## 第10章 真实源地址验证SAVA体系结构与关键技术

互联网已经成为我们日常生活中密不可分的一部分，然而从第8章和第9章的介绍中我们也看到了互联网实际上是非常脆弱的，非常容易受到各种网络攻击的危害。这些网络攻击严重危害了人们的财产安全、数据隐私，甚至对社会和国家稳定都带来了不可忽视的影响。如何从根本上解决网络安全问题已经成为各个国家的核心战略计划。

正如第8章中提到的，网络攻击的根本原因是源地址极易被伪造。本章针对这一问题，介绍真实源地址验证SAVA体系结构与关键技术，从根本上避免源地址被攻击者伪造，从而阻断网络攻击。全章分为三节，第一节介绍发展真实源地址验证SAVA体系结构的原因和必要性；第二节从关键的设计原则出发介绍了真实源地址验证SAVA体系结构；第三节通过一些实例介绍了真实源地址验证SAVA体系结构在演进过程中围绕分层优化、兼容性、可扩展性、安全性做出的新发展。表10.1为本章的主要内容及知识框架。

表10.1 真实源地址验证SAVA体系结构与关键技术

|  |  |  |
| --- | --- | --- |
| **SAVA体系结构** | **知识点** | **概要** |
| 设计背景 | * 网络攻击频发原因 * 当前互联网体系结构脆弱性 | 当今互联网体系结构缺乏安全可信基础，存在诸多脆弱性，为网络攻击供了可乘之机 |
| 设计原则 | * 已有源地址验证技术问题 * 合适的真实地址验证粒度划分标准 * 合理的真实地址寻址问题分层结构及层间关系 * 有效的真实地址寻址部署激励机制 | SAVA的设计从体系结构入手，结合三个设计需求，具有简单，松耦合，多重防御，支持增量部署，便于对上层可信任应用提供支持，和激励运营商部署的新特点 |
| 演变原则 | * 分层优化 * 兼容性 * 可扩展性 * 安全性 | 为提高SAVA的可用性与效率，接入网、域内、域间技术都围绕分层优化、兼容性、可扩展性、安全性进行技术演进 |

引言

根据互联网世界统计（Internet World Stats，简称IWS）数据统计显示，截至2020年6月，全球互联网用户数量达到46.48亿人，占世界人口的比重达到59.6%。从最初服务于简单的资源共享，到如今社交网络、物联网、云计算等新的概念不断出现，互联网的功能愈加丰富，也逐渐成为人们日常生活中密不可分的一部分。互联网经过50多年的发展，已成为人类社会的重要基础设施和国家的重要战略资源。

随着互联网的重要性不断加深，网络攻击所带来的危害也日益增大。常见的攻击类型包括数据泄露攻击、网页篡改攻击、DDoS攻击、钓鱼攻击等，这些攻击给个人、企业、政府带来了严重的经济损失，一些针对政府的网络攻击甚至影响了国家的发展，使得世界格局动荡不安。因此在互联网飞速发展的今天，网络空间安全越发得到全世界各国的重视。

目前对于网络攻击的防御大多都属于修补型防御，这些防御措施在解决网络攻击的同时，可能会给互联网带来沉重的负担，甚至引入新的不安全因素。如果想从根本上解决网络攻击问题，必须探究其发生的根源，进而从根源入手进行防御。本章接下来就首先剖析网络攻击频发的根本原因，进而带大家走入真实源地址验证SAVA体系结构的设计。

### 10.1 真实源地址验证体系结构背景

当前网络攻击频发严重影响社会、国家的稳定与发展。针对当今网络攻击频发的问题，互联网图灵奖获得者、互联网之父Vinton Cerf指出根本原因是当前的互联网体系结构缺乏安全可信基础。本章首先解释了为什么当前互联网体系结构缺乏安全可信基础，以及由此带来的脆弱性表现，最后引出建设真实源地址验证体系结构的必要性。

#### 10.1.1 当前互联网体系结构缺乏安全可信基础

互联网的前身是ARPAnet，该网络是1969年11月由美国国防部高级研究计划管理局（Advanced Research Projects Agency，ARPA）开始建设，最初节点只有四个，分别是洛杉矶的加利福尼亚州大学洛杉矶分校、加州大学圣巴巴拉分校、斯坦福大学、犹他大学四所大学的4台大型计算机，建设的目的是便于这些学校之间互相共享资源，因此早期互联网的节点之间是彼此信任的。后期随着TCP/IP协议的出现，越来越多的个人、组织加入到了互联网中，互联网的节点数逐渐增长，网络结构越发复杂，节点之间逐渐丧失了信任。

