

天地一体化内生安全多标识网络体系

韦国华, 李 挥, 白永杰, 李更新, 邢凯轩

(北京大学深圳研究生院, 广东 深圳 518055)

摘 要: 深入分析一种适用于天地一体化环境的新型网络体系——天地一体化多标识网络体系, 阐述该网络体系的基础理论、天地一体化联合路由、标识管理系统和内生安全机制, 总结天地一体化多标识网络的原型实验进展, 并分析其相对于TCP/IP网络体系的优势。

关键词: 多标识网络体系; 天地一体化信息网络; 区块链; 内生安全; 原型系统

中图分类号: TN393

文献标识码: A

doi: 10.11959/j.issn.2096-8930.20200209

Space-Terrestrial Integrated Multi-Identifier Network with Endogenous Security

WEI Guohua, LI Hui, BAI Yongjie, LI Gengxin, XING Kaixuan

Shenzhen Graduate School, Peking University, Shenzhen 518055, China

Abstract: A novel network architecture, named space-terrestrial integrated multi-identifier network (STI-MIN) was proposed, which was suitable for the environment of space-terrestrial integrated situation. In the following passage, the fundamental theory, Space-Terrestrial integrated routing strategy, identifier management system and endogenous security mechanism of STI-MIN were depicted. Then prototype experiment progress was summarized and the merit of STI-MIN by comparing with traditional network was analyzed.

Keywords: multi-identifier network, space-integrated-ground information network, blockchain, endogenous security, prototype system

1 引言

近年来, 地面通信系统飞速发展, 但其服务质量受到地表形态和自然灾害等因素的限制。不受时间、地点、环境限制的卫星通信逐渐引起了人们的关注, 并形成了联合天基网络、空基网络和地基网络3层异构的天地一体化信息网络, 提供高容量无缝覆盖的通信服务^[1]。天地一体化信息网络跨陆、海、空、天的多层级建设以及天基网络的特殊性导致其具有卫星节点暴露、信道开放、异构网络互联、拓扑高度动态变化、传输高时延、时延方差大及星上处理能力受限等特点, 面临诸多安全挑战。

依靠目前主流的TCP/IP网络体系来构建天地一体化信息网络在服务质量、安全性、移动性上天生不足^[2]。因

此, 全球先进国家都开始研究独立于IP的新型高安全性的天地一体化信息网络体系。目前科技界的共识是, 天地一体化信息网络应当安全可信、可控可控, 支持包含身份、内容、服务等多种标识。天地一体化的多标识体系是人类共同拥有的网络空间, 必须由各国多边共管、共治、共享。

2 天地一体化多标识网络总体架构

2.1 天地一体化多标识网络体系基础理论

单一通信语义的网络层无法满足天地一体化信息网络中丰富的通信情景。新型网络通信需求和服务需求的涌现对IP网络“细腰”结构构成巨大的压力。IP无法适应深空网络大时延、间歇式连接、非对称链路和高信噪比的特

点,因而难以构建基于IP的空间网络环境。

本文提出符合空间组网需求的天地一体化多标识网络体系架构(Space-Terrestrial Integrated Multi-Identifier Network, STI-MIN),该网络体系的基本原则包括以下4点。

共管共治原则:以基于投票的联盟链构造网络管理面多标识系统,构建包括身份、内容、北斗地空、IP等多标识平行共存的网络层,让各国共管并获得除IP外的标识空间主权。

内生安全原则:天地一体化多标识网络通过多标识管理系统将个人、组织和设备所有者的真实身份信息与网络通信标识绑定,要求所有网络分组都携带发出者签名,且至少带有首跳转发路由器的签名,以支持所有网络分组可溯源。同时引入标识自认证、可信计算和人工智能威胁感知等技术,提升网络体系内生的安全强度。

多种标识共存原则:将网络分组划分成不同的类型,携带不同的标识。通过不同的网络标识表达不同的通信语义(推送、拉取、网内缓存等),扩展多标识网络层功能,并通过网络层服务接口为网络上层应用提供各种网络层通信服务。

兼容与演进原则:多标识网络体系通过隧道技术支持与IP网络的相互通信,以实现网络渐进部署。对网络运营者开放标识扩展的接口,支持标识扩展和未来网络层功能创新。

多标识网络提出以上几点设计原则,让多标识网络层更适应空天地网络一体化组网的特点。这些特点包括移动性、轻量级、大时延、间歇式连接、非对称链路、安全性要求高和高信噪比等。

