个环节的安全性越发不可控，存在恶意功能被隐蔽植入、“漏洞”功能被隐匿预留以及“后门”功能被隐蔽预埋的危险。天地一体化信息网络承载涉及国家战略安全利益的核心应用，担负网络安全保障由传统的国土信息网络向陆、海、空、天全球覆盖信息网络转变的责任，急需在核心技术、关键芯片和设备方面实现自主

可信、可靠和可控，面向不确定威胁实现动态灵活安全防护。

（2）开放式通信环境带来的信道安全威胁

天地一体化信息网络开放、透明的特征，使得通信信道面临极为复杂严峻的安全威胁态势。一方面来自太空太阳黑子爆发、宇宙射线等诸多不可抗的自然因素，会对星载基础设施形成严重的物理影响和破坏；同时无线链路也极易受到高空电离层反射信号、空间电磁辐射等复杂恶劣自然环境的干扰，致使正常的通信产生畸变、数据传输受到影响甚至发生中断。另一方面开放式的通信环境也使得无线信道极易受到来自恶意用户的非法窃听和截获，并有针对性地利用卫星信号转发、模拟伪造、噪声干扰等方式实现对星地/星间通信信道的蓄意欺骗、干扰和压制，产生用户身份不可信、网络地址易伪造、系统服务不可控、信息易被篡改、系统保密性差等安全问题。

（3）大尺度跨域防护带来的接入安全威胁

天地一体化信息网络大时间/空间尺度跨域传输与组网，任意可能存在的脆弱点、安全漏洞、无效配置等安全缺陷带来接入安全威胁，面临恶意用户非法利用、病毒/木马等各类恶意代码或程序被植入的风险，致使网络系统发生异常，甚至被远程操控或瘫痪，如星地大尺度传输的脆弱性形成的通信中断后的数据重传，使非法用户劫持、冒充原有合法网络节点，泄露、篡改、伪造正常传输数据成为可能；传统网络中 SYN 攻击、中间人攻击、DDoS 等攻击方式，也使得一体化网络面临路由转发节点数据被篡改、传输时延大幅增加、通信资源被耗尽等安全威胁风险；不同安全等级用户网络的接入以及网络拓扑的动态变化，带来跨域统一身份管理、可信认证、访问控制等安全问题。

（4）一体化服务保障带来的可靠性安全威胁

天地一体化信息网络面向用户提供可靠的服务保障，军民共用的现实需求面临身份冒用伪装、

非法权限窃取、越权操作等安全威胁,亟需开展对服务请求的军民身份鉴别、不同粒度安全层级的隔离等研究,防止网络数据的泄露和控制权限被窃取。同时,卫星自身载荷能力有限,自身数据计算、处理能力和硬件可扩展性受限,加之面对天地复杂物理环境和全维度空天一体化服务保障需求,亟需开展抗攻击的网络资源弹性重组、安全服务快速部署与迁移以及故障组件的诊断、清洗与恢复等技术,以提高一体化网络在(未知)攻击、故障或事故(包含自然干扰、人为攻击等造成)存在的情况下服务可靠保障能力和服务中断时快速有效恢复的弹性性能。

3 现有主要安全防护技术思路

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,涉及系统的各个层面,需要体系化的安全防护设计。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。

参考文献[3]认为天地一体化信息网络在设计及建设初期就要将网络及电磁空间安全问题放在首要位置,解决好网络开放性带来的安全性挑战,相关建议可为我国天地一体化信息网络的建设提供参考。参考文献[4]指出天地一体化信息系统规模大、覆盖广、体系开放,极易被攻击和入侵,除了考虑传统网络协议层的安全外,还要考虑物理层和链路层节点间的安全机制,采取抗毁防压措施,设计安全协议,筹备安全方案,完善网络系统的生存能力。参考文献[5]认为必须将安全防护思想融合到天地一体化网络的体系结构中,保障天地一体化网络的正常运行,通过深入分析天地一体化网络面临的安全威胁,提出一体化网络安全防护未来发展亟待解决的关键技术。参考文献[6]分析了目前信息网络空间的脆弱性和主动自

