

通信与安全一体化的天地异构融合网络体系架构

章小宁¹, 朱立东²

(1.电子科技大学信息与通信工程学院, 四川 成都, 611731 ;

2.电子科技大学通信抗干扰技术国家级重点实验室, 四川 成都, 611731)

摘要: 为了实现天基信息网与高铁、船舶、民航等地面专网的深度融合, 提出采用标识映射机制构建通信与安全一体化的天地异构融合网络总体架构模型, 包括天地异构融合网络服务层、业务层、路由层以及接入层4层架构以及服务标识、业务标识、路由标识、接入标识、主机标识5类标识。通过高效的标识映射, 在不改变天基信息网与地面各类专网内部组网机制与通信协议的基础上, 满足天基信息网与地面专网通信与安全一体化的要求, 实现天基信息网与各类地面专网的高效融合、安全可靠与资源整合。

关键词: 天地一体化信息网络; 标识映射; 路由; 安全

中图分类号: TN393

文献标识码: A

doi: 10.11959/j.issn.2096-8930.20200202

Communication and Security Integrated Space-Earth Heterogeneous Network Architecture

ZHANG Xiaoning¹, ZHU Lidong²

1.School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

2. National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China

Abstract: To achieve the integration of space information networks and high-speed rail, ship and civil aviation private communication networks, this article proposes to leverage the mechanism of identifier and locator separation to construct the communication and security integrated space-earth heterogeneous network architecture. The proposed network architecture included four network layers (i.e., space-earth heterogeneous network service layer, space-earth heterogeneous network traffic layer, space-earth heterogeneous network routing layer and space-earth heterogeneous network access layer) and five network identifiers (i.e., service identifier, traffic identifier, routing identifier, access identifier and host identifier). With the method of efficient network identifier mapping, the communication and security integrated requirement for space information networks and ground private communication networks could be guaranteed.

Keywords: space-integrated-ground information network, identifier mapping, routing, security

1 引言

天地一体化信息网络^[1-3]贯穿海洋、太空、网络空间, 是信息时代的战略性公共信息基础设施, 能有效地弥补传统地面通信网络的不足, 提供全球/区域覆盖能力, 受地理环境影响较小。天地一体化信息网络采用

“天网地网”体系架构, 以地面网络为依托, 以天基信息网为拓展, 由天基骨干网、天基接入网、地基节点网互联并与地面互联网、移动通信网等地面网络融合形成“一张网”, 天空地多层次协同实现全球覆盖、随遇接入的网络信息服务能力^[4-5]。

近年来, 随着高铁、船舶、民航等地面通信专网

收稿日期: 2020-10-09; 修回日期: 2020-11-10

基金项目: 国家自然科学基金资助项目 (No.61671124)

Foundation Item: The National Natural Science Foundation of China (No.61671124)

的迅速发展以及行业信息化进程的不断推进,天地一体化信息网络正朝着陆地、海洋、空中、太空全域全时组网的发展趋势快速发展。这就要求天地一体化信息网络能在任何时间、任何地点以高效可靠的方式提供信息通信服务,以满足全球范围内陆地、海洋、空中、太空各类用户互联互通的要求。然而,现有的天基信息网与高铁、船舶、民航等地面专网均相对独立,且具有异质异构的组网机制和通信协议,在网络的移动性、可扩展性、安全性、业务QoS等方面存在明显的差异。这将导致天基信息网无法直接实现与各类地面专网的高效互联,难以实现跨越多个异构网络的信息共享和资源整合,形成信息“孤岛”并影响专网用户的服务质量^[6]。当前天基信息网与高铁、船舶、民航等各类地面专网之间相对孤立的状况,无法从根本上满足信息化时代下社会、经济、科技、国防等方面发展的重大需求。

本文针对天基信息网与地面专网的动态异构特性,提出基于标识映射机制^[7-10]构建通信与安全一体化的天地异构融合网络,实现陆地、海洋、空中各类用户应用的互联互通、信息共享、安全可靠、按需服务。在此基础上提出天地异构网络组网机制,在不改变天基信息网与地面各类专网内部组网机制与通信协议的基础上,实现天地异构网络的深度融合。

