网络出版时间：2015-04-08 21:20
网络出版地址：http://www.cnki.net/kcms/detail/11.1826.TP.20150408.2120.001.html

ADN：地址驱动的网络体系结构

吴建平[1,2] 李丹[1] 毕军[2] 徐恪[1] 李星[2] 朱晶[1]

[1]清华大学计算机科学与技术系，北京市海淀区，100083

[2]清华大学网络科学与网络空间研究院，北京市海淀区，100083

摘 要 以 TCP/IP 架构为基础的互联网，在可扩展性、高效性、安全性和灵活性等诸多方面面临着重大挑战。究其根源是因为现有的大部分解决方案下，IP 地址的多重属性没有得到充分体现和应用。本文提出了一种以地址为驱动的网络体系结构 ADN（Address Driven Network）。ADN 的核心思想是以 IP 地址的创新管理和使用方法为驱动，充分利用 IP 地址的多重属性，包括长度属性、逻辑属性、拓扑属性、时间属性、空间属性、所有者属性等，来解决当前互联网面临的规模扩展、平滑移动、安全可信、服务质量、网络虚拟化等问题。ADN 在 IP 地址多重属性得到应用的基础上，能够实现多种技术或应用，包括真实 IP 地址、二维路由、动态 IP 等。其中，二维路由将 IP 报文的源地址和目的地址一齐作为路由的依据，在保持纯 IP 路由的前提下能够完成许多现有扩展协议在牺牲一定性能和可管理性的基础上才能够完成的复杂路由；真实 IP 地址和动态 IP 则分别对报文的源地址和目的地址的真实有效性进行验证，防止恶意终端通过伪造源地址的方式发起规避追踪的网络攻击，或者对其他终端发起未得到授权的访问。

关键词 地址驱动网络，真实 IP 地址，二维路由，动态 IP

中图法分类号 TP393

ADN: Address Driven Internet Architecture

Wu Jianping[1,2] Li Dan[1] Bi Jun[2] Xu Ke[1] Li Xing[2] Zhu Jing[1]

[1] Department of Computer Science and Technology, Tsinghua University, 100086

[2] Research Institute of Network Science and Cyberspace, Tsinghua University, 100086

Abstract The Internet, which is constructed based on the TCP/IP structure, has been facing many challenges towards its scalability, efficiency, safety and flexibility. Most proposals today fail to solve these problems all together because they have not fully explored and exploited the multiple attributes of IP addresses. This paper proposes an address driven network architecture, called ADN. The core idea of ADN is solve the key problems faced by Internet, such as space scalability, smooth mobility, security and privacy, service quality, network virtualization, by innovative management and usage of IP addresses, with an extensive exploit of the multiple attributes of IP address, including the length attribute, logic attribute, topology attribute, time attribute, space attribute, ownership attribute, etc. The key technologies of ADN include validated IP address, two-dimensional routing, dynamical IP address, etc. The two-dimensional routing uses the source address as well as the destination address of an IP packet. On the premise of pure IP routing, two-dimensional routing is capable of

本课题得到国家 863 课题“地址驱动网络关键技术和验证”（SS2015AA010203）和国家发改委 CNGI 课题“一种新型网络体系结构：地址驱动的网络体系结构、技术研发和试验”(CNGI-12-03-001)的资助。吴建平，男，1954 年出生，博士，教授，主要研究领域包括计算机网络系统架构和协议设计，等等。Email：jianping@cernet.edu.cn。李丹，男，1981 年出生，博士，副教授，主要研究领域包括互联网架构、数据中心网络和云计算，等等。Email：tolidan@tsinghua.edu.cn。毕军，男，1972 年出生，博士，教授，主要研究领域包括新型互联网体系结构，等等。Email：junbi@tsinghua.edu.cn。徐恪，男，1974 年出生，博士，教授，主要研究领域包括计算机网络结构、高性能路由器和大规模 P2P 系统，等等。Email：xuke@mail.tsinghua.edu.cn。李星，1956 年出生，博士，教授，主要研究领域包括信息科学技术，等等。Email：xing@cernet.edu.cn。朱晶，1989 年出生，博士在读，主要研究领域包括下一代互联网体系结构、分布式计算系统，等等。Email：zjinn@aliyun.com。

realizing many complex routing strategies which most existing routing extensions cannot achieve without sacrificing its efficiency and manageability. The validated IP address and dynamical IP address verify the facticity and validity of the source address and destination address, respectively. They prevent the malicious users from launching attacks without being traced using source address forgery, or accessing other end-hosts in the Internet without authorization granted.

Key words Address driven network, validated IP address, two-dimensional routing, dynamical IP.

1 引言

1.1 IP协议与IP地址

TCP/IP 架构被广泛认为是互联网（Internet）取得巨大成功的关键原因所在。作为协调无限的用户需求和有限的网络资源之间的矛盾的传输协议，TCP 协议通过其拥塞控制机制实现了全网效率与用户公平性之间的有效折衷。作为无连接的分组交换协议，IP 协议不但实现了网络资源的充分复用，而且可以支持任意类型的应用。由于 IP 模型对应用类型不作限定，互联网上的应用创新得以以前所未有的速度发展，大大提高了社会生产力并便利了大众生活。

IP 协议的模型主要包括两大部分。第一是无连接的分组转发模型。与基于电路的交换方式不同，无连接分组转发不用在通信之前建立固定的通信信道，因此也不用把通信信道与特定的会话相关联，从而使得不同的数据分组可以充分复用网络信道资源，并且可以在网络上进行灵活的路由。第二是基于 IP 地址的寻址模型。IP 地址是 IP 协议为了统一标识网络层的所有通信实体而引入的命名空间。为了实现对异构物理网络（如以太网、FDDI、令牌环等不同网络）的互联，必须有一层与物理网络的链路层技术无关的网络实体命名空间，这也是 IP 地址诞生和存在的根本原因之一。

当前互联网体系结构非常依赖于 IP 地址，主要表现在两个方面。首先，从互联网命名空间来看。互联网的主要命名空间包括链路层地址（如 MAC 地址）、IP 地址和域名。其中链路层地址与传输介质有关，全局通用的命名空间主要是 IP 地址和域名。IP 地址不但用来标识网络接口的位置，而且被用来标识主机的身份，而域名是用一种易于记忆的方式来标识访问对象（主机或服务器）。DNS（域名解析系统）负责把域名解析为 IP 地址。可以说，IP 地址是整个互联网命名空间的核心，也是最不可或缺的命名空间。互联网是对大规模主机、服务器和网络设备进行互联的巨大系统，所有通信和访问归根结底需要转化为“点到点”的信息传输，而 IP 地址就是对这些“点”的全球统一标识。