防御具有的功能,提出了天地一体化信息网络空间支持技术应实现从被动反应式防御到主动自防御转变的概念,并给出了一种基于DTN(delay/disruption tolerant networking)的组网架构和主动自防御建模仿真实现方法。参考文献[7]分析了当前无线网络面临的现实问题,通过构建主动积极的无线网络安全防御体系,提出了一种适合军民融合的无线网络安全体系模型,其安全设计思路可为空天地一体化网络提供指导。参考文献[8]针对天地一体化信息网络面临的安全威胁,从通信、网络、应用3个层面研究天地一体化网络安全体系结构和安全策略,涉及网络与通信传输安全、区域边界安全、应用环境安全、统一密码管理中心和统一安全管理中心等方面。参考文献[9]基于信息安全模型^[14],结合天地一体化信息网络安全实际,从物理安全、运行安全、数据安全3个层面对其安全保障技术的研究现状进行了阐述,其中,物理安全主要采用抗毁技术、抗干扰技术、人工噪声、多波束通信等保障技术对网络中物理装置或设备进行防护,运行安全主要采用安全接入、安全切换、入侵检测、访问控制等保障技术对网络的运行过程、状态等进行保护,数据安全主要采用安全传输、密钥管理等保障技术对数据的收集、处理、传输等过程进行保护。参考文献[10]总结了目前天地一体化信息网络在各个层次中可能受到的攻击方法和防御手段,见表1,并对其安全防护系统进行建模分析。参考文献[11]认为天地一体化网络系统复杂、技术体制多样,其中安全技术涉及系统的各个层面,难以通过单项技术试验实现系统层面的验证和评估,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,支持实现密钥管理、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,为天地一体化网络安全各方面技术的集成演示验证提供一个综合试验环境。



表 1 天地一体化信息网络所面临的攻击

攻击类型	发生层次	预防机制
拥塞	物理层	扩频、较低占空比
篡改	物理层	有效密钥管理方案
窃听	物理层	加密
碰撞	数据链路层	错误检测
耗尽	数据链路层	传输率限制
通信量分析	网络层	链路加密、匿名通信
操控路由信息	网络层	认证、加密
选择性转发	网络层	冗余、探测
Sybil 攻击	网络层	认证、加密
重放攻击	网络层	双向认证、3 次握手
黑洞攻击	网络层	认证、监控、冗余
虫洞攻击	网络层	监控、灵活路由选择
Hello flood 攻击	网络层	双向认证、3 次握手
泛洪攻击	传输层	限制链接数目、客户难题
克隆攻击	应用层	唯一密钥对

上述研究可为天地网络安全防护体系的设计提供重要参考。然而，随着空间网络形态的不断演化，网络设备泛在互联、攻击技术的不断进化，网络攻击呈现“隐蔽性、协同性、精确性”等诸多特点，导致现有安全防护技术思路面临巨大挑战，主要表现在如下几个方面。

- 现有安全防护技术思路大都依赖于攻击先验知识(如杀毒软件、防火墙、IPS/IDS 等)，属于“威胁特征和攻击行为感知”的被动式防御思路，首先必须获取攻击的先验知识才能有效防御，这和攻击先验知识难以准确获取本身是一对矛盾。因此，对已知的网络威胁能够高效、精确识别，但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 0day 攻击、APT 等)。
- 部署模式严重依赖于边界且静态化。现有安全防护技术手段大都采用各类专用软硬件堆叠而成，静态、固化地部署在用户侧或网络边界处。然而，由于各类安全功能彼此间接口封闭，缺乏统一的联动机制，因此，安全能力之间难以形成协同，无法有效应对高强度和复杂网络攻击；同时单

一性、静态性的防御技术尽管一定程度上提高了攻击成功的门槛，但易被攻击者通过目标对象内部的安全漏洞以及可能被预先植入的后门绕过、穿透。

- 网络技术和安全技术难以实现共生演进。对于防护目标而言，传统安全防护技术机制一般通过“外挂”或“附加”功能外置方式提供安全防护能力，与防护目标自身结构与功能的设计基本是相互独立的，在网络变化时需要重新设计和部署安全机制，导致安全技术始终滞后于网络技术的发展，无法实现与网络技术的协同演进；同时由于采用专用软硬件开发完成，研制周期长，难以适应信息化战争条件下瞬息万变的威胁态势，难以满足用户、网络和业务等的动态化安全防护需求；特别是固定防御能力的安全组件(尤其是星载设备载荷有限、设备更新升级难度大^[12,13])，随着环境的不断变化以及攻击者攻击能力的不断提升，其防御能力的持续性和有效性面临考验。

作为面向 2030 的重大科技工程，天地一体化信息网络的建设既要立足现有国家和军队网络需求，又要兼顾网络和安全技术的长远发展。因此，天地网络安全防护技术思路必须能够应对网络攻击技术的不断进化以及新网络体制和技术机制下新的安全威胁。从技术发展的角度来看，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由于能够主动适应用户、网络和业务的快速变化得到迅速发展，为天地一体化网络的安全防护提供了新思路和技术途径。