2 天地异构网络的总体架构

为构建通信与安全一体化的天地异构融合网络,提出如图1所示的天地异构融合网络架构。该3层结构自下而上分别是异构网络资源层、一体化协同组网层以及智慧网络控制层。作为底层的物理网络资源,异构网络资源层不仅包含各类专用通信网络以及具有通用业务能力的天基信息通信网络,还包含能够承载通用数据传输业务的互联网、3G、4G、5G、Wi-Fi等移动通信网以及地面各类专网。

为了实现多种异构网络的融合以及全局网络资源的分配,在异构网络资源层之上构建一体化协同组网层。面对各类专网,一体化协同组网层利用网关对专网进行适配从而将其接入天基信息网,同时对专网业务进行细粒度的特征感知,结合安全认证技术确保网络接入的安全和业务可控。面对具有周期性变化特征的天基信息网,一体化协同组网层结合网络感知技术和备份技术,构建能够抗毁、自愈,实现自驱动(Self-driving)优化的天基地基网络组网技术。

基于一体化组网层提供的网络资源抽象,智慧网络控制层将构建安全的网络资源切片,利用增强学习实现资源的智慧分配,为各类业务提供差异化、细粒度的数

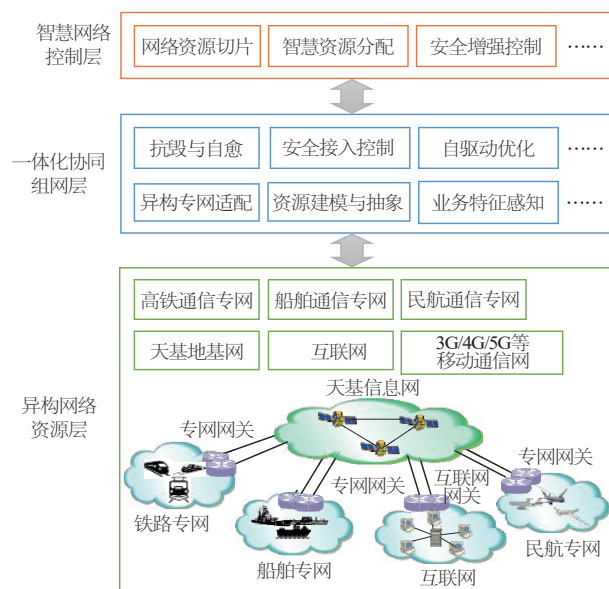


图1 天地异构融合网络架构

据传输服务。与此同时,网络控制层还将从全局统一安全管理、威胁感知和预警的角度,将网络安全所需的网络功能(Network Function)放置到不同的接入网关中以实现严格的安全接入、安全切换、入侵检测、访问控制等,并利用网络功能虚拟化技术实现复杂网络任务的优化配置和安全服务卸载。

3 天地异构融合网络的标识体系与映射机制

本文针对天基信息网与高铁、船舶、民航等专网的动态异构特性,基于标识映射机制提出通信与安全一体化的天地异构融合网络架构,实现异构网络间的深度融合。通信与安全一体化的天地异构融合网络架构,即在同一种网络体系架构内为陆地、海洋、空中等异构专网用户,提供通信与安全一体化的服务。根据上述总体思路,在兼容现有网络协议体系的基础上构建了天地异构融合网络的总体结构模型。该模型可概括为“四层架构、五类标识、四种映射”,如图2所示。

天地异构融合网络接入层包含了高铁、船舶、民航等各类地面异质异构的专网,统一接入天基信息网中。在天地异构融合网络接入层引入主机标识(Host ID, HID)的概念,标识天地异构融合网络中各类地面异构专网中的主机;同时引入接入标识(Access ID, AID)的概念,标识天地异构网络中各类地面专网的网关节点,即地面专网到天基信息网的接入节点,也可以用接入标识标记一个特定的地面专网。通过接入标识(即专网的网关节点),可以实现地面各类异质异构专网在天基信