其次，从互联网路由转发体系来看。互联网路由转发系统主要解决的问题是网络访问的“可达性”问题，即如何正确地将数据报文逐跳转发到目的地址。为了实现这一目的，必须在报文中携带目的 IP 地址，由中间路由器以查找路由表的方式将数据报文向目的地转发。同时，为了使得报文请求的内容能够被正确返回给请求者，报文中还携带了源 IP 地址。数据接收方收到报文之后，将目的 IP 地址与源 IP 地址交换位置，返回回复的数据报文。而中间路由器的转发表也是以 IP 地址为对象进行构建的。

1.2 当前互联网面临的主要问题

当前互联网在许多方面面临新的挑战，从互联网用户的角度看，比较重要的问题包括联网 IP 地址匮乏、服务质量缺乏保障、安全问题日益严重等等。下面一一介绍。

第一，“联网”需求是用户使用互联网最基本的需求。如果不能让用户以方便易用的方式连接互联网，其他的问题更无从谈起。随着互联网用户数量的飞速增长甚至物联网节点在内的“物物”相联的需求出现，传统 IPv4 的地址格式已经无法满足更多互联网用户的接入。NAT 等地址转换设备为互联网引入了许多 middlebox，破坏了互联网的端到端特性。随着 32 位的 IPv4 地址空间已经分配完毕，采用 128 位的 IPv6 地址格式进行互联网联网和通信，已经刻不容缓。

第二，在基于 IP 模型的互联网体系结构下，并不“严格”保证每个数据流的服务质量。用户服务质量体验的提升，依靠物理带宽的提升和充分利用物理带宽的分组交换技术来保证。从体系结构的角度看，路由体系的设计应该在保证可达性

的基础上，尽可能充分地利用互联网的网络带宽。但由于当前的互联网路由系统是基于目的 IP 地址进行“最短路径”路由的，所有到达同一目的地的流量将被聚合到相同的链路上，无法充分利用互联网的丰富链路资源，当存在流量热点是此问题更加明显。要实现对网络带宽资源的均衡使用，需要设计粒度更细的路由方式。此外，随着互联网已成为公众基础设施，对不同的应用、不同的用户进行区分路由，也是提高服务质量的一种方式。

第三，安全问题是互联网长期存在且广受关注的问题。当前的互联网安全解决方案，大多是针对不同的网络应用或网络场景下的安全攻击行为而设计。但本质上讲，与人类社会一样，网络攻击行为是难以从根本上杜绝的。从互联网体系结构的角度看，实现 IP 地址的可信任，并且尽可能降低网络被攻击的概率，是实现安全可信互联网的通用技术。保证源 IP 地址的真实性，从而互联网上每个数据包都有“责任人”，使得任何互联网攻击行为都可追溯，是对网络攻击行为进行震慑和追查的重要手段。IPv6 的巨大地址空间也使得我们能够对主机和路由器分配一个巨大的地址空间前缀，如果能让主机或路由器的具体 IP 地址在这个大地址前缀下进行动态变化，那么将可以极大地保护主机和路由器的 IP 地址隐私，减少主机和路由器地址泄漏的机会（因为在巨大 IP 地址前缀空间中进行地址扫描的成本非常高），降低被攻击或被控制为僵尸网络的风险。

第四，移动通信过程中 IP 地址切换带来的通信中断问题，一直是 IP 模型面临的主要挑战之一。在互联网体系结构中，IP 地址事实上承载了多重语义，既被用来标识主机身份，又被用来标识主机位置。在移动过程中，主机的位置发生了变化，而身份并未改变。如果用同一个 IP 地址来作为主机身份和位置标识，必然会引起 TCP 连接中断。但在 IPv6 地址提供的巨大空间中，可以把部分 IP 地址块用来固定作为主机身份标识，而部分 IP 地址块可以用来固定作为主机位置标识。在主机位置移动之后，只是作为主机位置标识的 IP 地址发生了改变，而主机身份标识并未改变。这样，我们在不引入新的命名空间的前提下，避免主机移动过程中的 TCP 连接中断问题。

1.3 从“地址”入手解决互联网面临的问题

基于以上分析，当前互联网面临的一系列问题，从本质上讲，大多与“IP 地址”的管理和使用方法有关。事实上，对于任何一个分布式复杂巨系统，其命名和寻址问题都是一大根本性难题；而由于互联网已经广泛服务于大众生活，这一问题显得尤为突出。任何试图解决互联网面临问题的体系架构和技术，从根本上讲，最终都需要落地到围绕“IP 地址”的一系列问题：地址空间的扩展和管理、地址（及其所表示身份）的安全性和隐私性、以地址为标识进行高效的路由、地址的移动，等等。

针对互联网面临的以上问题，我们从 IP 地址的使用和管理着手，提出了“地址驱动的互联网体系结构（ADN）”。

2 相关工作

下面介绍最近几年受关注较多的国际上提出的一些新型网络体系结构，主要包括美国 NSF 资助的下一代互联网项目以及软件定义网络 SDN。

2.1 NDN

NDN（Named Data Networking）[1]认为，传统的面向主机地址的通信方式已经越来越不能满足丰富的应用需求，同时面临着严重的可扩展性问题和安全问题。因此 NDN 改变网络沙漏结构中以 IP 地址为核心的设计方法，将数据的名称标签代替 IP 作为网络体系结构的核心层，即“窄腰结构”。用户在网络上的数据通信不再以“点对点”的方式进行，而是以数据内容为核心来进行。用户只用想要什么数据，而不用不再关心数据在哪里。

NDN 把数据传输过程分为“请求”和“响应”两个阶段[2]。通讯是通过接受方主动发出请求来完成的。在发起请求的 Interest 包中包含有所请求数据的名称。而路由器会根据转发表中对应名称（或者最长匹配前缀）的接口来转发请求。一旦找到了所请求的内容，会沿着转发的路径返回内容报文。为了提高效率，路由器会维护一个最近转发的请求列表和转发数据缓存。如果收到的请求存在于请求列表中，路由器不会重复转发请求，而是在之前发出的相同请求得到响应后一并发送数据。