所以由于当前互联网体系结构设计之初多依赖于节点彼此信任，没有考虑到网络规模的爆炸式增长以及网络应用的日趋多元化导致信任面逐渐缺少，由此带来的一些结构性安全隐患开始频繁出现。下一节我们进一步阐述当前互联网体系结构以及其具体脆弱性表现。

#### 10.1.2 当前互联网体系结构脆弱性表现

互联网体系结构是通信系统的基础和核心，它对网络中通信系统的功能组织和通信规则进行了定义。现有互联网体系结构如图10.1所示，是一个窄腰的结构。链路层和物理层进行底层数据报文传输；网络层承上启下，运行IP协议，保证整个网络四通八达，是整个体系结构的核心；应用层在传输层和网络层的基础上运行各种应用协议，支撑丰富的网络的应用。

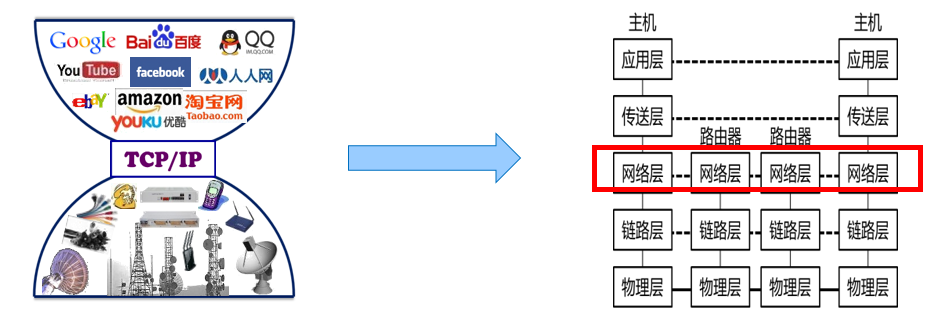


图10.1 当今互联网体系结构

现有的互联网体系结构是一种面向服务和性能的设计，基于特定的应用场景和设计初衷，缺乏基本的安全需求考虑和安全设计，其脆弱性表现在以下三个方面。

1、IP地址易被伪造

路由设备只基于报文的目的IP地址对报文进行转发，而不对转发报文源地址的真实性进行任何验证。随着互联网越来越开放，网络成员的可信性无法得到保证，而报文源IP地址的真实性难以验证。IP协议是互联网的核心协议，源IP地址真实性的缺失影响到互联网体系结构的各个层面。例如，基于IP协议的许多协议（例如TCP，UDP等）使用IP地址这个并不安全的标识作为通讯对方的标识，因而只要伪造了源地址，相应地就欺骗了这些协议，这使得伪造源地址攻击的能力超出网络层范围，危害到其它层的协议。利用源地址伪造的手段，网络攻击的发起者可以隐匿自己的身份和位置，逃避法律的制裁。使用伪造的源地址的网络攻击行为难以被追溯，这是当前伪造源地址行为泛滥的原因。随着源地址伪造手段的大量使用，基于真实地址的网络计费、管理、监控和安全认证等都无法正常进行，对互联网基础设施和上层应用都造成了严重的危害。

2、数据转发易受攻击

数据包从源主机发出，经由十几个路由器转发，最终达到目的主机。数据包承载了源主机和目的主机之间的数据信息，当数据包经过恶意节点时，恶意节点可以实现中间人攻击，或者收集数据信息，造成隐私泄露。即使原本路径不经过恶意节点，恶意节点也可能通过通报不正确的路由信息，使得相应的数据包经由自己转发，从而完成网络攻击。当今互联网体系结构无法对数据包的转发路径进行验证和追溯，无法对中间节点的行为造成约束，因此当数据转发受到攻击时，很难定位到恶意节点。

3、网络安全基础设施存在单点信任风险

节点彼此信任构成早期互联网的信任面，如今网络安全基础设施为当今互联网提供了信任面支撑，而其中大部分网络安全基础设施都是基于中心化的体系架构，例如公钥基础设施（Public Key Infrastructure，PKI）和资源公钥基础设施（Resource PKI，RPKI）。然而，作为许多现有网络安全技术的核心，这些基础设施却暴露出了严重的信任问题，如荷兰安全证书提供商DigiNotar曾遭受入侵，为超过500个网站发布恶意证书；证书颁发机构赛门铁克误发超过三万个证书扩展凭证等……这些安全事件表明，一旦这些基础设施发生问题，将对整个互联网造成严重的影响。