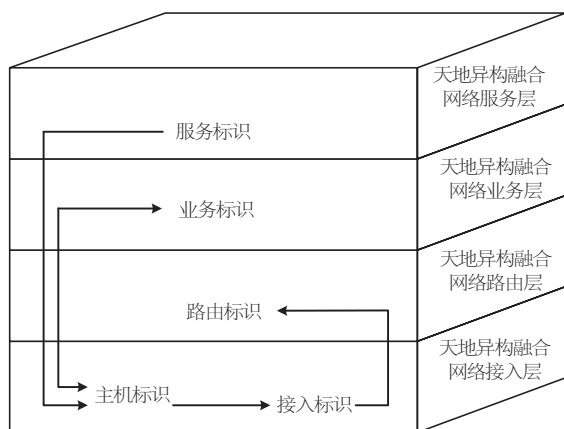


图2 天地异构网络总体结构模型

息网中的统一接入。在现有互联网中，使用IP地址同时代表了端点名和地址。这种方式将端点局限为一个主机；其次，当端点的地址发生变化时，其本身也就发生了变化，虽然端点没变，但由于IP地址的改变，导致了端点名的改变，并且旧的IP地址被重新分配，这样更不利于对端点行为的审核和追踪；第三，只要有IP地址，即地址的信息，恶意者只要获取目的主机的IP地址就可以伪造数据分组对其发起DoS攻击，阻塞其带宽，也可以对整个IP地址空间进行扫描，进行蠕虫传播等，而且所有这些行为都因为源地址伪装而变得难以追踪。因此从严格意义上来说，需要一种可以区分端点和地址的能力，也就是分别对这两者进行命名。使用主机标识来代表端点，使用接入标识来代表端点接入地址。在天地异构融合网络接入层，将建立从主机标识到接入标识的映射，用以说明当前某个主机已经接入某个专网中。

天地异构融合网络路由层包含提供路由能力的天基信息网，主要包括低轨和高轨卫星路由节点，为地面各类接入专网间通信提供路由和寻路能力。在天地异构融合网络路由层引入路由标识（Route ID, RID）的概念，标识天基信息网中的卫星路由节点。在天地异构融合网络中，由于受地面专网和天基卫星节点移动性的影响，接入时需要建立接入标识到路由标识的映射，用以说明当前某一个专网接入天基信息网中某个卫星路由节点上。通过接入标识到路由标识的映射，可以更好地满足天地异构融合网络路由的移动性要求，并能实现天基路由核心系统的屏蔽。

天地异构融合网络业务层描述专网与专网之间、专网与公网之间端到端的业务，通过对主机身份与网络位置的解耦，可以更好地满足高铁、船舶、民航等专网业务在移动性和安全性等方面的要求。在天地异构融合网络业务层中引入业务标识（Traffic ID, TID）的概念，

用于标识从源主机标识到目的主机标识间一个特定的业务，同时在业务标识中加入该业务的QoS字段，便于为后续的网络资源映射提供有效的参考。业务标识可以提供对主机信息的隐藏，并具有对通信双方信息进行校验的能力。在实际通信中网络需要对不同通信业务进行区分才能有效地实现针对流的控制，而主机的传输层才能完成向应用层的数据递交，可以将这种对通信连接的表示抽象为业务标识。在TCP/IP中，五元组（源宿IP地址、协议、源宿端口号）在实质上表明了一个业务。首先，该业务直接与主机所在IP地址进行绑定，因此根据这种显式的业务就可以明确地知晓此数据流是属于哪个端点，从而在流经过的任何网络位置都可以对此主机的行为进行观测。其次，五元组是主机自行生成的，主机可以任意篡改此信息，即此业务标识本身缺乏对主机信息进行校验的能力，也就是说网络通过这种显式的五元组并不能对用户信息进行校验审核。因此，业务标识应该是一种由第三方生成的，能够隐蔽主机信息的隐式的实现方式。本文建立主机标识到业务标识的双向映射，即 $TID=F\{\text{源HID、宿HID、源端口、宿端口、协议类型}\}+QoS\text{字段}$ ，其中函数F是一个可逆的加密函数。