2.2 基于双曲模型的天地一体化协同路由

为了解决路由器资源受限以及新型网络标识转发表规模庞大的问题,针对地基网络设计基于双曲距离的贪婪路由策略,针对具有星间链路的天基网络设计轻量级的基于时延的分布式自适应卫星路由算法,针对不同的应用场景设计不同的路由方案和转发策略。

天地一体化多标识网络路由模型如图1所示。

基于双曲模型的天地一体化协同路由方案将网络拓扑嵌入双曲空间中,计算出映射后节点的双曲坐标^[4]。路由时采用贪婪策略,依赖很少的路由信息,当前节点仅需计算每个邻居节点和目的地节点之间的双曲距离,并优先选择距离最小者进行转发,可以有效解决转发表规模指数膨胀问题。由于卫星的高速运动、星上存储空间以及运算能力不足的影响,采用基于时延的概率路由在一定程度上可以减少数据包传输的时延,降低网络出现拥塞的可能性。基于天基网络和地基网络在可操作性与

性能之间存在的差异,根据不同的应用场景灵活设计天-天、天-地、地-地之间的协同路由方案,优化转发策略并提高路由成功率。

天地一体化多标识网络的标识空间采用层级化的思想,将网络域划分为 k 个层级,并将各层级域的网络拓扑分别映射到双曲空间,此时每个域节点的边界路由均被分配了一个双曲坐标作为该域节点的双曲标识。每个域节点本地记录自身的双曲标识和一定数量(比如20~50个)同等级邻居域节点的双曲标识。假设网络标识域划分为 k 个层级, k 由实际需求与拓扑稳定性确定,每级路由器能支持 N 个网络标识,依次对每一层级的网络拓扑做双曲嵌入,得到各个层级节点的双曲坐标集合 (R_i, Θ_i) ,其中 $i=1,2,\dots,k$ 。划分后的网络支持 N^k 数量级的网络标识空间。

以三级网络域为例,一级域包含多个域节点,把一级域节点组成的网络拓扑嵌入双曲空间,得到一级网络域的双曲坐标集合 (R_1, Θ_1) ,将其作为节点的双曲标识指引一级域间路由;再将一级域划分为多个二级域,把二级域节点形成的网络拓扑嵌入双曲空间,得到二级网络域的双曲坐标集合 (R_2, Θ_2) ,将其作为节点的双曲标识指引二级域间路由,考虑到其归属的一级域,则二级域节点完整的双曲标识为 $(R_1, \Theta_1):(R_2, \Theta_2)$;以此类推,再将二级域划分为多个三级域,三级域内包括各个用户节点。

基于时延的分布式自适应卫星路由算法,适用于具有星间链路的天基网络,算法通过计算每个候选下一跳的传播时延和队列时延,得到选择下一跳的概率,然后按照概率转发数据包。另外,在天基网络负载低、状态良好的情况下,天基网络设备之间的数据传输优先通过天基网络进行;当天基网络出现负载过高、链路状态失效的情况,数据会被下发到信关站,由地基网络进行中继。天地一体化多标识管理系统架构如图2所示。

算法要求每个卫星建立接入信息表(Access Information Table, AIT)和状态信息表(Status Information Table, SIT)。在接入信息表中,表项 AIT_u 记录与当前卫星连接的用户和信关站信息,表项 AIT_u 、 AIT_d 、 AIT_l 和 AIT_r 分别记录其上、下、左、右方向卫星连接的用户和信关站信息。在状态信息表中,表项 SIT_u 、 SIT_d 、 SIT_l 和 SIT_r 分别记录当前卫星上、下、左、右方向卫星的链路状态、缓冲队列数据包的大小、缓冲队列负载和信道衰减系数。

2.3 共管共治天地一体化多标识管理解析系统

在天地一体化多标识网络的管理面基于层级化的联盟链技术,设计去中心化的身份、证书和网络标识管理解析方案。每层级联盟链采用投票共识算法(PPoV)。该算法核心在于分离投票权与记账权,记账节点团队根

据联盟节点的投票结果进行去中心化仲裁。

PPoV共识为区块链节点设置3类节点身份：联盟、记账或领导节点。联盟节点负责对待生成的区块和潜在记账节点进行投票。基于“少数服从多数”的原则，投票结果被作为系统生成有效区块和记账节点竞选成功的合法证明。