NDN 对于传统网络层结构的颠覆性改变，虽然为适应其应用模式的上层应用提供了便利，但也存在一定的问题。一方面，NDN 是改变了当前

IP 网络无连接的转发结构，加重了交换机和路由器的负担，在大规模部署的扩展性方面有待验证；另一方面，NDN 对于围绕点对点通讯模式设计的现有应用来说，其全新的通讯模式需要后者花费相当的时间和精力来适应，其部署的渐进性受到挑战。

2.2 MobilityFirst

MobilityFirst[3]主要解决互联网的移动性问题。MobilityFirst 项目认为，传统 IP 网络结构下的路由是通过最长前缀匹配的方式来进行的，而当移动终端切换位置时，为了继续保证通讯能够继续进行，只能在所需要经过的路由器上加入新的路由项，或者为终端分配新的路由地址。但这些现有的方案都不能提供较好的 QoS 保证，也影响了网络的可扩展性。

MobilityFirst 的主要思想是，今后的互联网中，移动平台必将取代固定终端/服务器应用成为最主要的接入设备。同时移动应用的模式也会有更全面的发展，从以手机和笔记本移动应用为主流的现状发展到移动传感器、车载移动设备等方向。因此，下一代互联网体系结构的设计必须要以可移动性作为最主要的考虑因素。在覆盖率、服务稳定性和可靠性等要求得到满足的前提下，MobilityFirst 将架构设计的主要目标总结为以下六点：终端和网络的可移动性，不需要以单个固定的可信根节点作为基础，传输必须符合策略要求，必须具备拜占庭鲁棒性，网络上的内容必须可以寻址，同时对可能产生的新应用要有兼容性。

2.3 Nebula

Nebula[4]主要解决互联网如何适应云计算模式的问题。Nebula 项目认为，云计算应用的诞生和日益推广，实现数十年来计算机工作者的一个梦想：让计算就像电话系统那样时刻在线，可以满足多种服务需求，同时还要与时俱进，适应未来所有可能出现的新的应用。这种新的应用模式在经济效益、节能、安全和统一管理方面都体现了其优势。然而云计算依然缺乏一个有效支持的网络架构。

Nebula 的主要设计目标是一个能够更好地符合云计算需求的下一代互联网体系架构。这个网络架构除了需要在解决现有网络架构的安全性、移动性等问题以外，还必须满足数据中心网络的高带宽低延时等特点。这个架构本身必须具备安全性、灵活性和可扩展性，以及对多种策略机制的包容性等等。未来的云计算系统要能应对现有的和即将出现的网络威胁，支持不断更新的应用模式，同时在分配上还要做到可以兼顾技术可行性、经济效益和其他规章制度。

Nebula 的设计和实现主要包含三个部分：网络层协议 NDP 和对应的报头格式，可扩展的控制策略 NVENT，以及高速核心路由器 NCore。NDP 报头的设计加入了进行路由验证所可能需要的所有信息，并使用类似 MPLS 标签的结构的提供了多条备选路径。当终端需要开始通信时，NDP 会将路径查询需求和参数一并发送给 NVENT，而 NVENT 会通过一个类似 BGP 的协议来找到一条或者多条拓扑和协商策略上都可行的路径，并且连同需要经过的域的授权证明一并返回给 NDP。这样，在经过每个域时，都可以对当前流经过自己的合法性进行验证。然而在大规模的云计算系统下，普通的路由器 CPU 可能无法负载顶级 ISP 所需要处理的流量。为了支持所设计的协议，NEBULA 还开发了高可用性核心路由器 NCore。

2.4 XIA

XIA[5]项目认为，未来网络体系结构的设计依然需要延续沙漏结构，但是将以新的要素作为中心。许多设计根据需求将内容、服务或是用户等要素取代 IP 作为新体系结构的中心，之前提到的 NDN 就是一例。这些架构在自己面向的应用模式上都能达到很高的效率，因此都有自己的可取之处，但在其他应用模式上则难以发挥作用，因此没有一个有充分的优势可以取代其他的架构成为互联网的主宰。

XIA 的主要设计目的是，能够像今天的基于 IP 的互联网体系结构一样完美地承载和过渡到上面这些面向各种中心设计的架构，适应不同的应用模式，同时克服传统网络体系结构下可扩展性和安全性等方面的问题。为了达成这一目标，XIA 从更广泛的层面上定义了一个要素作为整个网络结构的核心，而实际通讯应用可以根据自己的需求将这个要素指定为具体的一个或者多个实例，例如内容、服务等等，只要这些实例符合 XIA 提出的可表达性、可扩展性和安全性三大要求，从而实现对于多种不同中心架构的网络协议的支持。在路由方面，XIA 用表达型互联网路由协议 XIP 取代了现有的 IP 路由协议，定义了报头的格式和如何对用户指定的实例进行操作。XIA 支持

在同一个网络中采用多个实例，并且在每个路由节点都根据得到用户描述的实例信息来进行选路。

尽管 XIA 给网络在可扩展性和安全性上可以带来显著的改善，但代价却是采用了相对于今天基于 IP 的互联网架构差别较大的基于语义标签的路由模式。因此，XIA 想要融入互联网的实际应用，若非在短时间内得到大范围部署，就必须构建在覆盖网络之上。无论是通过何种方式实现，XIA 和现有网络的兼容性是不够的。因此实际推行过程中要如何兼容现有的网络模式和应用，保持和未部署地区之间的互联，是 XIA 难以解决的问题。

2.5 SDN

SDN[6]的倡导者们认为，当前互联网设备的实现方式是封闭式和分布式的，造成控制协议过于复杂，路由器的软件设计开销太大，不但增加了路由器的成本、限制了更灵活的路由和传输策略，而且无法向上层应用开放网络功能。因此，SDN 提出把控制层面和转发层面分离，通过在一个集中式的控制器（Controller）上来实现更灵活的路由策略计算，并把结果通过标准的通信协议配置到路由器/交换机上。

SDN 体系架构主要包括三个方面，即控制器，路由器/交换机转发层面，以及控制器和路由器/交换机之间的通信机制。SDN 的优点是把控制层面从传统路由器中剥离出来，使得研究人员或者运营商能更灵活地配置和控制路由，并降低了路由器本身的复杂性和成本。此外，将网络功能开放给上层应用，使得网络管理者可以按照自身需求对网络功能进行按需编程。

从本质上而言 SDN 实际上是一种技术手段，而非网络架构。近些年来集中在 SDN 上的研究虽然多，但大多都是解决网络中一些局部性或者针对性较强的问题。同时，SDN 集中控制的属性也有碍于跨域部署，其应用更多局限于域内或者企业级数据中心等局域网环境中。