天地异构融合网络服务层描述了陆地、海洋、空中、太空等各类异质异构的网络提供的的数据交付及信息共享服务。在天地异构融合网络服务层中引入了服务标识（Service ID, SID）的概念，标识天地异构融合网络中的特定服务和数据，并且实现服务与位置的解耦。将通信建立主体由面向主机转变为面向服务，实现与服务实际提供者和公共监听端口的隔离。当用户或应用在获取一个服务或者数据的时候，其需要关心的仅仅是这些服务的本身，这个数据是由谁提供的是不需要关心的，但是现有互联网的实现原则违背了这个基本事实。基于DNS的域名系统仅能以主机为主体进行互联网的注册和审核，而没有对服务和数据本身进行审核，这就使得恶意用户可以任意提供非法和虚假的信息。另外一方面，也是更容易被人忽视的一方面，即在互联网上的服务还和公共监听端口进行了绑定，无论服务的内容是什么，所有的HTTP必须都在80端口、Telnet都在23端口，SMTP在25端口上监听，攻击者可以对这些公共端口进行扫描以收集主机的信息，并进行蠕虫传播和DoS攻击，使提供服务的主机完全暴露于恶意攻击者。因此需要引入对服务和数据进行标识的新的命名，称之为服务标识。本文建立服务标识到接入标识的映射，即在天地异构融合网络的映射系统中记录那些主机及端口号，可以提供某一种服务。天地异构融合网络中专网用户可以向映射系统申请特定的服务标识，映射系统查询后返回该服务标识对应的主

机标识以及端口号,可以便于建立通信连接。

4 天地异构融合网络组网原理

本文将从专网与公网间通信以及专网与专网间通信两大场景出发,研究通信与安全一体化的天地异构融合网络组网原理。

首先考虑天基信息网支持专网与公网间通信的场景。公网中的互联网服务提供方将提供某一互联网服务的主机标识及其端口号发送给服务标识映射服务器,并加入相应的服务映射表中。当某个专网主机向公网请求某一互联网服务时,会将该主机标识及其端口号发送到服务标识映射服务器,并等待分配相应的服务。服务标识映射服务器对服务请求方请求的服务进行查找,找到相应的服务标识,同时找到该标识下可用的服务提供方。查找结束后,返回该服务提供方的主机标识及其端口号,进行服务标识解析处理。在服务标识解析处理过程中,采用可逆的加密函数根据服务请求方的主机标识及其端口号、服务提供方的主机标识及其端口以及协议类型,生成加密的业务标识,以达到隐藏通信双方主机标识的目的,具体过程如图3所示。

在图3中,公网中的服务提供方1将其主机标识 HID_1 和端口号12、45提交到服务标识映射服务器上,与服务标识 SID_1 相映射。专网中的服务请求方请求 SID_1 提供服务,同时发送了主机标识 HID_3 和端口号34给服务标识映射服务器。这时服务标识映射服务器对服务标识 SID_1 进行查找,选择主机标识 HID_1 和端口号12为服务请求方提供服务,并根据 $\langle HID_3, HID_1, \text{源端口}34, \text{宿端口}12, \text{协议类型} \rangle$ 的五元组,使用可逆的加密函数 F 生成加密的业务

标识,并将业务标识返还给专网中的服务请求方。

专网与公网间通信场景分组转发过程如图4所示。在图4中,专网中的服务请求方 HID_3 在得到服务标识映射服务器返回的业务标识后,首先将数据分组在专网内部从 HID_3 发送到专网的网关节点 AID_3 ,同时在数据分组中还需携带业务标识 TID 信息(如图4中的步骤①所示)。需要指出的是在源专网内部, HID_3 和 AID_3 作为专网内部路由协议的源地址和宿地址,在不改变专网组网机制和路由协议的基础上实现专网内路由。当数据分组到达源专网的网关节点 AID_3 之后, AID_3 对数据分组中的业务标识字段 TID 进行解密,发现该数据分组的源主机为 HID_3 ,宿主机为 HID_1 (如图4中的步骤②所示)。于是专网的网关节点 AID_3 向映射系统发起查询请求,询问 HID_1 当前对应哪一个 AID ,以及该 AID 对应哪一个 RID (如图4中的步骤③所示)。映射系统收到 AID_3 的查询请求后,通过对映射数据库的查询,发现 HID_1 当前对应 AID_1 ,同时 AID_1 对应 RID_1 (如图4中的步骤④所示)。然后,专网的网关节点 AID_3 向其对应的天基卫星路由节点 RID_3 上传该数据分组,图4中从 AID_3 到 RID_3 这一跳可以采用二层通信的方式完成。在天基信息网内部,该数据分组继续从卫星路由节点 RID_3 发往卫星路由节点 RID_1 ,数据分组内需要携带对应的接入网节点 AID_3 与 AID_1 的信息,以及加密的业务标识 TID 信息(如图4中的步骤⑤所示)。需要指出的是在天基信息网内部, RID_3 和 RID_1 作为天基信息网内路由协议的源地址和宿地址,在不改变天基信息网组网机制和路由协议的基础上实现天基信息网内的路由。天基信息网的卫星路由节点 RID_1 在收到数据分组后,根据其