通过应用并行技术促使记账节点团队全力联合工作，PPoV共识在理论上达到每秒数十万级事务处理性能，能够支持成百上千个联盟节点共同参与管理。基于PPoV共识和可扩展拓扑的多标识管理系统能够同时满足强一致性、高可用性及分区容忍性三性。

通过对网络标识的分层级管理，各组织或机构拥有独立的标识管理解析权，同时基于区块链投票共识原理，实现各组织对顶层网络标识共管共治的最终目标。

3 天地一体化多标识网络内生安全机制

3.1 面向联盟链的可信计算主动免疫安全技术

多标识管理系统中的区块链节点使用TCM（可信密码模块）芯片用作密钥管理，负责生成联盟区块链中所用到的公私钥。私钥保存至芯片中不可泄露，公钥可以导出以标识节点身份，由此保证了系统的安全性。同

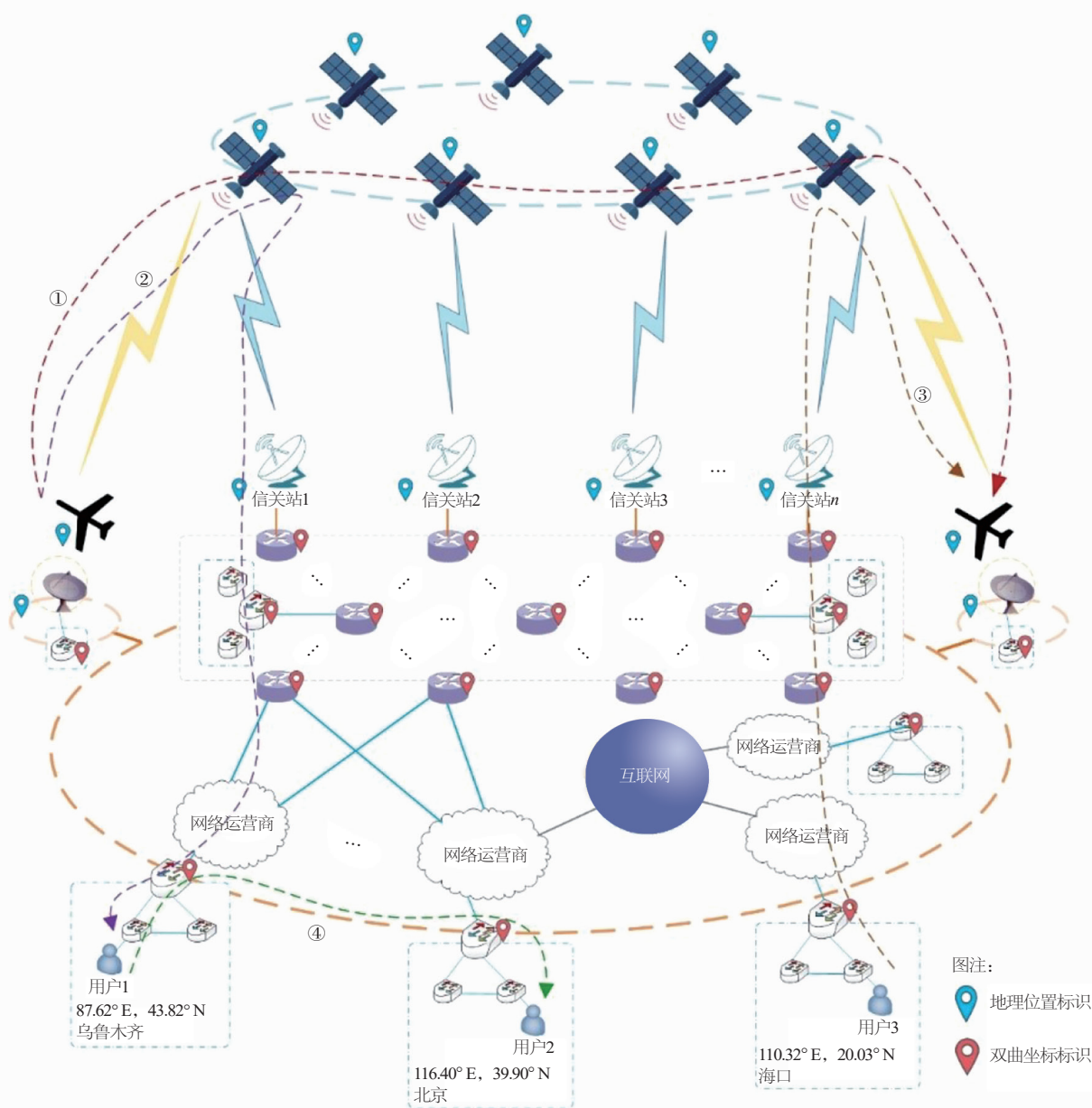


图1 天地一体化多标识网络路由模型

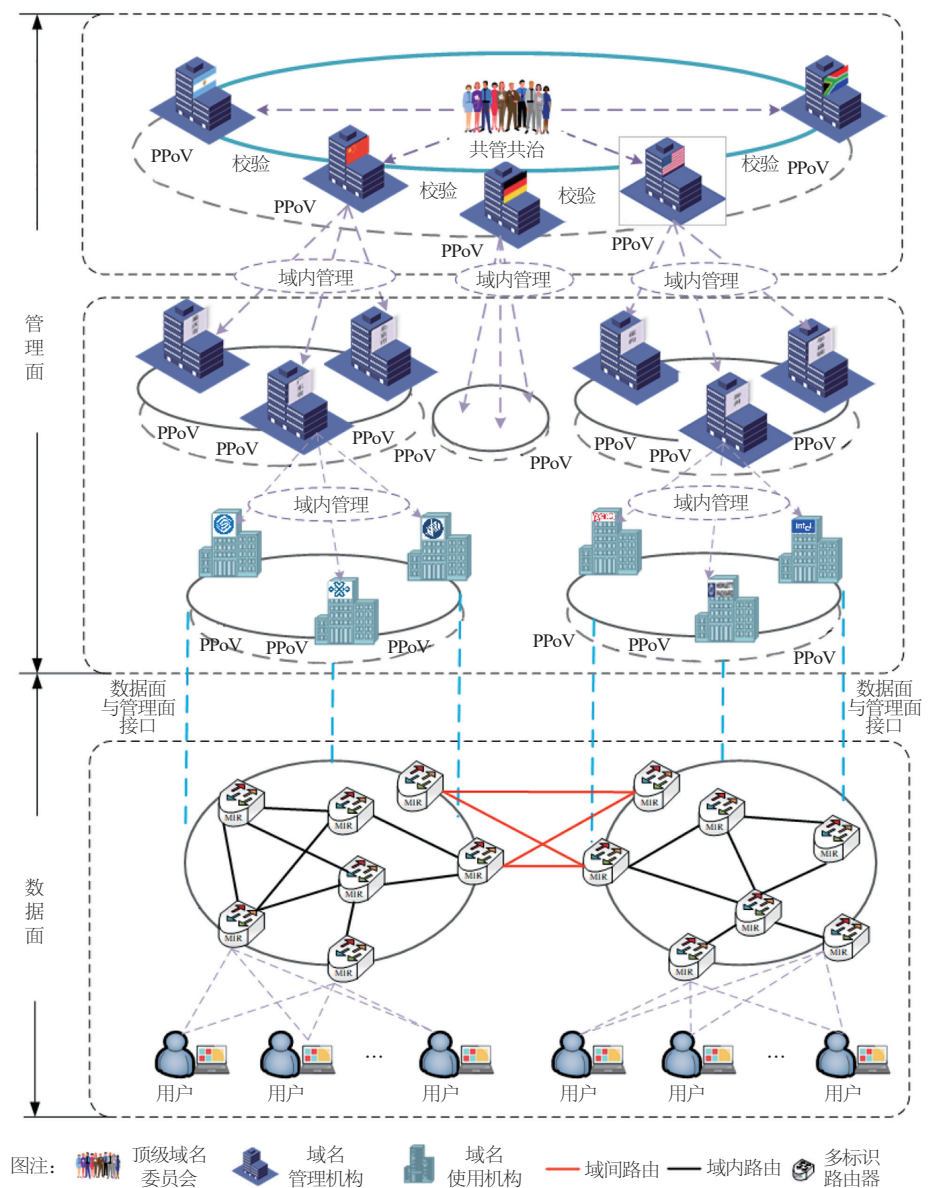


图2 天地一体化多标识管理系统架构

时，对节点产生的各种数据（如区块、交易等）使用TCM提供的签名算法进行签名，保证了数据的完整性和不可篡改性。

采用可信计算的扩展信任传递过程为：TCM→BIOS→OS Loader→OS→MIS，如图3所示。各阶段的完整性基准值由信任根提供的密码接口计算，并存储在TPCM（可信平台控制模块）安全区域中。当进行认证时，后一级模块负责计算对比前一级模块的完整性度量值，以判断其是否遭受篡改。通过一级认证一级，达到一级信任一级的目的，直至将这种信任扩展到整个系统。信任