通过以上分析，当今互联网体系结构存在诸多脆弱性，为网络攻击供了可乘之机。如果想从根本上解决网络安全问题，关键是增补安全可信基础，弥补上述脆弱性，保证源地址的真实可信、数据转发真实可信、网络安全基础设施稳定，设计并建设真实可信的互联网体系结构[1]。本章着重介绍保证源地址真实可信的真实源地址认证技术。

### 10.2 真实源地址认证SAVA体系结构设计

针对当前互联网体系结构的脆弱性，已经有大量研究工作从各个层次保证源地址的真实可信，具体如表10.2所示。但是这些技术存在一些不足，比如算法复杂协议开销大、缺乏部署激励、完备性不足、可扩展性不足等[2]。此外现有的IP源地址验证方案，相互独立，只能部分地解决源地址验证的问题，没有形成一个完整的覆盖整个网络的整体结构。此外，从体系结构的角度出发解决假冒源地址问题，既能从整体上与现在互联网运行管理体系相适应，又能够分而治之。

现有方案主要针对现有IPv4的网络设计，由于IPv4网络已经实现部署多年，大规模修改网络核心设备，增加真实地址访问的实现机制已不可行。而IPv6下一代互联网的更新换代为我们提供了研究、实现和部署的历史机遇。基于IPV6设计真实可信的互联网体系结构需满足以下要求。

表10.2 已有真实源地址验证技术

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 类别 | | 名称 | 说明 | 不足 |
| 接入网内 | 端口绑定类 | IP Source Guard | 监听DHCP报文或基于手动绑定，建立地址和交换机端口之间的绑定关系 | 不能用于IPv6环境 |
| 基于EAP扩展 | 对用户进行认证的同时，向用户分配地址，并将此地址绑定到交换机的端口 | 不兼容现有的地址分配方式 |
| Ethane | 地址和用户身份的绑定关系 | 不适于现有网络 |
| 自验证 | CGA[3] | 利用密码学中的自验证技术产生地址（IPv6地址）和验证地址的技术 | 对网络设备有较多的修改需求 |
| 端到端 | SAV-Edge | 基于会话密钥生成报文内容哈希值 | 修改主机操作系统协议栈，部署额外的验证设备 |
| 域内 | uRPF[4] 、ACL 、SAVO等 | | 对来自其它子网及本子网的报文源地址进行验证 | 存在验证效果、实用性、适应性等问题 |
| 域间 | Ingress Filtering[5] 、SPM[6] 、DPF[7] | | 过滤来自这个网络的、但是源地址却不属于这个网络的报文的技术 | 配置过于复杂 |
| 其它 | IPsec、HCF、SAVE[8] 、HIP[9]、AIP[10]、APIP、Packet Passports[11] | | 部署在多层次的源地址验证 | 存在开销、兼容性等系列问题 |

#### 10.2.1 合适的真实地址验证粒度划分标准

网络在可部署性上并不是均匀的，在部分区域，能够做到主机粒度的验证，但是很多区域却很难控制。尽管希望能够达到全局的主机粒度的源地址验证，但是考虑到实际部署的限制，达到这个目标是不现实的。而全部采用粗粒度的源地址验证，则无法满足部分区域对细粒度源地址验证的需求。为此，需要划分可变的源地址验证粒度，满足不同部署区域的需求。但是确定合适的源地址验证的粒度，需要找到可靠的依据，才能符合实际的部署需求。

源地址在分配上是存在层次性的。自治域从RIR获取多个前缀，而这些前缀在被拆分为更细粒度的前缀之后被分配到自治域内的各个子网。主机在使用地址时，需要从所接入的子网获取地址。SAVA体系结构按照地址分配的粒度，将源地址验证划分为自治域、前缀、主机这三个粒度，在三个粒度上分别解决源地址验证问题。

#### 10.2.2 合理的真实地址寻址问题分层结构及层间关系

尽管IP网络是一个扁平化的结构，但是扁平的源地址验证结构会导致严重的可扩展性问题，因为这时需要每一个验证实体具备所有对等实体的信息来完成验证，而IP地址的数量是非常巨大的。为此，需要层次化地解决这一问题，使得整个结构具有可扩展性。此外，需要寻找合理的层次间关系，使得各层之间可以共同协作，同时避免层次之间的过渡依赖。