4 天地一体化信息网络内生安全机制设计

从前面的讨论可以看出，传统被动式防御技术思路难以有效适应天地网络的长期演进和攻击技术的快速发展变化。为此，本文提出基

于拟态防御的天地一体化信息网络内生安全机制应用设计思路。首先介绍了拟态防御的基本思想和技术特性,在此基础上进一步探讨了拟态防御在天地一体化信息网络架构、关键信息系统中的应用设想,并以拟态地面节点网络路由器和拟态地面信息港云平台为典型系统进行应用示例。

4.1 拟态防御

4.1.1 基本思想

“拟态防御”基本思想^[15]是在可靠性领域非相似余度构造中导入动态性和随机性元素,从而创造出一种功能等价条件下的动态异构冗余架构。其基于多模裁决的策略调度和多维动态重构机制,既能给借助目标系统内部“漏洞后门”的网络攻击造成“防御迷雾”,也能屏蔽由于服务装置设计缺陷或随机失效导致的“差模故障”。其高可靠、高可用、高顽健三位一体的“内生安全”属性,允许目标对象在拟态界内使用“全球化条件下可信性不能确保供应链”的软硬构件,且能在缺乏攻击者信息和行为特征的情况下对“已知的未知”风险或“未知的未知”威胁实施可度量的安全防护。

从技术思路上来说,网络空间拟态防御本质上创造了“动态异构冗余—多模裁决—异常清洗”的网络防御新模式,如图 1 所示,具体为:对于拟态界内被保护的功能过程,动态异构冗余构造建立和动态调度功能等价的异构执行体集合,从时间、空间两个维度上动态改变系统功能与实现结构之间的对应关系,使攻击者对目标对象的结构、运行环境等陷入迷茫,探测感知或预测防御行为的难度呈非线性增加;多模裁决对异构冗余执行体的输出矢量进行表决,产生正确的输出响应,并裁决出“与众不同”的可疑执行体,从而将攻击事件转换为对防御者而言概率可控的可靠性问题,迫使攻击方必须面对非配合条件下对动态目标实施协同一致攻击的挑战;此外,防御方

实时对攻击效果进行度量和评估,有策略地执行清洗和多维动态重构,使得攻击者视在的防御场景更趋动态复杂,攻击经验无法复制或继承,呈现出对目标体结构和运行环境的“测不准”效应,攻击行动无法产生可规划、可预期的效果。这些机制对传统攻击理论和方法将产生颠覆性的影响,大幅增加攻击难度和成本,从根本上改变“易攻难守”的攻防格局。

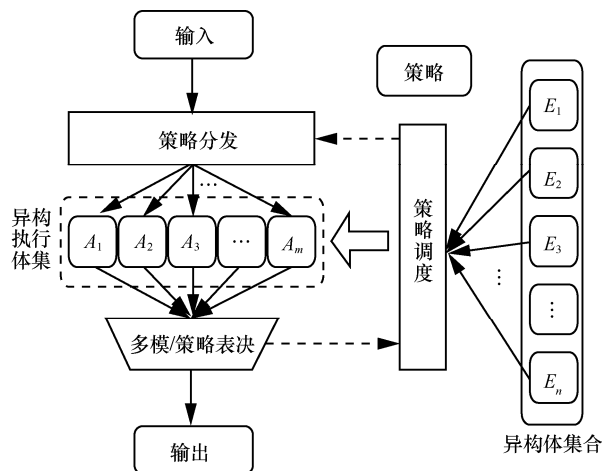


图 1 拟态防御的动态异构冗余构造

4.1.2 技术特性

从技术体制上来说,拟态防御是一种内生的融合式防御机制,其内生性体现为在非相似余度构造上导入生物拟态伪装策略的“动态异构冗余构造”,类似于脊椎动物非特异性和特异性双重免疫机制的物理构造,基于该构造的防御机制具有“通杀”能力,使得目标对象能够在不依赖任何先验知识或者“攻击行为特征库”、不需要现有防御技术手段支撑的条件下,独立有效地应对基于已知和未知漏洞后门的已知和未知威胁。同时,能够降低基于目标对象未知漏洞后门等未知攻击的确定性,并将不确定攻击效果转变为概率可控的可靠性事件。这些防御效果使得防御方只需采用统一的内生安全架构即可破解基于未知漏洞和后门的安全威胁,而攻击者必须面对“动态冗余空间,非配合条件下多元目标协同一致攻击”的挑



战，大幅提升了其难度和代价。即便攻击者一次攻击成功，其攻击手法和经验也难以复现或继承，失去传播利用价值，实现了防御方获得对攻击方的非对称优势。其次，拟态防御不再需要防御方预先掌握攻击方的先验知识，消除了攻击方在行为、时空等方面不确定而带来的“出其不意、先发制人”的战略主动优势。再者，采用拟态防御的信息系统的安全性由内生安全架构决定，不依赖于特定异构执行部件的先进或安全与否，在符合功能等价的条件均可使用，缓解了技术先进国家对后进国家的“卖方市场”优势。