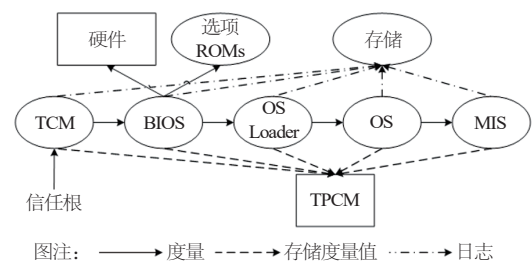


图3 联盟链节点信任链模型

链是在联盟链节点启动时进行的一次完整性度量。

同时,利用可信计算3.0的主动免疫技术进行各个节点的监控,在联盟链节点以外单独构建监控可信管理中心,监控在管的各节点健康情况,对各节点的安全策略和配置进行统一管理^[5]。在系统运行期间,对联盟链节点按需进行动态的主动免疫可信管理。

联盟链可信管理系统架构如图4所示。每个域内包含了多个区块链节点终端,二级可信管理中心负责与某个域内的所有可信终端(Windows、Linux、Android等)进行统一管理,包括终端注册注销、资源监测、终端身份证书管理、策略管理、审计分析等。可信管理中心节点内集成了安全策略模板化管理模块(增加、删除、下发),包括静态度量策略、动态度量策略、自主访问控制策略、强制访问控制策略、外设控制等。一级可信管理中心负责与所有二级可信管理中心节点交互,收集区块链节点终端的安全信息,并对二级可信管理中心进行安全策略管理,以实现不同安全等级和不同敏感度的系统和文件进行分等级保护的管理。

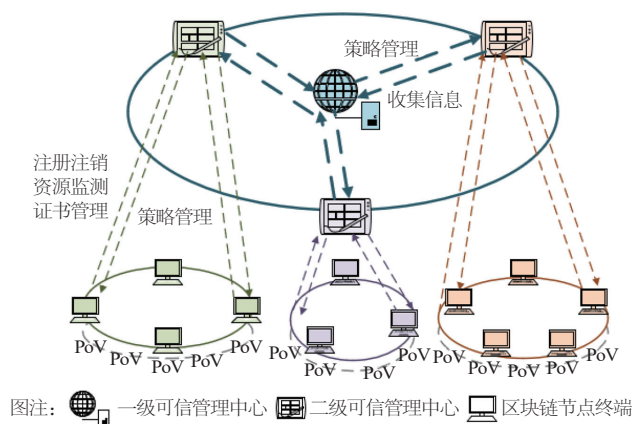


图4 联盟链可信管理系统架构

3.2 信任内嵌的身份认证机制

针对天地一体化信息网络多种入网实体,天地一体化多标识网络提出统一的用户身份自认证机制,认证过程中不依赖第三方可信机构,构造在保证路由可用的情况下,通信过程中对每个数据包的签名方法,保证用户信息的机密性和用户行为的可追溯性。

天地一体化多标识网络的基础标识被称为身份标识,身份标识是网络用户的公钥的哈希值。假设一个主机的身份标识为 X ,它对另一个主机的身份标识 Y 进行验证的过程是一个双边质询响应过程:

(1) X 可以通过给 Y 发送一个随机数 $[n]$ 来作为一个质询;

(2) Y 应该应答 $[K+, K-(n)]$,其中 $K+$ 是 Y 的公钥,而 $K-(n)$ 是 $K+$ 用对应的私钥加密 n 后得到的数;

(3) X 收到应答消息后,先检验 $H(K+)=Y$,其中 H 是哈希函数,然后再检验 $K+(K-(n))=n$ 。如果两个检验都通过了,那 Y 就通过了 X 的检验。并且 X 拥有了 Y 的公钥。

当两个不同域内的用户进行通信时,本文提出了一种基于HMAC的轻量级域标识认证方案。具体过程如下。

(1) 首先每一个域路由器都保存与其他各个域路由器做认证加密的对称密钥,并且域路由器之间的密钥相互独立,即一个域路由器无法得知其他任意两个域路由器之间的密钥,该密钥存储于可信计算芯片中,并且进行定期更新。

