Hidasav:一种层次化的域间真实源地址验证方法

李 杰[1),2)] 吴建平[1)] 徐 恪[1)] 陈文龙[3)]

[1)](清华大学计算机科学与技术系 北京 100084)

[2)](国防信息学院 武汉 430010)

[3)](北京科技大学信息工程学院 北京 100083)

摘 要 可信任是下一代互联网的重要特征,真实地址访问是可信任的基础和前提.自治域级真实地址访问是整个可信任互联网体系结构中最为复杂的一个层次.基于标签的源地址验证不受拓扑结构影响,无需中间节点特殊处理,是实现域间真实地址访问的有效方法.然而,现有方法中信任联盟过于扁平化和单一化的问题导致验证开销随联盟规模增大而急剧增大,影响和制约了机制的可扩展性和过滤能力,难以进行增量部署.对此,文中提出了一种层次化的基于标签替换的域间真实源地址验证方法(Hidasav),该方法通过合理规划联盟层次和聚类整合,构建出一种多级并存的信任联盟体系结构,通过引入实现轻量级标签替换的联盟边界,将每一层级联盟和外界网络隔离,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.与现有同类典型方法在CNGI真实环境中的实验结果比较表明,该方法能够在确保域间高速通信的同时有效降低边界路由设备的状态机存储、更新和报文验证开销.

关键词 层次化;自治域间;IP地址验证;网络安全

中图法分类号 TP393 **DOI号**:10.3724/SP.J.1016.2012.00085

An Hierarchical Inter-Domain Authenticated Source Address Validation Solution

LI Jie[1),2)] WU Jian-Ping[1)] XU Ke[1)] CHEN Wen-Long[3)]

[1)](*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084)

[2)](*National Academy of Defense Information, Wuhan* 430010)

[3)](*School of Information Engineering, University of Science and Technology Beijing, Beijing* 100083)

Abstract Next generation Internet is highly concerned with the issue of trustworthy. An important foundation of trustworthy is authentication of the source IP address. With existing signature-and-verification based defense mechanisms, there is a lack of hierarchical architecture, which makes the structure of the trust alliance excessively flat and single. Moreover, with the increasing scale of trust alliances, costs of validation grow so quickly that they do not adapt to incremental deployment. Via comparing with traditional solutions, this paper proposes a hierarchical, inter-domain authenticated source address validation solution named Hidasav. Hidasav employs two intelligent designs: lightweight tag replacement and a hierarchical partitioning scheme, each of which helps to ensure that Hidasav can construct trustworthy and hierarchical trust alliances without the negative influences and complex operations on de facto networks. Experiments in CNGI also indicate that Hidasav can effectively obtain the design goals of a hierarchical architecture, along with lightweight, loose coupling and "multi-fence support" as well as supporting incremental deployment.

Keywords hierarchical; inter domain; IPv6 source address validation; network security

收稿日期:2010-10-22;最终修改稿收到日期:2011-10-25.本课题得到国家"十一五"科技支撑计划课题(2008BAH37B02)、国家"九七三"重点基础研究发展规划项目(2009CB320501)、国家"八六三"高技术研究发展计划重大课题(2008AA01A326,2009AA01A334)资助.
李 杰,男,1979年生,博士,主要研究方向为下一代互联网体系结构、域间真实源地址验证.E-mail:jieli@csnet1.cs.tsinghua.edu.cn.**吴建平**,男,1953年生,博士,教授,博士生导师,中国计算机学会(CCF)高级会员,主要研究领域为下一代互联网体系结构、网络协议工程学.**徐 恪**,男,1974年生,博士,教授,博士生导师,中国计算机学会(CCF)高级会员,主要研究领域为下一代互联网体系结构、交换和路由体系结构.**陈文龙**,男,1976年生,博士,主要研究方向为网络体系结构、网络协议.

1 引 言

可信任是下一代互联网的重要特征,其内涵是下一代互联网在开放、简单的技术基础上,以安全性、真实性、可审计性、私密性、抗毁性和可控性为主要特性,建立完备的安全保障体系,从网络体系结构上保证网络信息的真实和可追溯,进而提供安全可信的网络服务和应用.从可信任的角度出发,真实IP地址访问的问题实际上是地址的归属关系问题:网络实体发出的报文只应携带它拥有的地址,报文只应被拥有其源地址的实体发出,真实源IP地址验证则是对实体发出的报文进行检验和追溯进而确保实体本身、信息来源、信息内容的真实性.当前的互联网,报文转发的基本依据是目的IP地址,一般不对报文的源IP地址做真实性检查,导致其易被伪造,接收方不能判别报文源IP地址的真实性,也就无法确定报文是否来自真实的发送方.因此,目前的网络服务只是停留在尽力而为地向目的端转发的层次,而达不到确保源端可信的高度.

随着互联网规模的日益拓展和商业应用的日益丰富,网络用户的成分变得异常复杂,来自某些高级用户的恶意攻击常常是通过伪造报文的源IP地址来实施的,伪造的源IP地址同时又为恶意攻击者隐匿真实身份、逃避制裁提供了温床,并由此引发了很多安全、管理和计费问题.例如DoS[1]/DDoS攻击[2]、僵尸网络(Botnet)[3]、垃圾流量(SPAM)[4]等等,目前已有许多研究工作是就它们展开的[5-10].当前,源IP地址的真实性验证已给互联网的安全运营和可持续发展提出了诸多挑战.致力于互联网的长远利益,互联网只有提供高度可信的网络服务,才能满足未来发展的需求.因此,确保源IP地址的真实性是实现可信任下一代互联网的核心问题.