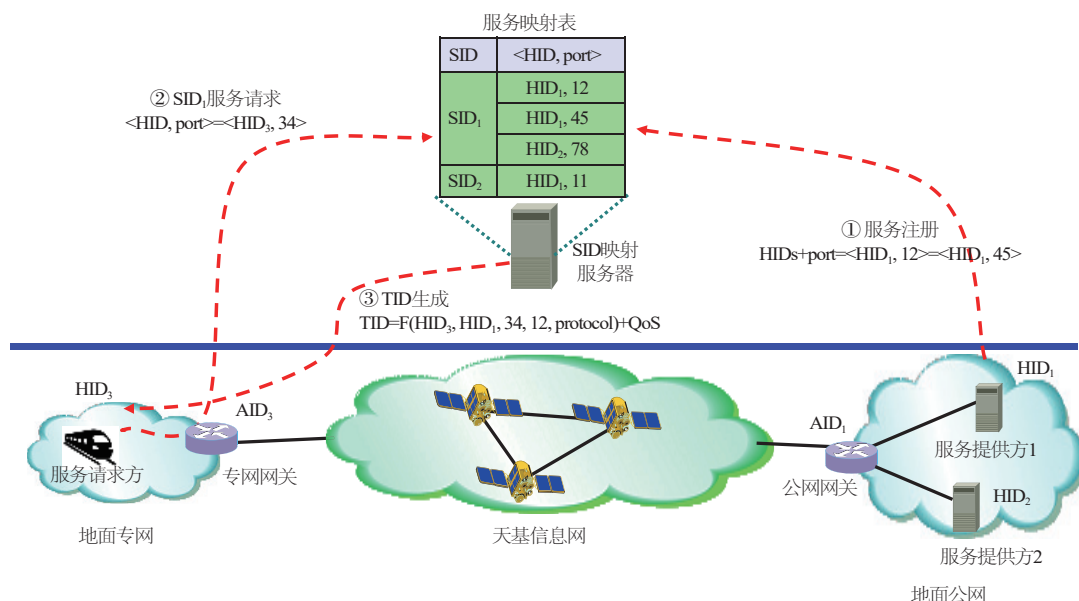


图3 专网与公网间通信场景中服务标识查询示意

携带的接入网关节点AID₁的信息,仍然以二层通信的方式转发到公网的网关节点AID₁。当公网的网关节点AID₁收到数据分组后,通过对数据分组中携带的TID信息的解密,发现该数据分组的源主机为HID₃,宿主机为HID₁(如图4中的步骤⑥所示)。最后,在公网内该数据分组从公网的网关节点AID₁发送到宿主机HID₁(如图4中的步骤⑦所示)。需要指出的是在公网内部,AID₁和HID₁作为公网内的路由协议的源地址和宿地址,在不改变公网的组网机制和路由协议的基础上实现公网内的路由。通过图4中的分组转发过程,发现通过高效的标识映射机制,可以实现天基信息网、地面专网以及地面公网的深度融合。

进一步分析图4分组转发中的安全性问题。首先,专网中的主机只需要通过映射系统查找需要的服务标识,就能与相应的服务提供方建立连接。对于主机而言,连接的是服务,至于服务提供方的具体对象是由哪个映射系统提供的,主机本身并不知道。同时,映射系统将源主机标识和服务提供方的主机标识通过函数变换隐性地表达出来,

只有具有解密能力的网络实体才可以进行解析,从而避免了恶意用户利用服务提供方的IP地址和端口号进行DoS攻击,提高了服务提供方的安全性。其次,在天基信息网内部路由过程中,通过TID信息对通信的对端实体进行了隐藏,进一步提高了专网通信双方的安全性。最后,通过专网网关节点AID到卫星路由节点RID的映射,实现了路由核心系统的隐藏,进一步提高了天基信息网核心路由的安全性。综上所述,本文所提出的标识体系及映射机制能满足天地异构融合网络中通信与安全一体化的要求。