(2) 若Alice给Bob发送跨域网络分组时,该网络分组会从域A至域B,当域A的域间路由器得知该网络分组需要跨域时,则给该网络分组加上域A的域间路由器的身份标识“/A”及时间戳信息,并且使用域A与域B共享的密钥将当前网络分组进行加密,生成密文 s ,附加在网络分组后面发送给域B的域间路由器。加密算法使用HMAC-SHA1。

(3) 当域路由器B要对用户Alice的请求做域标识认证时,会使用域A与域B共享的对称密钥加密域A发来的消息,查看加密后的 s' 是否和 s 相等。这样能够防止域标识的恶意伪造。

3.3 多标识网络智能威胁感知

安全感知系统利用AI分类方法,同时感知IP和多标识网络的威胁行为,它可以直接部署在关键的多标识路由器中^[6]。安全感知系统采用了Endsley的安全感知模型,即将态势感知分为感知、理解和预测3个层次。感知包含对网络环境中重要组成要素的状态、属性及动态等信息,以及将其归类整理的过程;理解则是对这些重要组成要素的信息的融合与解读,不仅是对单个分析对象的判断分析,还包括对多个关联对象的整合梳理。同时,理解是随着态势的变化而不断更新演变的,不断将新的信息融合进来形成新的理解。在了解态势要素的状态和变化的基础上,本文对态势中各要素即将呈现的状态和变化进行预测。

4 实验与评估

4.1 天地一体化多标识网络测试床建设

2020年4月,北京大学深圳研究生院与中国卫星通信集团股份有限公司(以下简称中国卫通)基于天地一体化多标识网络架构展开测试,目前已通过原理测试,验证了基于天地一体化多标识网络的可行性。该原型网络如图5所示,测验网络部署了几个有代表性的小型多标识

子网, 包括喀什、成都与北京3个信关站的MIN-IDC子网, 以及北京大学深圳研究生院、香港中文大学、澳门科技大学等几个MIN-IDC子网, 并通过中星十六卫星将多个子网连接起来。子网间通过IP隧道通信, 而子网内部则使用链路层协议直接传输多标识网络分组。

4.2 两级多标识管理系统部署测试

基于天地一体化的多标识网络试验床, 这个在每个单位的内部多标识网络中选择一台服务器作为区块链节点, 用于组成多标识管理系统的一级链。一级链包括北京大学深圳研究生院、中国卫通、澳门科技大学、香港中文大学、香港科技大学、华南理工大学、金山云和中国联通共8个一级节点。

在中国卫通私有网络内部, 基于中星十六卫星通信部署中国卫通二级标识管理链。中国卫通二级管理系统中共包含5个二级节点, 用于管理天空网络通信标识。实验表明二级管理系统能正常运行, 且多标识管理系统在层级扩展上有很大的灵活性。

4.3 天地一体化多标识网络基础通信测试

将文件放在中国卫通机房的wt3节点上, 并在北京大学深圳研究生院node11节点上使用简单的多标识网络传输程序, 进行文件传输下载实验。测试网络拓扑以及传输结果如图6所示。

传输速率平均为1.2 Mbit/s, 而传输链路的总带宽为20 Mbit/s。影响下载速度的主要原因是该传输程序使用固定的传输窗口来发送多标识网络数据分组, 且卫星通信时延较大, 可见充分利用带宽需要设计良好的传输控制机制(这部分本文暂不深入讨论)。

4.4 天地一体化多标识网络攻击实验

按照经典攻击链和攻击方式, 在中国卫通多标识网络子域内部选择具有代表性的两个主机进行攻击实验, 并构建两个IP网络下的主机做对比实验。本文分别在IP-IP、IP-MIN和MIN-MIN 3种情况下进行了3个方面的攻击测试, 包括目标侦察、攻击植入和内网ARP攻击。结果表明, 即使在局部部署MIN网络(IP-MIN)的情况下, 也能提升网络的安全性。

4.5 多标识智能态势感知系统

将安全感知系统部署在多标识网络与IP网络的交界路由器上, 分别在IP和多标识网络中向边界路由器发起传统的IP攻击和基于新型网络协议的攻击。IP攻击主要包括DDoS攻击、主机端口扫描和漏洞扫描等, 而在多标识网络下主要进行的攻击包括DDoS攻击、标识冒用攻击和新型木马注入攻击等。