3 ADN 体系结构

IP 地址的属性

IP 地址具有多重属性，包括长度属性、逻辑属性、拓扑属性、空间属性、时间属性、所有者属性等。下面将作一一叙述。

长度属性的含义非常简单，即 IP 地址的比特位长度，它意味着 IP 地址可以标识的物理或逻辑实体的数量。

逻辑属性，指的是 IP 地址的逻辑含义。在一般情况下，IP 地址表达一个网络接口在巨大网络空间中的位置。在现有的传输协议（如 TCP）设计中，IP 地址也用来标识一个终端的身份，即传输层会话的连接实体。在组播通信中，IP 地址还被用来作为一组会话的逻辑标识，即表示一个组播组（或者说一组数据发送者和数据接收者的集合）。事实上，我们还可以对 IP 地址进行更加灵活的使用以支持更加丰富的逻辑语义。

拓扑属性，指的是 IP 地址所标识的网络接口在整个网络拓扑中的层次化位置。由于互联网拓扑结构是层次化的，每个 IP 地址都表示其在全球互联网拓扑中的特定位置。这个特定位置决定了任意两个 IP 地址之间的路由路径、路由跳数（而不一定是物理距离远近）、传输延迟等性质。

空间属性，指的是一个 IP 地址表示的网络接口所在的物理空间，可以用经纬度来表示。IP 地址的空间属性可以为很多在线服务提供支持，比如与地理位置有关的广告，天气预报，等等。也有研究人员利用 IP 地址的空间特性提出“地理位置路由”（Geographical Routing）[7]。

时间属性，是指一个 IP 地址的时间有效性。IP 地址是由“国际域名与 IP 地址管理机构”ICANN 统一进行分配的。从分配的那一刻起，IP 地址就开始有效，但目前 IP 地址的回收很少进行。但对某一个具体的主机而言，如果通过 DHCP 协议得到动态分配的 IP 地址，则其 IP 地址的生命周期就是被 DHCP 协议分配地址到主机下线这段时间。

所有者属性，是指 IP 地址的所有者。当前互联网是一个全球分布式巨系统，由许多运营商通过自治域的形态分别运营。一旦一个 IP 地址（段）被分配成功，从管理角度而言其所有者（某个运营商，或某个机构，或某个终端用户）就是确定的。

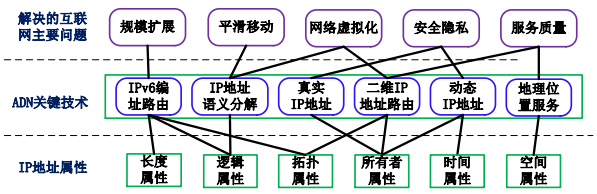

图 1 ADN 体系结构示意图

3.2 地址驱动网络架构

经过研究，我们认为当前互联网体系结构并未充分利用 IP 地址的多重属性。具体而言，对 IP 地址的拓扑属性使用较为充分[8]（主要用于路由转发体系），对 IP 地址的长度属性预计不足（已提出 IPv6 协议解决这一问题），对 IP 地址的逻辑属性有一定程度的使用单并不充分（主要是用 IP 地址来表示组播会话、广播通信等），但对 IP 地址的所有者属性、时间属性、空间属性等利用并不充分。而对 IP 地址多重属性的开发和使用，是解决当前互联网面临问题的重要手段之一。

如图 1 所示，地址驱动网络 ADN（Address Driven Network）的核心思想，就是通过对 IP 地址属性的高效灵活使用，来解决当前互联网面临的主要挑战。ADN 并未改变互联网的五层（七层）体系结构，但对网络层 IP 地址的使用、管理以及基于 IP 地址的路由和安全隐私机制进行了大大增强。IPv6 提供的巨大 IP 地址空间是 ADN 的基础。ADN 体系结构包含的关键技术阐述如下。

第一，把 IP 地址空间分解为身份 IP 地址空间和位置 IP 地址空间。IPv6 提供了 2^{128} 大小的地址空间。在可以预见的未来互联网环境下，IP 地址的总数量是远远大于实际可联网的节点数量的。因此可以预见，在未来我们不仅不用担忧 IP 地址空间不足带来可扩展性问题，甚至可以去达成之前的网络架构中受地址空间所限所不能达成的目的。

具体来说，在 IPv6 下提供的 128 位大小的地址空间中，我们只需要利用前 64 位地址空间就可以完美地完成路由的工作，同时还能保证 IP 地址具有相当丰富的拓扑属性和空间属性等。那么，我们完全可以自由利用剩下的 64 位空间去实现更加丰富的语义。例如，我们可以将 IP 地址后 64 位作为每个节点的身份标识，和 64 位前缀构成的位置标识可能随着节点的移动而改变不同，身份标识在节点的生命周期不会轻易改变。这就可以为节点的平滑移动提供一定的支持。

第二，保证源 IP 地址的真实性。把每个分组的源 IP 地址（前缀）作为其责任人。当互联网攻击行为或危害安全的行为发生时，通过真实源 IP 地址追溯到责任人；同时，通过端口过滤及时将伪造了源地址的报文阻断在互联网的入口处。保证源 IP 地址的真实性非常重要。在子网内，通过将源 IP 地址与交换机端口绑定，避免源地址假冒现象发生[9]。在自治域之间，通过建立信任联盟，避免假冒其他自治域源 IP 地址的分组。这一技术主要利用 IP 地址的所有者属性。

第三，基于源 IP 地址和目的 IP 地址进行“二维”路由转发。[10][11]路由器对数据包进行路由转发时，不只考虑目的 IP 地址，还考虑源 IP 地址。这样，通往同一个目的 IP 地址的来自于不同源 IP 地址的流量可以被分散到不同的路径上，不仅能更灵活地利用网络链路资源，还能够根据源地址所附带的属性信息进行精确的调整。二维路由也可以代替通道技术成为网络虚拟化的主要实现手段。这一技术主要利用 IP 地址的拓扑属性和所有者属性。

第四，IP 地址动态化。每个主机或者路由器接口的位置 IP 地址在 2^{64}-1 的巨大空间中进行动态变化。位置 IP 地址动态变化的目的，在于尽可能地使主机或路由器的位置信息匿名化，从而降低主机和路由器被攻击的风险。一般情况下主机收到的发往当前不再使用的位置 IP 地址的数据包被自动丢弃，但在位置 IP 地址动态变化过程中，保证通信对端通过旧位置 IP 地址发来的数据包能正常接收。这主要利用 IP 地址的时间属性和所有者属性。