4.2 应用设想

4.2.1 具备内生安全的防护体系架构

本文提出的具备内生安全的天地网络安全防护体系的基本思路是：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2所示。

智能态势感知层面提供威胁情报、数据融合、智能分析、决策预警和全局安全可视等；安全支

撑层面提供身份管理、权限管理、密码资源管理、密码服务、密码算法、密码协议等基础安全能力；接入层面支持接入认证、动态授权、接入控制、无线接入安全、链路可信保持和无缝安全切换等能力；利用具有多维动态重构特性的拟态防御内生安全技术机制，在系统层面提供硬件、软件和运行环境等的内生安全能力；在网络层面提供源地址认证、网络实体认证、边界安全、安全路由交换协议、信息安全管理网间互联安全等能力；安全防护中心在安全云平台的支撑下提供安全服务编排、安全服务管理和网络运行监测以及按需安全服务和协同联动感控能力。

在具体实现上，通过将动态异构冗余基因应用到云网架构层面，形成动态路由、动态IP地址、动态拓扑结构、动态异构协议等安全机制；应用到天基骨干网、天基接入网、地基节点网和服务平台等节点层面，形成拟态化网络控制器、拟态化路由器、拟态化DNS服务器、拟态化威胁感知器和拟态化云服务平台等；应用到构件层面，形成各类拟态化构件，如图3所示。