经测试, 感知系统检测新型和传统攻击的准确率较

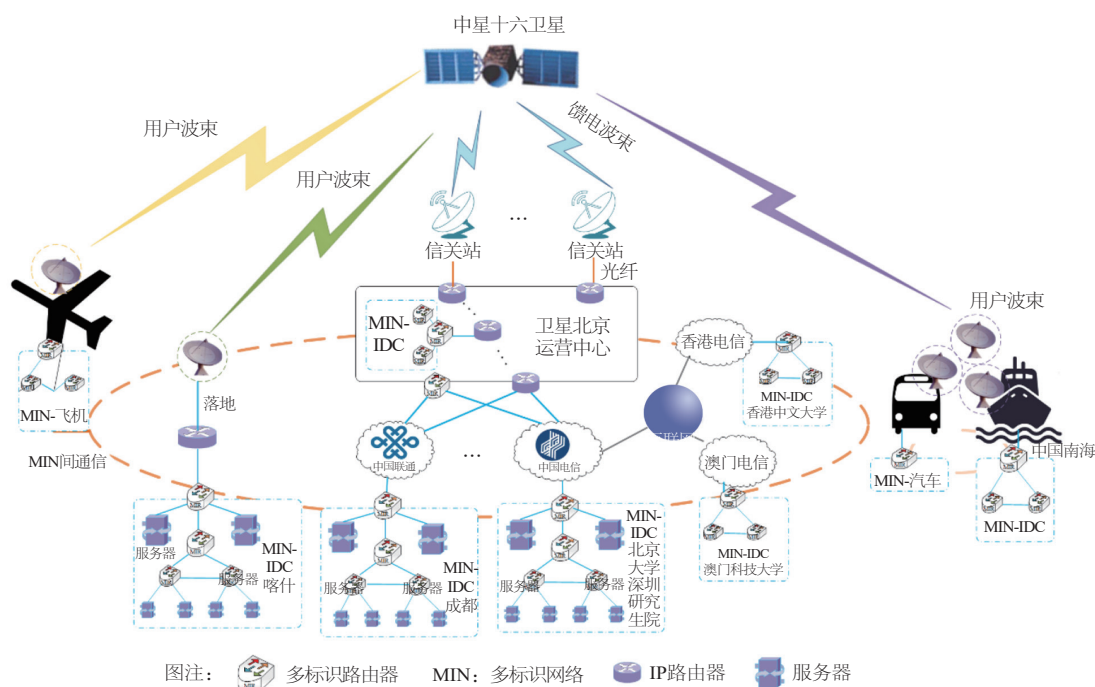


图5 天地一体化多标识网络试验床

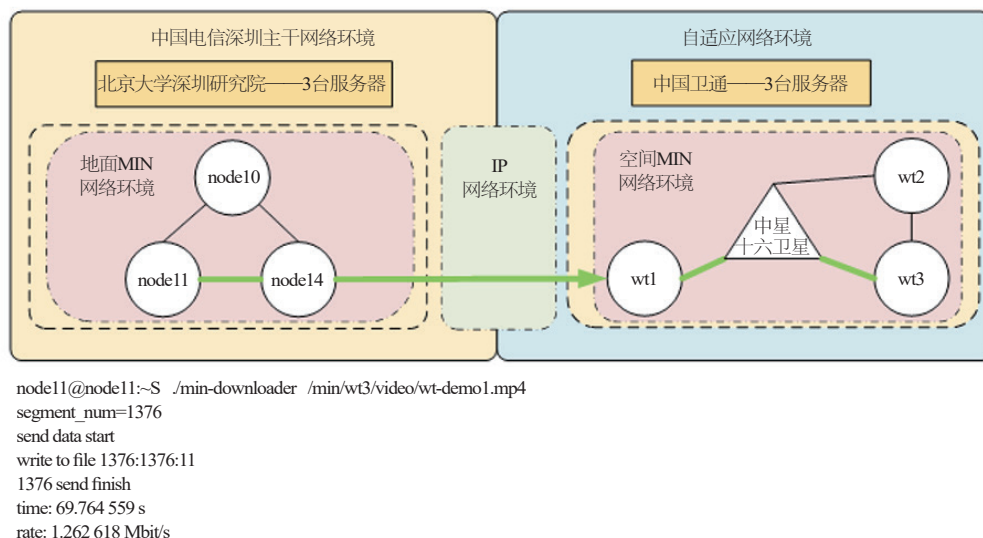


图6 基础通信网络测试拓扑以及传输结果

高，并且感知系统能正常通过AI技术对当前安全态势做出合理的评估。

4.6 分析与比较

天地一体化多标识网络与IP网络相比，其关键的优势包括以下几点：

(1) 允许多种标识与传输模式共存，使用更适宜的标识满足不同场景，如在地面网络中使用层级化标识，而在空间网络中使用地理空间标识直接寻址；

(2) 内生安全特性，包含上文提到的可信计算、网络分组多重签名、自认证标识和智能威胁感知等技术；

(3) 标识共管共治技术，通过联盟区块链技术实现对标识的投票式管理；

(4) 标识可扩展性，天地一体化多标识网络不再使用固定的标识和通信模式，而是为未来的标识与通信模式扩展预留接口，使得未来网络架构创新的阻力更小。

5 结束语

本文设计了一套更适应天地一体化组网环境的网络体系架构。该网络体系架构在网络层上支持多种传输标识和通信语义，设计了多种内生安全机制，兼容当前IP网络同时支持标识的创新和扩展，利用多层级的联盟区块链来实现网络标识共管共治。天地一体化多标识网络体系原型已在北京大学深圳研究生院、中国卫星、澳门科技大学、香港中文大学、香港科技大学、华南理工大学、北京金山云网络技术有限公司（简称金山云）和中

国联通组成的现IP网络和天空网络组合环境上测试了天地一体化多标识网络的基本功能，测试结果表明了天地一体化多标识网在许多方面优于IP网络。

天地一体化多标识网络在基础测试床上通过了基本的功能测试，但其中涵盖的各类技术还有待深入研究与完善。天地一体化多标识网络的未来工作重心在于搭建更加接近物理环境的测试床，在动态的拓扑环境中对天地一体化路由器方案进行功能与性能测试，设计和实现高性能可扩展的标识寻址转发策略，设计和实现针对多种标识和多种传输语义的传输控制协议等。

鸣谢：在此衷心感谢参与天地一体化多标识网络原型系统实现的各合作单位，感谢中国卫通、澳门科技大学、香港中文大学、香港科技大学、华南理工大学、金山云和中国联通等单位对本实验的大力支持。

参考文献：

- [1] 李贺武, 吴茜, 徐恪, 等. 天地一体化信息网络研究进展与趋势[J]. 科技导报, 2016, 34(14):95-106.
LI H W, WU Q, XU K, et al. Progress and tendency of space and earth integrated network[J]. Science & Technology Review, 2016, 34(14):95-106.
- [2] 李挥, 鄢江兴, 邢凯轩, 等. 多边共管的多模态网络标识域名生成管理解析原型系统[J]. 中国科学:信息科学, 2019(9):1186-1204.