第五，基于 IP 地址的地理位置服务（Location based Service）。基于地理位置的互联网服务越来越重要。虽然很多设备如手机都采用 GPS 进行物理位置定位，但一来并非所有设备都有 GPS（比如桌面电脑或网络设备），二来 GPS 定位无法应用于室内，因此对 IP 地址进行准确物理定位并提供基于 IP 地址地理位置，是提高互联网服务质量的一个重要技术手段。该技术主要利用 IP 地址的空间属性。

下面重点对真实 IP 地址、二维 IP 地址路由和动态 IP 地址技术进行论述。

3.3 真实IP地址

IP 报文所携带的 IP 地址字段包括目的 IP 地址和源 IP 地址。目的 IP 地址是进行路由转发的基础，因此一般而言，目的 IP 地址是真实可信的。但源 IP 地址在当前的互联网路由转发体系中并没有得到非常有效的真实性检查。事实上，源 IP 地址表示分组的发出地，也是一个分组的直接“责任人”。在现有互联网体系结构下，分组转发过程中，并不对源 IP 地址进行检查，因此可以很轻易地假冒源 IP 地址。这样，对于大量网络攻击报文

或者危害网络安全的报文，将难以溯源，也因而很难对网络攻击者形成威慑力。

真实 IP 地址技术，其核心思想就是使得网络中传输的每个报文的源地址都是真实可信的，保证可以对每个分组进行溯源。尽管在当前网络技术条件下，对每个分组进行线速存储代价较高，但对分组的抽样缓存并溯源，仍然可以保证对绝大多数网络行为找到其责任人。事实上，与人类社会类似，任意的安全解决方案都不可能杜绝所有的攻击行为，总会有新的危害安全的主体和行为发生。“让每个行为有其责任人”，这是人类社会中解决安全问题所采取的根本和共性技术手段，也同样适用于互联网环境中。

实现真实 IP 地址，防御地址伪造攻击的方法有多种，根据检测伪造地址机制，可以分为密码检测、特征匹配检测和路由信息检测等等。其中，密码检测安全性好但部署开销较大；特征匹配检测只能根据大量历史信息建立的特征库来检测可能来自伪造源的报文，因此不能从根本意义上解决地址伪造攻击的问题，其精确度也不高；而路由信息检测在效果和部署难度上相对较为均衡，成为真实 IP 地址研究中广为采用的一种机制。

用路由信息检测来验证地址的真实性，其基本原理在于根据流量来源路径的合理性来判断报文的源地址是否被伪造。这一原理在互联网中已经得到了相当的应用。比较有代表性的包括反向路径转发机制 RPF[12]。RPF 假设报文对于来自某个源地址的流量，其入端口应该和转发向该地址流量的出端口是一致的，否则就可以认为该流量的源地址是被伪造的。然而，RPF 的缺点在于无法兼顾到互联网在域间路由上的不对称性，无法在多个自治域间得到广泛的应用。

2008 年清华大学提出了 IPv6 真实源地址验证架构 SAVA[13],[14]，根据 IPv6 地址分配的特点进行了更加系统和有效的分层真实地址验证。如图 2 所示，SAVA 提出了保证源 IP 地址的真实性需要从子网、域内、域间三个层次进行验证。在子网内部，通过分组源 IP 地址、分组源 MAC 地址、交换机端口号、DHCP 服务器相互合作的方式，保证每个源 IP 地址不但是已经真实分配存在的 IP 地址，而且要跟实际发出报文的主机相匹配。如果每个子网都进行了真实 IP 地址部署，那么一般情况下域内路由转发可以认为是真实可信的；否则，需要在域内路由器上进行反向接口检查来降低源地址假冒的概率。在全网范围内，如果某些自治域部署了真实 IP 地址技术，而其他自治域并未部署，可以让部署了真实 IP 地址的自治域之间组成可信任联盟，从而以激励的方式促使真实 IP 地址技术的增量部署，同时防御来自其他 AS 的诸如 BGP 劫持之类的恶意攻击。

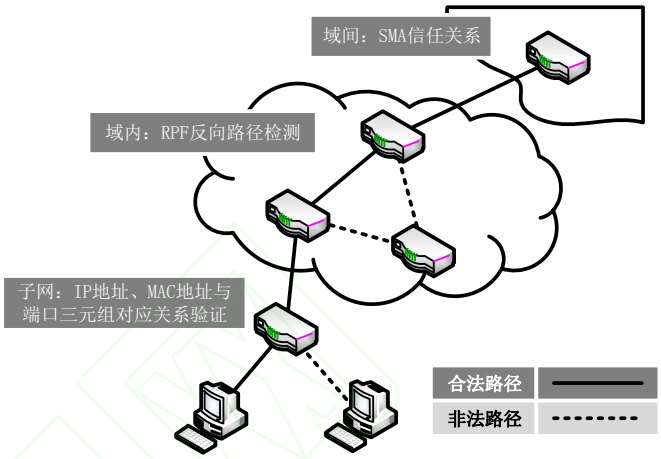

图 2 SAVA 三层源地址验证架构示意图

3.4 二维IP地址路由

传统的路由转发体系中，路由路径的生成仅仅依赖于目的地址。因而对于某个特定的目的地址，其路由生成图具有树形结构的特点，如图 3 所示。在其路由生成图中来自任意点的流量一旦在某个网络节点汇聚在一起后，不借助其他转发系统（如 MPLS[15]，源路由）和应用（如负载均衡器，load balancer）的帮助就无法再进行分流。虽然 MPLS 和源路由技术也可以灵活地确定路由路径，但它们都存在各自的问题。源路由需要由终端系统来决定每个报文的路由方案并且植入到报头内，因此将路由的任务和权限暴露给了端系统，不仅加重了端系统的负担、不能得到全局最优的路由方案，而且还具有一定的安全隐患。MPLS 多部署在自治域内部，将包的转发策略映射为域内节点可识别的二层标签，在自治域的边界进行转译，而在域内通过标签进行高速转发。虽然 MPLS 映射规则的灵活性给其带来相当高的自由度和效率，但 MPLS 系统的封闭性也给网络测量、管理和安全方面的工作带来了相当的不便，特别是对于基于纯 IP 网络的协议和应用，例如路径追踪等等的支持性很差。