再考虑天基信息网支持专网与专网间通信的场景,如图5所示。图5中专网与专网间数据转发示意与图4中专网与公网间数据转发示意基本类似。其主要区别在于业务标识TID由通信的源主机生成,其他过程保持不变。从图5中可以发现,天地异构融合网络中专网与专网间数据转发过程仍能满足通信与安全一体化的要求。

在基于标识映射的通信与安全一体化的天地异构融合网络架构中,还需要重点研究映射系统的设计问题。

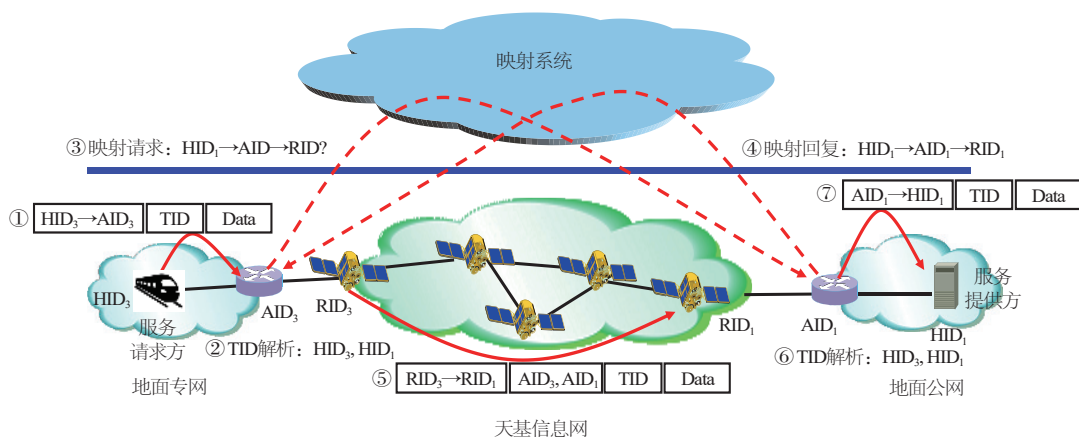


图4 专网与公网间通信场景分组转发示意

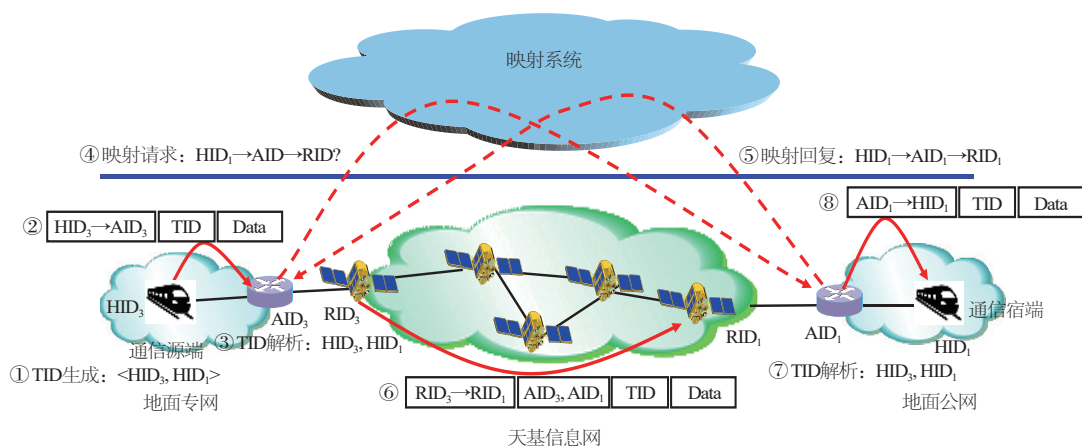


图5 专网与专网间通信场景数据转发示意

考虑到天地异构融合网络广域覆盖、拓扑动态时变、专网与卫星节点快速移动、时延大等特点,天地异构融合网络中的映射系统在设计时需要重点解决时延、移动性、可扩展性、全网同步等方面的问题。初步方案是在充分考虑天地异构网络拓扑特性的基础上,在高轨星座系统及地面公网的数据中心内建立全网同步的全局的映射系统,在互为备份的基础上可以适应不同场景的查询需求。考虑到全局映射系统的存储规模和查询效率,可以采用Chord环等经典方法构建分布式的全局查询系统。另外,由于天基异构融合网络中,部分节点距离高轨星座及公网数据中心接入时延过大影响查询效率,本文提出可以在低轨星座和地面专网网关节点上依据标识映射的查询热度进行本地Cache,并且为Cache表项设置生存时间以减小存储开销。本文认为,通过全局映射系统和本地映射系统的互补,可以最大限度地适应天地异构融合网络映射关系的查询需求。