LI H, WU J X, XING K X, et al. Prototype and testing report of

- a multi-identifier system for reconfigurable network architecture under co-governing[J]. SCIENTIA SINICA Informationis, 2019(9):1186-1204.
- [3] LI H, WU J, YANG X, et al. MIN: Co-governing multi-identifier network architecture and its prototype on operator's network[J]. IEEE Access, 2020, 8:36569-36581.
- [4] LV S, LI H, WU J, et al. Routing strategy of integrated satellite-terrestrial network based on hyperbolic geometry[J]. IEEE Access, 2020(99):1-1.
- [5] 沈昌祥. 用主动免疫可信计算3.0筑牢网络安全防线营造清朗的网络空间[J].信息安全研究,2018,4(4):282-302.
- SHEN C X. To create a positive cyberspace by safeguarding network security with active immune trusted computing 3.0[J]. Journal of Information Security Research, 2018,4(4):282-302.
- [6] FRANK J. Artificial intelligence and intrusion detection: Current and future directions[J]. Computers & Security, 1995, 14(1):31-31.

[作者简介]



韦国华（1995-），男，北京大学深圳研究生院硕士生，主要研究方向为未来网络体系架构、新一代网络通信技术等。



李挥（1964-），男，北京大学深圳研究生院教授、博士生导师，鹏城实验室双聘教授，国家重大科技基础设施——未来网络CENI北大实验室主任，深圳市信息论与未来网络体系重点实验室主任，主要研究方向为网络空间安全与区块链技术、人工智能与未来网络体系、分布式存储编码理论及系统、智能大数据分析 & 数据标准等。



白永杰（1995-），男，北京大学深圳研究生院硕士生，主要研究方向为区块链技术、网络路由算法等。



李更新（1997-），男，北京大学深圳研究生院硕士生，主要研究方向为未来网络安全协议、人工智能安全技术等。



邢凯轩（1994-），男，北京大学深圳研究生院助理研究员，主要研究方向为未来网络体系架构、新一代网络通信技术等。