SAVA体系结构根据网络管理的层次性，将源地址验证划分为域间、域内、接入网三个层次，并形成松耦合的层间关系，以利于方案的部署。

#### 10.2.3 有效的真实地址寻址部署激励机制

源地址验证的一个核心问题就是方案要能够提供明确的激励。缺乏激励的方案是难以被部署的。一个难点是，如何找到运营者真正关心的问题，提供真实有效的激励。

SAVA体系结构根据运营者在三个层面上关注的重点不同，在各个层面提供满足相应需求的方案，以提供部署所需要的激励。具体而言，SAVA体系结构在接入层面提供主机粒度的源地址验证能力，以保证地址使用的可追溯性；在域内层面提供前缀级别的保护能力，以保护核心设备不被攻击；在自治域间层面提供自治域级别的联盟内可验证能力以及保护自身不被伪造的能力。

结合以上三个设计需求，最终真实源地址验证体系结构SAVA如图10.2所示[12]。其中接入子网内真实地址方法保证主机只使用在合法地址分配过程中获得的地址[13]，域内真实地址方法实现地址前缀级的真实地址验证功能，域间真实地址方法实现AS粒度的真实地址验证功能[14]。真实源地址验证体系结构SAVA，具有简单，松耦合，多重防御，支持增量部署，便于对上层可信任应用提供支持，和激励运营商部署的新特点。

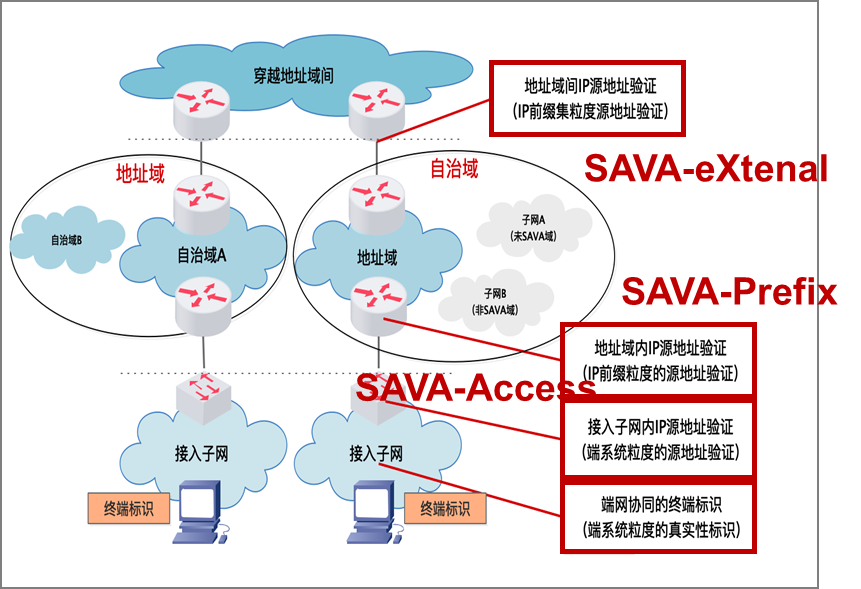


图10.2真实源地址验证体系结构SAVA

### 10.3 真实源地址验证SAVA体系结构演进

真实可信互联网SAVA体系结构既不属于简单改良型的下一代互联网体系结构，也不属于完全革新型的下一代互联网体系结构，其属于可演进的互联网体系结构，需要在保持原有体系结构完整性的前提下，以最小代价不断适应新的需求变化。随着真实可信互联网SAVA体系结构逐渐从设计走向应用，为提高SAVA的可用性与效率，无论是整体的体系结构设计还是接入网、域内、域间真实源地址验证技术都有了更高的发展需求，SAVA整体围绕分层优化、兼容性、可扩展性、安全性进行技术演进。

#### 10.3.1 分层优化

分层优化一直是网络领域重要的优化方式，比如OSI七层模型，TCP/IP四层模型等。分层具有灵活性好、结构上可分割、易于实现、维护和标准化等优点，各层之间只需要按协议进行简单交互而不用关注对方实现细节，大大提升了体系的效率。下面通过SAVA域内分布式路由同步以及域间层次化联盟两个实例来说明SAVA演进中的分层优化。