基于二维 IP 地址的路由转发方案则在解决分流问题的基础上，很好地克服了上述转发系统的缺点。二维路由的基本思路在于，生成转发规

则时不仅要考虑报文的目的地址，也要考虑源地址信息。如图 4 所示，二维路由的转发表结构为源地址、目的地址对到转发接口的映射。

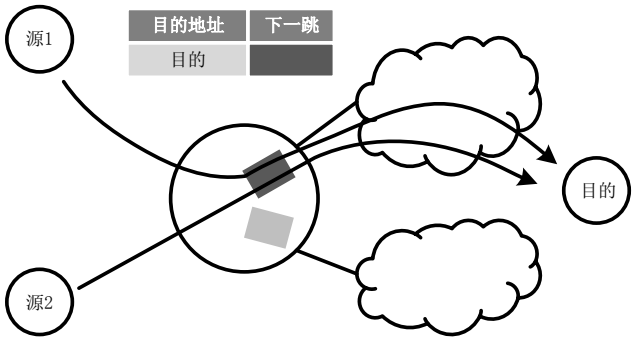

图 3 传统转发系统示意图

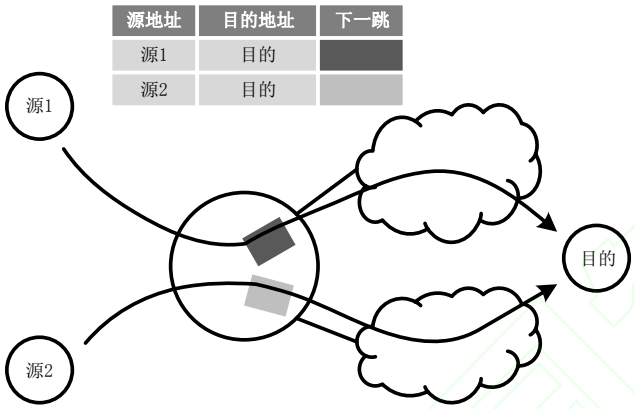

图 4 基于二维路由的转发系统示意图

在我们的现实生活中，尽管可能对于某个特定目的地址可能存在规模较大或者分类繁杂的流量，但这些流量来自相同的源地址或者前缀的可能性是几乎不存在的。对于以某个特定地址为目的地的流量，即便在网络中的某个节点被汇聚在一起，在此后依然可以依据其不同的源地址进行分流。这种分流既可以是为了均衡链路负载，也可以是为了能够根据源地址的身份信息提供不同级别的服务。因此，二维路由相对于传统的一维路由来说更加灵活，也可以支持更多的自定义路由策略。

同时，二维路由依然是纯 IP 转发系统，其报头格式和传统一维路由并无二致，其报文在仅支持一维路由的系统上也可以正常转发，并且完美支持任何基于 IP 转发设计的应用。这种纯网络层实现的分流系统能够继续保有原纯目的 IP 路由的高效性和兼容性。

二维路由因为其灵活性，相对于传统路由来说可以支持更多自定义的路由策略和应用。包括：

1）分级服务。根据端采用的不同源地址所体现的用户身份信息，可以识别流量的优先级和需求信息，从而为不同的流量提供分级服务。不仅不同的用户可以依据其源地址被识别出来，同一个用户也可以合理利用自己分配得到的数个 IP 地址去请求不同等级的服务。

2）流量均衡。传统路由下，流量均衡多通过 MPLS 的方式来实现。而二维路由完全可以给来自不同源地址的流量选择不同的通路，从网络层完成流量均衡的任务。在图 2 中的示例就体现了二维路由充分利用多路径实现流量均衡避免拥塞的特点。

3）多路和反向代理。在二维路由的帮助下，多路和服务器反向代理可以完全实现在网络层，直接通过报文的源地址进行重定向。相对于传统的重定向来说，二维路由的吞吐率和精确度都更高。

4）快速故障恢复。在基于一维路由的转发系统中，快速故障恢复仅仅能够对于单点故障保证百分之百的保护率。而在二维路由中，快速故障机制可以根据报文的源地址和目的地址推测报文在转发过程中所经过的节点，从而能以更高的几率让报文在接下来的转发过程中绕开故障节点并避免环路的出现。

3.5 动态IP地址

和一般服务器的 IP 地址信息不同，对主机而言，其 IP 地址作为重要的身份和位置信息，隐私性需要得到保护。这是因为从效率和安全的角度考虑，主机没有必要响应来自匿名主机和服务器主动建立的连接，因此也就不需要将 IP 地址透露给未授权的对端。相反，一旦主机的 IP 地址被恶意攻击者获取，将会带来各种安全隐患：攻击者既可以直接对主机发动攻击，也可以通过反射拒绝攻击的方式间接对主机发动攻击。

IPv6 提供了巨大的 IP 地址空间，也降低了主机暴露 IP 地址的概率。但一旦攻击者通过地址扫描成功找到主机的 IP 地址，仍然可以建立连接并进行攻击。真实地址验证可以防御来自伪造地址攻击者的反射拒绝攻击，但对于没有经过源地址伪造，或者通过隧道来进行的攻击却束手无策。因此，要从根本意义上解决地址泄露引发的安全问题，最直接的方法是提供一个访问控制系统。而动态 IP 地址则可以很好地实现访问控制的功能。

在 IPv6 环境下，为每个主机动态或者静态分

配的地址实际上为前 64 位地址构成的前缀，而后 64 位地址需要在主机接入互联网时自行动态生成。这种地址分配模式给了主机一定的选择自由，但就目前而言地址的后 64 位一般是通过主机的 MAC 地址或者随机的方式生成，其自由度几乎没有得到应用。而动态 IP 地址技术则利用了这一特性。

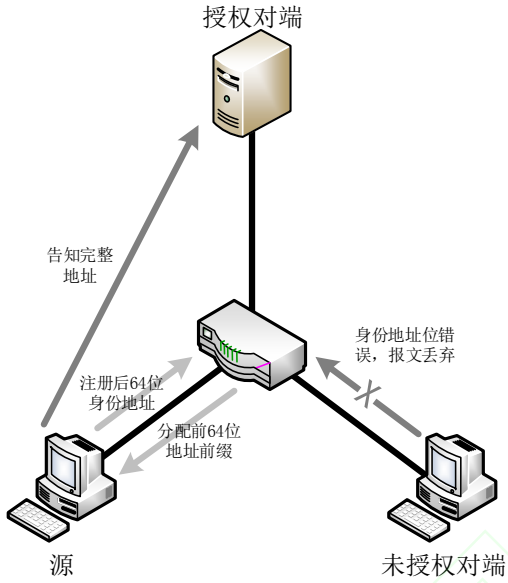

图 5 动态 IP 地址示意

如图 5 所示，动态 IP 地址技术允许主机以主动（主机自由决定并向 DHCP 服务器注册）或者被动（DHCP 服务器决定主机跳变的地址）的方式在短周期（10 秒级别）内，改变 IPv6 地址中后 64 位的可变部分。一旦地址发生跳变后，旧有地址只能在限定时间内由已经以此地址建立的 TCP 连接使用，主机不再接受以过期地址发起的新连接。IPv6 地址空间的庞大，加之跳变周期较短且可控，攻击者很难以扫描的方式快速定位主机跳变之后的地址，从而大大增加了主机 IP 地址的匿名性。只有主机主动连接、知晓正确地址的对端才能和主机建立连接；而其他对端即便得到了正确的主机 IPv6 地址前 64 位前缀，也会因为后 64 位动态地址错误而导致报文在转发过程中被丢弃。