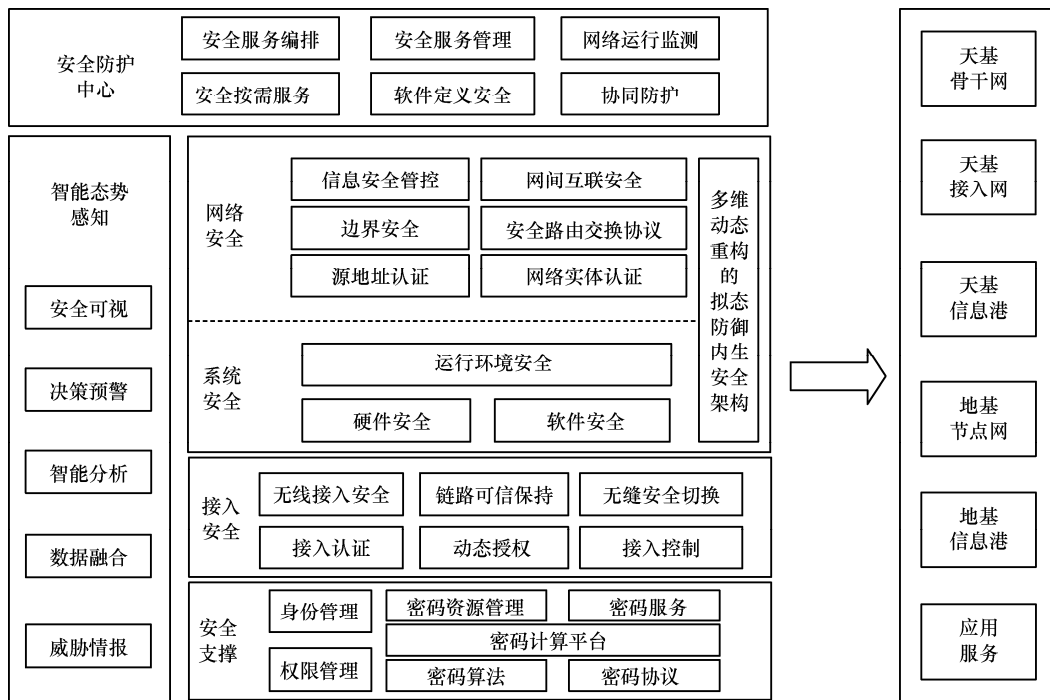


图2 天地一体化网络安全防护体系架构

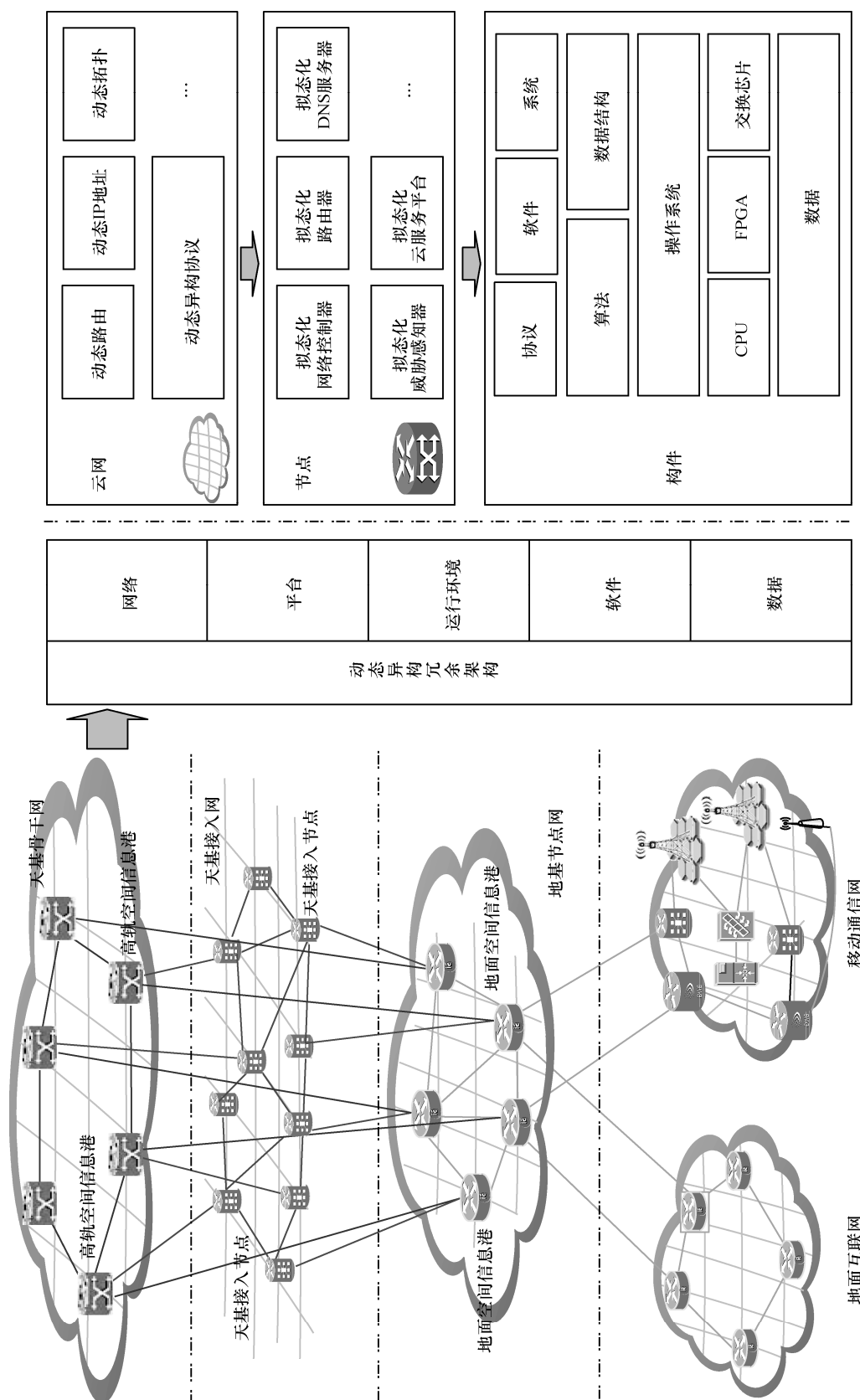


图3 内生安全防护架构的应用示意



4.2.2 典型系统应用示例

(1) 拟态地面节点网路由器

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。数据转发平面的功能就是对进入系统的数据进行查表，并按照查表结果将数据转发出去。路由控制平面通过运行各种不同的路由协议实现路由计算，并将产生的路由表项传送给转发平面使用，而各个功能的运行则由配置管理平面通过配置管理规则（如 CLI、SNMP 或者 Web 等）进行配置管理，处理流程可以归纳为：从网络中邻居节点接收路由通告，进行路由计算后生成路由表项，并向邻居节点输出本地计算的路由结果。配置管理平面的处理流程可以归纳为：接收网络管理者的管理配置请求，执行配置管理操作，输出配置管理结果。数据转发平面的处理流程可以归纳为：从接口单元获得接口输入的数据分组，进行输入操作后查找本地转发表，对数据分组进行匹配操作后，按照转发指示从对应接口将数据分组输出。

基于上述分析，设计的拟态路由器系统架构^[17]如图4所示，分为硬件层面和软件层面。硬件层面

为标准的 OpenFlow 交换机（OpenFlow switch, OFS），软件层面包括 OFC、代理插件、拟态裁决、异构执行体池、动态调度以及感知决策单元（这些单元统称为拟态插件）。在该系统架构中，OFC 基于消息的协议类型进行消息分发，由多个代理插件基于各自的协议机制进行有状态或者无状态处理后分发给各个执行体；各个执行体的协议软件对收到的消息进行处理，产生流表信息和对应的输出消息；各个执行体产生的路由表信息经拟态裁决产生“可信”的表项下发给 OFS。拟态裁决结果触发控制机制，实现对执行体调度、清洗修复或重构重组等操作。