1、域内分布式路由同步

域内源地址验证最常用的方法是uRPF协议。路由器uRPF对进入的数据包进行源地址的检查，检查的两个条件一是是否有到源IP的路由，二是IP包是否是从路由表中到源IP的下一跳对应的接口接收到，即需要IP出入端口一致。而实际上网络中路由对称是无法保证的，因此第二个条件是比较严格的，可能过滤掉一些真实的数据包。如何对数据包进入的端口是否合理进行精确的判断是困难的。

解决这一问题的方式是设计分布式路由同步，综合多个路由器视角，建立全局过滤规则，如图10.3所示。首先划分底层管理域和高层管理域，然后扩展路由协议，使其支持在路由转发信息内携带唯一标识属于低层地址域的前缀信息，高层地址域边界设备之间进行路由同步，识别低层地址域的全部前缀信息。这样就实现了可扩展、低时延、高准确率的地址域内前缀粒度真实源地址验证。

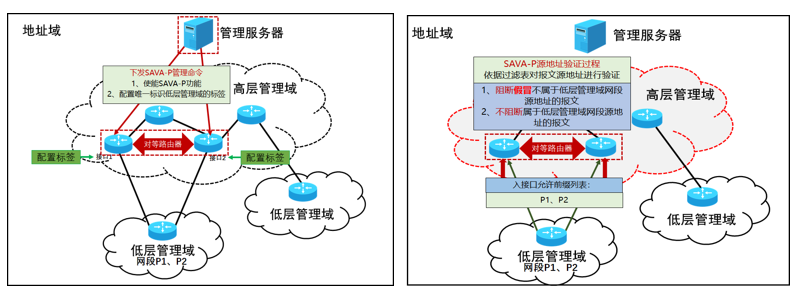


图10.3 分布式路由同步

2、域间层次化联盟

传统的域间源地址验证技术需要每个自治域协商并维护一个标签，随着自治域数目上升，维护同所有自治域的标签是十分耗费资源而且是不现实的。因此SAVA域间逐渐采用层次化联盟的方式（如图10.4所示），立足实际网络拓扑结构和域间路由机制,通过分层将部署了验证机制的所有自治域划分成多级联盟，每一级联盟可以作为成员(抽象为一个系统整体)自下而上的参加更高级别的信任联盟,形成一种多级并存的、层次化的信任联盟体系结构,通过引入实现标签替换的“中继代理”TAE(联盟边界)将每一层级联盟和外界网络隔离，在确保域间高速通信的同时使得下层联盟和更高层联盟内部的网络环境彼此互不可见、互无影响，有效降低了边界路由设备状态机存储、查找、同步和处理等验证开销,即使在规模较大的层次结构中仍然能保证验证的有效性和简单化，着力体现“先部署先受益”的特点，具有一定的增量部署激励。

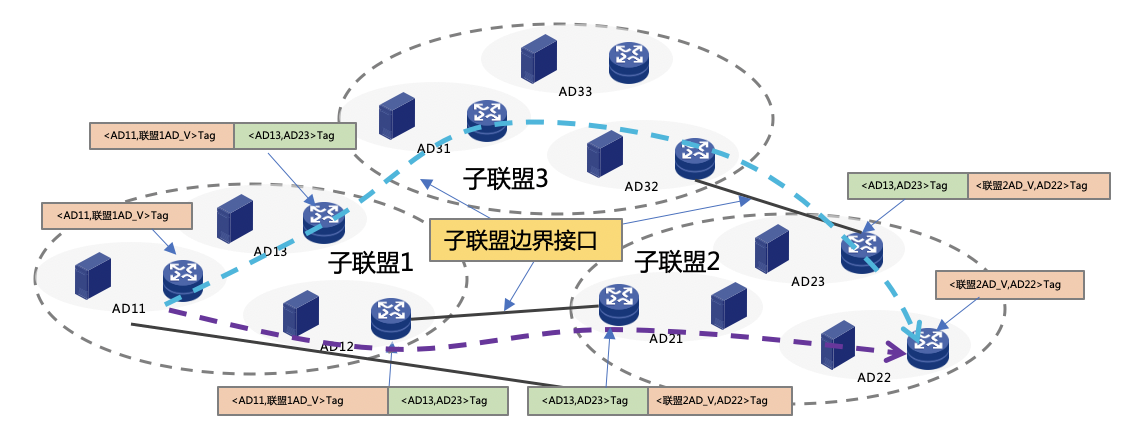


图10.4 域间层次化联盟

#### 10.3.2 兼容性

SAVA体系结构是对现有体系结构的改良，整体的技术依附于现有体系结构实现，因此必须要求技术对应协议与现有体系结构协议兼容，同时SAVA的部署是一个持续性的过程，需要考虑在发展部署的过渡阶段SAVA自身的兼容性。下面通过自适应的地址分配报文监听机制和地址域概念来说明SAVA演进中的兼容性。