5 结束语

本文针对天基信息网与高铁、船舶、民航等异构专网高效融合与安全通信的要求,采用标识映射机制,构建通信与安全一体化的天地异构融合网络标识体系。通过服务标识、业务标识、路由标识、接入标识、主机标识5类标识的高效映射,在不改变异构网络内部组网机制与通信协议的基础上,满足多域场景下天基信息网与地面各类专网间通信与安全的一体化要求,为天地异构网络的深度融合和互联互通提供了技术手段。

参考文献:

- [1] 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, 10(8): 19-30.
SHEN R J. Some thoughts of Chinese integrated space-ground network system[J]. Engineering Science, 2006, 10(8): 19-30.
- [2] 沈学民, 承楠, 周海波, 等. 空天地一体化网络技术: 探索与展望[J]. 物联网学报, 2020, 4(3): 3-19.
SHEN X M, CHENG N, ZHOU H B, et al. Space-air-ground integrated networks: review and prospect[J]. Chinese Journal on Internet of Things, 2020, 4(3): 3-19.
- [3] 周旭, 李泰新, 覃毅芳, 等. 基于边缘智能协同的天地一体化信息网络研究[J]. 电信科学, 2020, 41(7): 71-79.
ZHOU X, LI T X, QIN Y F, et al. Research on future space-ground integrated information network based on edge-intelligence collaborative[J]. Telecommunications Science, 2020, 41(7): 71-79.
- [4] 黄韬, 霍如, 刘江, 等. 未来网络发展趋势与展望[J]. 中国科学: 信息科学, 2019, 49(8): 941-948.
HUANG T, HUO R, LIU J, et al. Development trends and prospects of future networks[J]. Scientia Sinica Informationis, 2019, 49(8): 941-948.
- [5] 张亚生, 孙晨华, 谷聚娟. 天地一体化网络协议研究[J]. 无线电工程, 2018, 48(3): 178-182.
ZHANG Y S, SUN C H, GU J J. Research on protocols of space-ground integrated network[J]. Radio Engineering, 2018, 48(3): 178-182.
- [6] 刘立祥. 天地一体化信息网络的体系结构与协议分析[J]. 重庆邮电大学学报, 2018, 30(1): 9-21.
LIU L X. Analysis of architecture and protocol of space-ground integrated information network[J]. Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition), 2018, 30(1): 9-21.
- [7] 张宏科, 罗洪斌. 智慧协同网络体系基础研究[J]. 电子学报, 2013, 41(7): 1249-1254.
ZHANG H K, LUO H B. Fundamental research on theories of smart and cooperative networks[J]. ACTA ELECTRONICA SINICA, 2013, 41(7): 1249-1254.
- [8] 章小宁, 余腾腾, 邱恺, 等. 名址分离网络中一种新的双层映射系统研究[J]. 电子与信息学报, 2014, 36(10): 2357-2363.
ZHANG X N, SHE T T, QIU K, et al. A novel two-layer mapping system in networks with locator/identifier separation[J]. Journal of Electronics & Information Technology, 2014, 36(10): 2357-2363.
- [9] LUO H B, XU Y K, XIE W J, et al. A framework for integrating content characteristics into the future Internet architecture[J]. IEEE Network, 2017, 31(3): 22-28.
- [10] LUO H B, CHEN Z, LI J W, et al. D-PID: secure inter-domain routing with dynamic path identifiers[J]. IEEE Transactions Information and Forensics Security, 2017, 12(8): 1801-1815.

[作者简介]



章小宁 (1980-), 男, 博士, 电子科技大学教授, 博士生导师, 主要研究方向为天地一体化信息网络及未来网络架构。



朱立东 (1968-), 男, 博士, 电子科技大学教授, 博士生导师, 主要研究方向为卫星通信传输与组网、天地一体化信息网络。