利用动态 IP 地址技术来防御拒绝服务攻击等流量攻击，相对于传统方案来说更具备灵活性。在传统的解决方案中，识别合法和非法流量必须放在应用层进行，非法流量虽然得到丢弃但依然会造成网络拥塞。这是地址暴露带来攻击隐患的根源所在。动态 IP 地址下对于流量的识别完全可以在交换机或路由器的数据层面进行，未被授权的流量在未达到主机之前就可以被路由器识别、过滤和丢弃。这样，同时到达的，甚至是来自同一个源地址的流量，其合法流量和非法流量也可以在网络层被区分开来，在过滤非法流量的同时不会影响合法流量的传输。同时，在 IPv6 的架构下，同一个主机可以同时使用多个合法的 IP 地址。通过为使用中的不同 IP 地址进行分组并设定更换周期，主机可以将自己的通信对象，特别是需要在一定时限内被动与之建立连接的对象进行分级，为其提供不同的访问周期。

而目前我们为动态 IP 地址系统设计的分层地址动态机制，能够在保证可扩展性的前提下提供较为广泛的非法访问阻隔半径。目前现存的动态 IP 地址系统，为了能够真正达到不影响路由和应用的动态连接效果，需要借助 NAT 等中间件或者通过 SDN 的方式来实现。这种实现方法存在一定的扩展性问题，因为无论是 NAT 的地址映射表和 SDN 的转发表大多都是扁平结构的，一旦项目增多就会导致存储空间紧张。

而分层地址动态机制则利用 IPv6 丰富的地址空间去满足可扩展性。如图 6 所示，在分层地址动态机制中，IPv6 地址中的可变部分被分为多段。网络中的主机和路由器根据配置协议定义的层级负责所属段落地址的动态变化，将动态变化结果通知配置服务器，并且对直属子网段的动态地址负责过滤。

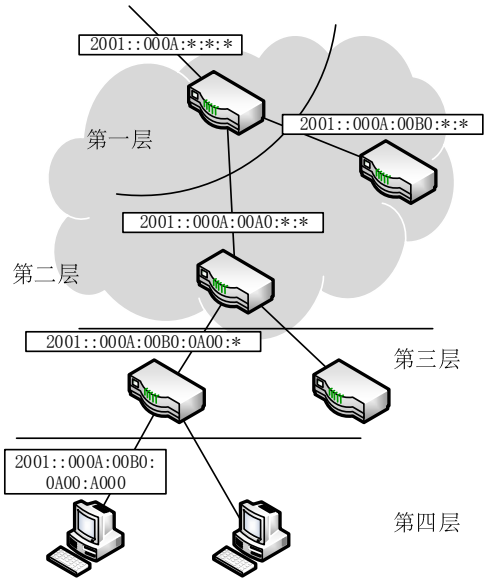

图 6 分层地址动态机制

在长达 64 位的可变 IPv6 地址空间中，以 8 位为单位可以最多负载多达 8 层的层次化域内网络结构，而路由器只需要对与其直连的路由器或者终端进行其所属层级动态地址的过滤，完全可以在端口过滤器上实现而不需要涉及复杂的过滤机制和匹配表结构。这种设计模式使得动态地址系统可以提供的服务终端数目以指数级增长，完全可以满足现有以及近未来的网络扩展需求。

4 ADN 与 SDN 和 NDN 的关系及区别

如第 2 章所述，近年来学术界提出了许多针对未来互联网架构的方案，其中最为广泛接受的是 SDN 和 NDN。SDN 的核心思想是把网络的控制层面与数据层面分离，并把网络功能开放给上层应用。因此，SDN 本质上是一种新型的互联网体系结构实现技术，而不是互联网体系结构本身。SDN 作为一种平台，为解决互联网所面临的规模扩展、平滑移动、服务质量、安全可信等问题提供了新的实现手段，但并未提出解决这些问题的具体方案。从这个角度讲，与 SDN 对应的是传统的分布式、封闭式的互联网体系结构实现方式，而不是某种体系结构方案。ADN、NDN 甚至其他的互联网体系结构既可以用 SDN 来实现，也可以用传统方式来实现。

NDN 的核心，在于以“标识内容的名字”代替“标识节点的地址”来作为互联网体系结构的基本要素、以及路由和传输的基本单元。每个内容都用一个名字来表示，一个接收者想接收数据，需要先发送对内容名字的请求；路由器维护一个请求列表，并且通过缓存内容把数据发送到所有发送过请求的接口。从本质上讲，NDN 的工作过程，与 IP 组播非常类似。主要不同的地方在于，IP 组播是通过把 IP 地址空间中的一部分拿出来作为会话或数据的标识，而 NDN 则引入全新的名字空间对内容进行标识。除此之外，NDN 提出在路由器上进行泛在缓存，但这种方案与 IP 网络中的“内容分布网络（CDN）”[16]的思想非常类似，也可以在 IP 网络中进行支持。

ADN 是一种通过对 IP 地址的管理和使用方式的增量式改进和创新，来解决当前互联网面临的一系列挑战的体系结构方案。通过对 IP 地址语义的灵活定义，完全可以实现 NDN 所希望达到的大部分目标（比如上面所举的 IP 组播的例子）。ADN 既可以用 SDN 实现，也可以基于现有网络的分布式架构来实现。而 ADN 的最大特点在于其没有改变当前互联网成功的“基因”即 IP 协议，可以在现有互联网上往未来互联网进行平滑过渡[17][18]。

5 结论

本文提出了地址驱动的网络体系结构 ADN。ADN 的核心思想是保留当前互联网成功的基因，即 TCP/IP 体系结构，并以 IP 地址的创新管理和使用为驱动，来解决当前互联网面临的一系列问题，并以平滑的方式从当前互联网过渡到下一代互联网。ADN 充分利用了 IP 地址的多重属性，包含了真实 IP 地址、二维路由、动态 IP 等多种创新技术。ADN 体系结构不但可以用于互联网的演进，还可以用于将互联网、移动通信网、空间网络等多种网络的融合。

参 考 文 献

[1] V Jacobson, DK Smetters and JD Thornton, etc. Networking named content. Proceedings of the 5th international conference on emerging networking experiments and technologies, Rome, Italy, 2009: 1-12.