1、自适应的地址分配报文监听机制

接入网是异构多样的。首先接入网中接入的终端包括手机、电脑、服务器、嵌入式设备等各种类型设备，即使同一种设备，其上运行的系统也可能不同，比如手机可能是安卓系统，也可能是IOS系统。再者IP地址的分配也是多种多样的，比如DHCP协议分配、SLAAC协议分配、静态配置等。这需要有对终端协议栈透明的普适的验证机制。最后接入网的接入方式也是多样的，包括有线、无线等，不同接入模式可用的绑定锚差别大，难以统一。

针对多种接入网技术、多种地址分配方式、多种终端类型的多模异构复杂环境，基于强认证的绑定锚，SAVA采用自动监听控制报文的学习算法[15][16]，同步获取地址分配表（如图10.5所示），解决多模异构场景下同步获取单个地址进行验证并且无漏判的难题，实现了地址级的无漏判源地址验证，并且通过将设备标识与合法IP地址关联，达到了端网协同的目标，同时也实现了接入网兼容性。

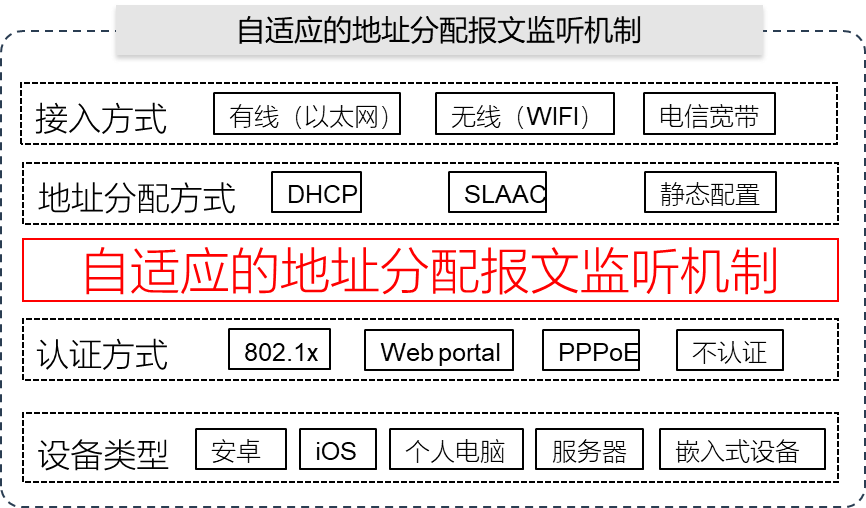


图10.5 自适应的地址分配报文监听机制

2、地址域概念

当SAVA处于发展过渡阶段时，经常出现一个自治域中部分子网部署了SAVA，而剩余子网尚未部署SAVA的情形，也就是出现了SAVA部署与地址管理范围的失配，如图10.6所示。这时候以自治域为力度进行真实源地址验证就不再合适。因此需要灵活定义“地址域”保障部署范围与管理范围的一致。

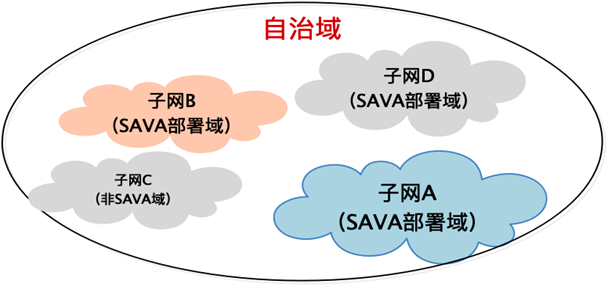


图10.6 SAVA部署与地址管理范围的失配

地址域定义为同一机构所属的全部IP地址中的可部分管理范围，“地址域”显著提升体系结构的灵活性，实现了部署结构灵活的源地址真实性验证体系结构。面向地址域的新型源地址验证体系结构分为接入网、地址域内和地址域间三层结构，具有松耦合、多重防御、支持增量部署等优点，如图10.2所示。