(2) 拟态地面信息港云平台

拟态云虚拟可信平台的基本思想是将拟态防御的动态、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，构建安全可信的拟态虚拟机、拟态容器、拟态存储和拟态控制组件，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。拟态云虚拟可信平台主要包括拟态虚拟机、拟态容器和拟态存储以及拟态调度器和控制器、镜像管理等，如图5所示。

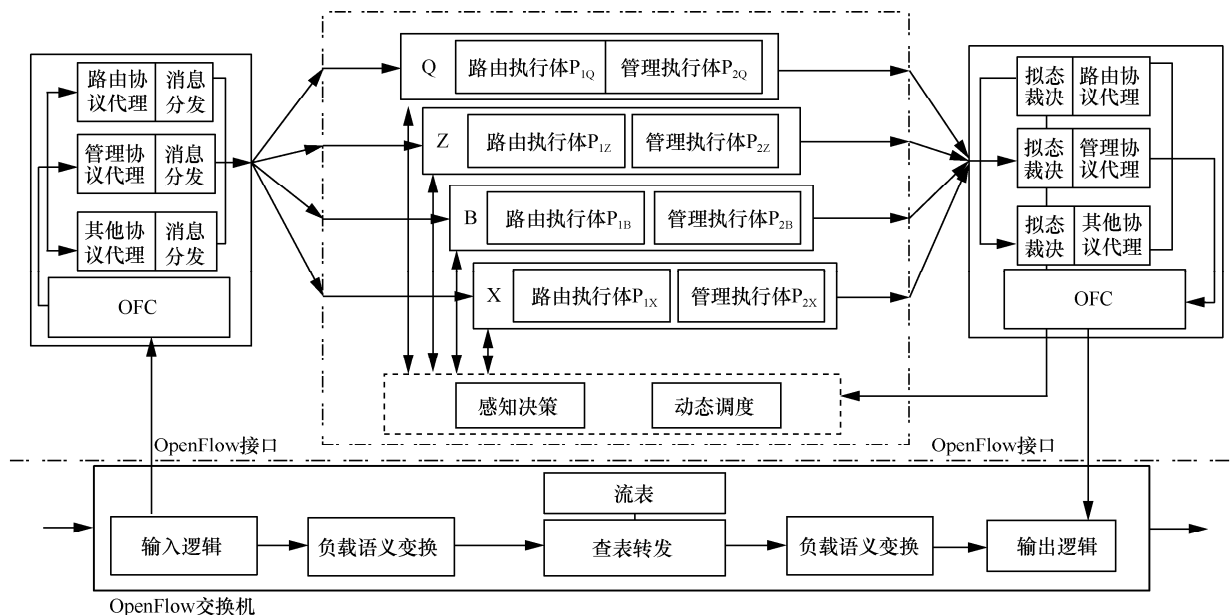


图4 地面节点网拟态路由器架构

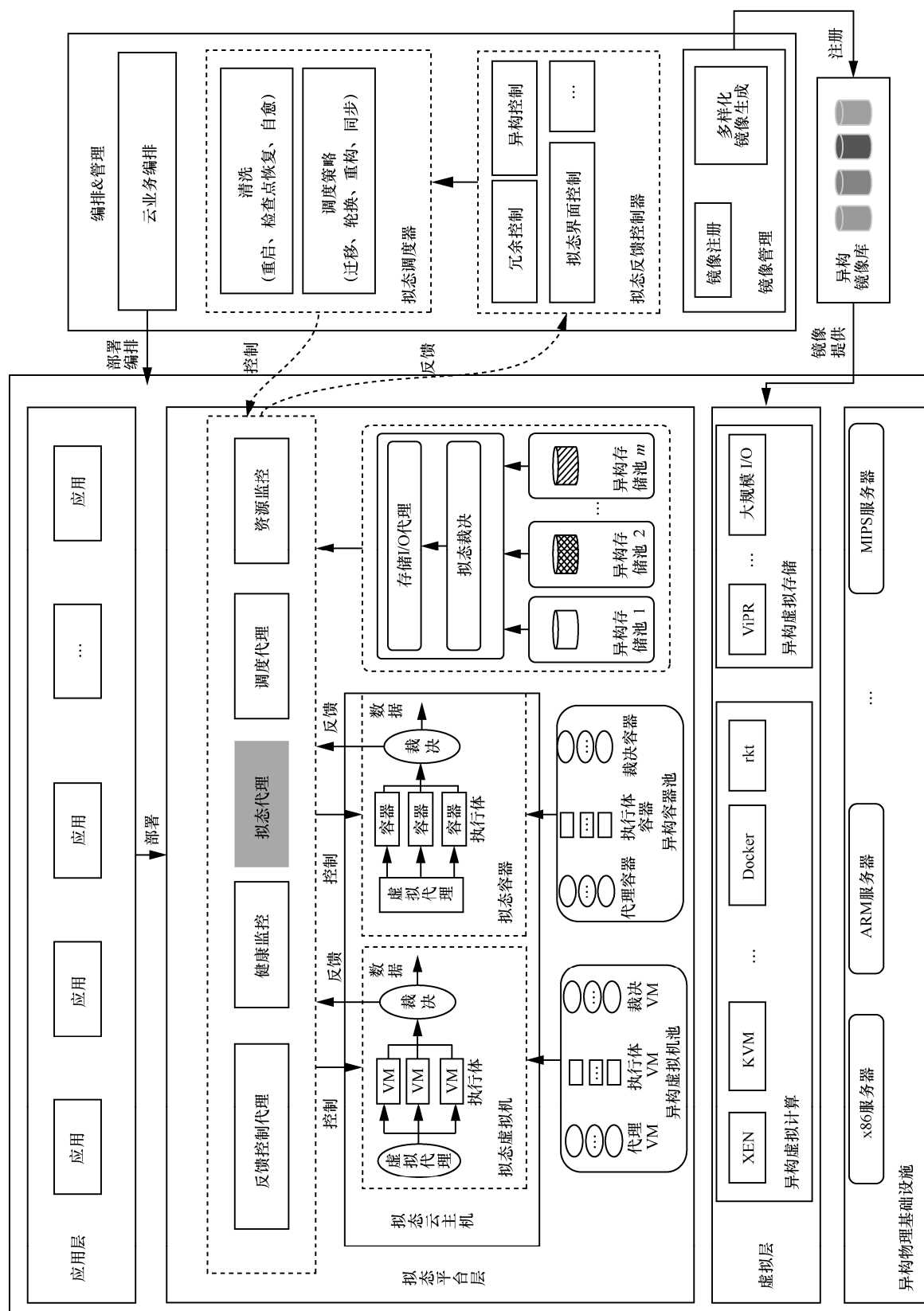


图5 拟态云虚拟可信平台实现思路



虚拟资源池提供异构的虚拟机、容器和存储组件, 拟态云虚拟可信平台对异构的虚拟机、容器和存储组件进行拟态化, 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, 每个结构内部均包括虚拟代理、异构冗余执行体、虚拟裁决器, 由“拟态代理”负责拟态结构对外的单一呈现, 控制代理、健康监控等负责将运行、裁决信息反馈至云管理系统中。在云管理系统中, 引入拟态调度器和控制器, 确保拟态组件的冗余性、异构性和拟态界面的选取等, 并根据拟态云虚拟机运行状态和安全策略进行动态调度和清洗。拟态虚拟机、容器和存储单元对外呈现为正常的计算、存储组件, 基于拟态虚拟机、容器和存储单元构建的应用, 确保虚拟机、存储存在漏洞和后门的情况下计算环境的安全可信。

5 结束语

本文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思路的基础上, 探讨了拟态防御技术在天地网络架构、关键信息系统中的应用设想, 提出具备内生安全的天地一体化网络安全防护体系架构设计, 并以拟态地面节点网络路由器和拟态地面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内生安全的天地一体化网络安全防护体系建设提供借鉴。

参考文献:

- [1] 孙晨华. 天基传输网络和天地一体化信息网络发展现状与问题思考[J]. 无线电工程, 2017, 47(1): 1-6.
SUN C H. Research status and problems for space-based transmission network and space-ground integrated information network[J]. Radio Engineering, 2017, 47(1): 1-6.
- [2] 吴曼青, 周彬. 天地一体化信息网络工程立项建议书(初稿)[R]. 中国电子科学研究院, 2015: 1-10.
WU M Q, ZHOU B. Integrated information network project proposal (draft)[R]. China Electronics Research Institute, 2015: 1-10.
- [3] 陆洲, 秦智超, 张平. 天地一体化信息网络系统初步设想[J]. 国际太空, 2016, 7(451): 20-25.
LU Z, QIN Z C, ZHANG P. Initial layout of space-ground integrated information network system[J]. Space International, 2016, 7(451): 20-25.
- [4] 周若飞, 王钢. 论天地一体化网络的建设与军民融合前景[C]//第三十二届全国通信与信息技术学术年会集, 2017年9月20-22日, 福州, 中国. [出版地不详: 出版者不详], 2017: 1-6.
ZHOU R F, WANG G. On the construction of space-ground integrated information network and prospects for the integration of military and civilians[C]// The 32nd National Conference on Communication and Information Technology. September 20-22, 2017, Fuzhou, China. [S.l.: s.n.], 2017: 1-6.
- [5] 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.
LI H, FAN X X, BI J N, et al. Analysis of security technologies in integrated space-air-ground networks[J]. Journal of China Academy of Electronics and Information Technology, 2014, 9(6): 592-597.
- [6] 胡圣波, 孟新, 蒋立正. 天地一体化信息网络空间战主动自防御支持技术[J]. 贵州科学, 2011, 29(1): 59-62.
HU S B, MENG X, JIANG L Z. Supporting techniques of proactive self-defense for cyberspace war with integrated space-ground network system[J]. Guizhou Science, 2011, 29(1): 59-62.
- [7] 鲁瀚. 军民融合无线网络安全体系建设思路[C]//第三十二届全国通信与信息技术学术年会论文集, 2017年9月20-22日, 福州, 中国. [出版地不详: 出版者不详], 2017: 333-337.
LU H. Construction ideas of military and civilian integration of wireless network security system[C]//The 32nd National Conference on Communication and Information Technology. September 20-22, 2017, Fuzhou, China. [S.l.: s.n.], 2017: 333-337.
- [8] 吴曼青, 吴巍, 周彬, 等. 天地一体化信息网络总体架构设想[J]. 卫星与网络, 2016(3): 30-36.
WU M Q, WU W, ZHOU B, et al. Overall framework design of space-ground integrated information network[J]. Satellite & Network, 2016(3): 30-36.
- [9] 李风华, 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[J]. 通信学报, 2016, 37(11): 156-168.
LI F H, YIN L H, WU W, et al. Research status and development trends of security assurance for space-ground integration information network[J]. Journal on Communications, 2016, 37(11): 156-168.
- [10] 闫大鹏, 赵军, 黄小红, 等. 基于天地一体化信息网络的安全防护系统建模及可靠性分析[C]//天地一体化信息网络高峰论坛, 2013年9月24日, 北京, 中国. [出版地不详: 出版者不详], 2013.

- YAN D P, ZHAO J, HUANG X H, et al. Security defense system modeling and reliability analysis based on space-ground integrated information network[C]//Global Integration Of Information Network Summit Forum., September 24, Beijing, China.[S.l.: s.n.], 2013.
- [11] 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[J]. 网络与信息安全学报, 2016, 2(8): 39-47.
- QIN Z C, ZHANG P, FAN X X, et al. Design of security verification platform for the integrated space-ground network[J]. Chinese Journal of Network and Information Security, 2016, 2(8): 39-47.
- [12] NASA. NASA space communications and navigation architecture recommendations for 2005-2030[R]. 2006: 1-50.
- [13] LOVELLY T M, BRYAN D. A framework to analyze processor architectures for next- generation on-board space computing[C]//IEEE Aerospace Conference, March 1-8, 2014, Big Sky, USA. New Jersey: IEEE Press, 2014: 1-10.
- [14] 方滨兴, 殷丽华. 关于信息安全定义的研究[J]. 信息安全学报, 2008(1): 8-10.
- FANG B X, YIN L H. Research on the definition of information security[J]. Netinfo Security, 2008(1): 8-10.
- [15] 邬江兴. 拟态计算与拟态安全防护的原意和愿景[J]. 电信科学, 2014, 30(7): 2-7.
- WU J X. Meaning and vision of mimic computing and mimic security defense[J]. Telecommunications Science, 2014, 30(7): 2-7.
- [16] 邬江兴. 网络空间拟态防御研究[J]. 信息安全学报, 2016, 1(4): 1-10.
- WU J X. Research on cyber mimic defense[J]. Journal of Cyber Security, 2016, 1(4): 1-10.
- [17] 国家数字交换系统工程技术研究中心. 路由器拟态防御原理

验证系统[R]. 2015.

National Digital Switching System Engineering & Technological R&D Center. Router mimicry defense principle verification system[R]. 2015.

[作者简介]



季新生 (1968-), 男, 国家数字交换系统工程技术研究中心教授、博士生导师, 主要研究方向为无线移动通信技术、信息安全、新型网络体系结构。



梁浩 (1987-), 男, 博士, 国家数字交换系统工程技术研究中心助理研究员, 主要研究方向为网络空间安全、主动防御技术。



扈红超 (1982-), 男, 博士, 国家数字交换系统工程技术研究中心副研究员, 主要研究方向为网络空间安全、主动防御技术。