[2] H Yuan, T Song and P Crowley. Scalable NDN forwarding: concepts, issues and principles. Proceedings of the 21st international conference on computer communications and networks (ICCCN). Munich, Germany, 2012: 1-9.

[3] I Seskar, K Nagaraja and S Nelson, etc. MobilityFirst future internet architecture project. Proceedings of the 7th Asian internet engineering conference. Bangkok, Thailand, Nov 2011: 1-3.

[4] T Anderson, K Birman and R Broberg, etc. NEBULA - a future internet that supports trustworthy cloud computing. White paper, the NEBULA team: Nov ,2010.

[5] A Anand, F Dogar and D Han, etc. XIA: an architecture for an evolvable and trustworthy internet. Proceedings of the 10th ACM workshop on hot topics in networks, Cambridge MA, USA: Article No.2.

[6] Software-defined networking: the new norm for networks. White paper, Open Networking Foundation: April 13, 2012.

[7] H Takagi and L Kleinrock. Optimal transmission ranges for randomly distributed packet radio terminals. IEEE transactions on communications, 1984, 32 (3): 246-257.

[8] V Fuller and T Li. Classless inter-domain routing (CIDR): the

internet address assignment and aggregation plan. RFC 4632, 2006.

[9] J Li, J Mirkovic and M Wang, etc. SAVE: source address validity enforcement protocol. Proceedings of the IEEE infocom 2002. New York, USA, 2002: 3, 1557-1566

[10] S Yang, M Xu and D Wang, et al. Scalable forwarding tables for supporting flexible policies in enterprise networks. Proceedings of the IEEE infocom 2014. Toronto, Canada, 2014: pages 208-216.

[11] M Xu, S Yang and D Wang, etc. Two dimensional-IP routing. Proceedings of the 2013 international conference on computing, networking and communications. San Diego, USA, Jan 2013: 835-839.

[12] F Baker and P Savola. Ingress filtering for multi-homed networks. RFC 3704, 2004.

[13] J Wu, J Bi and X Li, etc. A source address validation architecture (SAVA) testbed and deployment experience. RFC 5210, 2008.

[14] J. Wu, J. Bi, M. Bagnulo, F. Baker, C. Vogt, Source Address Validation Improvement Framework, RFC7039, 2013

[15] LD Ghein. MPLS Fundamentals. Indianapolis: Cisco Press, 2006.

[16] M Holfmann and LR Beaumont. Content networking: architecture, protocols, and practice. Cambridge MA: Elsevier, 2005.

[17] X. Li, C. Bao, "Address switching: Reforming the architecture and traffic of Internet", Science in China Series F: Information Sciences, 2009,52 (7): 1203-1216

[18] Jianping Wu, Song Lin, Ke Xu, Ying Liu, Ming Zhu. Advances in Evolvable New Generation Internet Architecture. Chinese Journal of Computers, 2012, 35(6): 1094-1108.
(吴建平，林嵩，徐恪，刘莹，朱敏. 可演进的新一代互联网体系结构研究进展. 计算机学报, 2012, 35(6):1094-1108.)

Jianping Wu, born in 1954, Ph.D., Professor. Email jianping@cernet.edu.cn. His research areas include computer network, system architecture and protocol design, etc.

Dan Li, born in 1981, Ph.D., Associate Professor. Email tolidan@tsinghua.edu.cn. His research areas include Internet architecture, data center networks and cloud computing, etc.

Jun Bi, born in 1972, Ph.D., Professor. Email junbi@tsinghua.edu.cn. His research areas include new Internet architecture, etc.

Ke Xu, born in 1974, Ph.D., Professor. Email xuke@mail.tsinghua.edu.cn. His research areas include computer network architecture, high performance router and large scale P2P system, etc.

Ke Xu, born in 1974, Ph.D., Professor. Email xuke@mail.tsinghua.edu.cn. His research areas include computer network architecture, high performance router and large scale P2P system, etc.

Xing Li, born in 1956, Ph.D., Professor. Email xing@cernet.edu.cn. His research areas include information science and technology, etc.

Jing Zhu, born in 1989, Ph.D. candidate. Email zjinn@aliyun.com. His research areas include next generation Internet architecture and protocol, distributed computing system, etc.

Background

TCP/IP protocol has been the basis of the entire global network since the very beginning of Internet. Benefiting from the multiple attributes of IP addresses, the IP protocol has been acting as the "narrow wraist" of the network protocol stack and successfully unified many diversely structured networks. Yet, many of the problems that today's Internet has been facing originate from our incomplete development of IP addresses' full potential. Though many of today's next generation Internet projects claim to provide a network environment which can meet the future requirements, they are either highly specialized so that they can only be deployed to networks with particular specifications to solve parts of the problems, or highly complicated so that their deployment introduces too many network devices and traffic workloads.

In this paper we propose an address driven network architecture (ADN) to cope with today's challenges on Internet that many existing approaches fail to overcome. Different from all existing architectures, ADN intends to solve all of today's problems solely dependent on the base of today's IP network architecture, so that it can be progressively deployed to a network of any scales or specifications with little efforts. ADN consists of three most important components: the validated IP address, two-dimensional routing and dynamical IP addresses. The validated IP address deploys a layer-structured ingress interface filtering mechanism similar to RPF to verify the source address of the incoming packets. It improves the security, the traceability and manageability of the Internet by neutralizing the address forgery. Two-dimensional routing replace today's destination address based routing with source/destionation address dual based routing. With the dimenisional growth the extended IP-based routing is capable of realizing more completed strategies and applications. The dynamical IP address enables hosts to change their valid IP address from time to time and keeps anonymous visitors away. It can effectively mitigate the impact of malicious attacks such as DDos and worms.

This work is part of and funded by National High Technology Research and Development Program (863 Program) of China (SS2015AA010203) and National Development and Reform Committee CNGI Project (CNGI-12-03-001).