#### 10.3.3 可扩展性

SAVA体系结构是可演进型的体系结构，除了与现有协议兼容外，同时也关注体系结构的可扩展性，以适应复杂的网络环境以及新的需求。下面通过统一的跨域终端标识来说明SAVA演进过程中的可扩展性。

1、统一的跨域终端标识

网络中存在多个管理域，整个网络的管理天然是分布式的，每个管理域可能独自设计真实可验证的终端标识，造成终端标识的跨域有效性降低。因此必须设计统一的终端标识。

关于真实身份嵌入的现已有的解决方案有HIP、SSL、Web认证、NBIOT/5G等。这些技术在适用范围、安全性、部署难度方面都存在各种各样的问题。SAVA在SAVI技术保障接入网内设备的IP地址真实不可伪造的基础上，真实身份技术通过利用IPv6地址强大的语义表达能力，将IPv6地址后64的设备标识符替换为可信设备标识符（如下图10.7所示），以此做到在部署子网内所有流量所有数据包的源端身份可信可追溯，增强了终端标识的可扩展性。可信设备标识符兼顾多种IPv6地址分配机制和组网环境，将端设备信息携带于数据包中，实现了端网协同的真实用户身份识别和溯源。

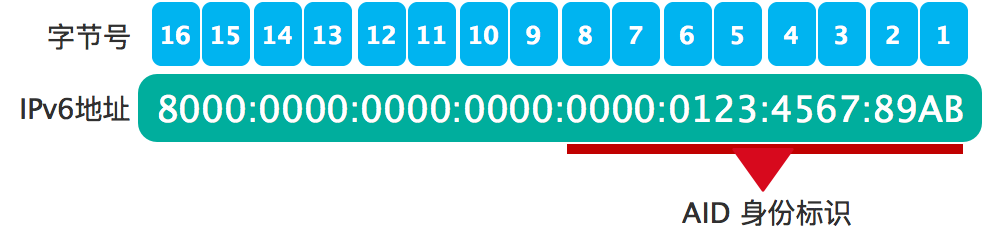


图10.7 真实身份嵌入IPv6地址

#### 10.3.4 安全性

SAVA体系结构的目标是构建真实可信的互联网体系结构，通过协议将安全性赋予现有体系结构，弥补信任面缺少的问题。换个角度保障SAVA自身的安全性是至关重要的，不能在对现有体系机构改良的同时引入新的不安全因素。下面从数据包防篡改机制来说明SAVA演进中的安全性。

1、数据包防篡改机制

SAVA体系保障真实地址和真实路径，对数据包的源地址以及传输路径都可追溯可验证。但是数据包在域间传递的时候仍有数据包内容被篡改的可能性，因此需要建立数据包防篡改机制。如图10.8所示，利用SMA标签证明源端身份，增加数据包摘要信息共同生存数据包签名，中间节点不具有源端SMA标签，无法伪造数据包签名，这样就防止了其它恶意节点篡改数据包。引入数据包防篡改机制后，真正达到了数据包的地址可信、内容可信，SAVA体系结构进一步增强了现有体系结构的安全性。

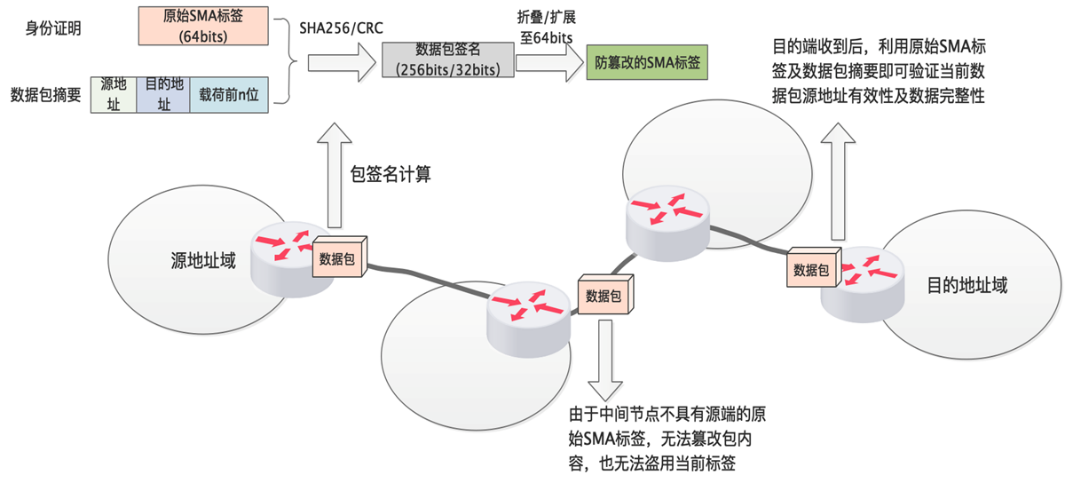


图10.8 数据包防篡改机制

### 10.4 总结

经过十多年的发展，下一代互联网的研究得到了越来越多的关注，发达国家纷纷将网络安全和互联网体系结构的研究纳入相关战略计划。中国在互联网基础研究上仍和发达国家存在差距，互联网核心技术是我们最大的“命门”。近年来，新一代互联网研究已经得到我国政府重视，目前已经在多层次开始推进建设网络安全和互联网体系结构。

真实源地址验证SAVA体系结构在2004年被首次提出，经历原型开发，2008年制定我国首个实验类IETF国际标准RFC 5210，到2012年形成了SAVA的初步框架。2012年后在接入、域内、域间关键技术上实现了重大突破，比如多域协作信任的域间机制等，形成了一系列的国际标准（RFC 7039、7513、7856等）。除了理论和技术突破外，SAVA在产品化和应用方面也取得了长足进步。清华大学与华为、新华三、中兴合作，形成覆盖接入网、域内、域间的全系列50余种网络产品和系统，成果在CNGI-CERNET2以及中国电信、中国移动等运营商网络和中石油、湖北地税等行业网络得到大规模应用。真实源地址验证SAVA体系结构产学研用相结合，在安全可信方面掌握了核心技术，在国际竞争中具备了先发优势，将有力支撑我国下一代互联网技术产业发展。

### 参考文献

1. Wu JP, Wu Q, Xu K. Research and Exploration of Next—Generation Internet Architecture. Chinese Journal of Computer, 2008,31(9):1536−1548
2. Xu K, Zhu L, Zhu M. Architecture and key technologies of internet address security. Journal of Software, 2014,25(1):78-97
3. Rafiee H, Loewis MV, Meinel C. Transaction SIGnature (TSIG) using CGA algorithm in IPv6. Internet draft, 2013
4. Ferguson P, Senie D. Network ingress filtering. RFC 2827, 2000
5. Baker F, Savola P. Ingress filtering for multihomed networks. RFC 3704, 2004
6. Bremler-Barr A, Levy H. Brief announcement: Spoofing prevention method. In: Proc. of the PODC 2004. Newfoundland: ACM Press, 2004. 375−375.
7. Park K, Lee H. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets. In:Proc. of the ACM SIGCOMM 2001. New York: ACM Press, 2001. 15−26
8. Li J, Mirkovic J, Wang MQ, Reiher P, Zhang LX. SAVE: Source address validity enforcement protocol. In: Proc. of the InfoCom 2002. New York: IEEE, 2002. 1557−1566
9. Moskowitz R, Hirschmann V, Jokela P, Henderson T. Host Identity Protocol. RFC5201, 2013
10. Andersen DG, Balakrishnan H, Feamster N, Koponen T, Moon D, Shenker S. Accountable Internet protocol (AIP). In: Proc. of the SIGCOMM 2008. New York: ACM Press, 2008. 339−350.
11. Liu X, Li A, Yang XW, Wetherall D. Passport: Secure and adoptable source authentication. In: Proc. of the NSDI 2008. San Francisco: USENIX Association, 2008. 365−378
12. J. Wu, J. Bi, X. Li, et al. Source Address Validation Architecture (SAVA）Testbed and Deployment Experience. RFC5210, 2008
13. J. Wu, J. Bi, M. Bagnulo, et al. Source Address Validation Improvement (SAVI) Framework. RFC7039, 2013
14. Liu BY, Bi J. SMA: State Machine based Anti-spoofing[OL]
15. J. Bi, J. Wu, G. Yao, et al. Source Address Validation Improvement (SAVI) Solution for DHCP. RFC7513, 2015
16. J. Bi, G. Yao, J. Halpern, et al. Source Address Validation Improvement (SAVI) for Mixed Address Assignment Methods Scenario. RFC8074, 2015