自治域间真实源地址验证是整个可信任互联网体系结构中最为复杂的一个层次.自治域间真实源地址验证方法旨在实现自治域粒度的真实源地址验证,其特点是:能够在不同自治域间协同工作;机制必须简单轻权,不给域间高速通信带来明显影响.然而,现有的域间真实源地址验证方法存在诸多不足.典型的有Bremler-Barr等人[11]提出的基于源-目的自治域对应密钥的域间IP欺骗过滤机制SPM,能够过滤自治域间IP欺骗报文,保护本域范围网络用户.然而密钥的管理、协商和同步引入了较大的通信开销,降低了验证性能,增大了验证复杂度.Shen等人[12]借鉴SPM的加密认证机制,提出了基于标签的域间真实源地址验证方法(APPA).参与的自治域构建信任联盟,联盟内源和目的自治域间通过状态机来生成用于源地址检查的轻量级标签,标签随着状态的变迁而自动更新,从而减小了标签管理、协商和同步等通信开销,同时加快了标签更新的频率和速度,进一步提高了安全性能.但是,过于扁平化和单一化的信任联盟体系结构导致了状态机存储和处理等验证开销随联盟规模增大而急剧增大,影响和制约了机制的可扩展性和过滤能力,难以适应增量部署.

对此,本文提出了层次化的基于标签替换的自治域间真实源地址验证方法(Hidasav).与传统的扁平化的基于标签的验证方法相比,本方法着力解决了以下3个方面的问题:(1)通过分层,改变传统方法中扁平的、单一的信任联盟体系结构,构建了新型的多级共存的、层次化的体系结构,避免了联盟成员间建立不必要的全连接的状态机双向共享关系和覆盖全局的前缀和自治域对应信息,实现了验证机制的简化;(2)通过引入实现标签替换的"中继代理"——联盟边界,将每一层级联盟和外界网络隔离,使得不同层级联盟内部网络环境彼此互不可见,在确保域间高速通信的同时排除了拓扑结构和成员变化(加入和退出)带来的影响,有效控制了验证规则信息更新的范围和频度;(3)减少了用于标签添加、替换和验证的状态机的数量,降低了边界路由设备的状态机存储和更新开销,缩减了数据报文验证开销.实验证明,本方法在规模较大的层次化信任联盟体系结构中仍能保证验证的简单、轻权、有效,具备"先部署先受益"的激励机制,可以实现增量部署.

第2节介绍问题的研究背景和相关工作;第3节回顾基于标签的域间真实源地址验证方法的基本思想;第4节阐述Hidasav的设计原理;第5节描述Hidasav构建的层次化信任联盟的体系结构并详细论述验证机制的实现;第6节对本方法的有效性进行分析并通过实验论证本方法的性能;第7节总结全文.

2 相关研究

近年来,在源地址验证研究领域,国际学术界和工业界已做出了许多研究工作,概括起来可分为3类:基于追踪的方法、基于过滤的方法和基于加密认

证的方法.

基于追踪的方法的核心思想是对伪造报文的传输进行全程跟踪，解析其相应的转发路由，最终追溯和定位报文的真实发送源. 依据追踪过程中对相关信息的记录方式，基于追踪的方法可分为 3 类：(1) 将报文传输途径的路由器信息记录在报文头的某一区段，主要有 PPM[13] 和 DPM[14]. 该类方法的局限性体现在只能追踪流量规模较大的报文流；(2) 在路由器上追踪记录一定时间间隔内经过的报文的部分信息，主要有 SPIE[15]. 该类方法的局限性体现在给路由器带来庞杂的计算和存储开销；(3) 利用 ICMP 消息报文存储报文转发路由路径，主要有 iTrace[16] 和 iTrace-CP[17]. 该类方法的局限性体现在实施追溯时无法有效避免 ICMP 协议本身的缺陷即 ICMP 报文易被伪造和匿名攻击. 从根本上讲，基于追踪的方法强调一种事后弥补的被动追溯机制，无法实现在源地址假冒等网络灾害发生前主动性、前瞻性的采取防御.

基于过滤的方法是一种预先处置的方法，该类方法通过预先设定的一些过滤规则检查报文中的某些字段，以验证报文是否来自真实源，将伪造报文过滤在到达接收方之前的网络中. 典型的有 DPF[18]、SAVE[19]、Ingress Filtering[20]、uRPF[21]、HCF[22] 以及基于转发表的过滤方法[23] 等. 基于转发表的过滤方法规定，报文的进入端口必须与源地址的转发端口一致. 然而，网络中报文实际转发路由的不对称性往往导致很多来自真实源地址的合法报文被滤除；uRPF无法解决非对称路由的问题；Ingress Filtering 要求在边界路由器上部署报文过滤器，引入了一定的额外开销，不仅导致网络性能有所下降，而且必须得到设备制造商的支持和各 ISP 间的合作以及广泛部署才会奏效，因此缺乏部署激励. DPF 将验证规则的部署位置从边缘网络延伸到了核心网络且支持增量部署，但代价是需对 BGP 协议进行扩展，当路由动态变化时可能导致滤除合法的报文；SAVE 设计了一种新的协议，在网络中传递源地址验证规则信息，但是协议没有考虑路由系统的层次结构，变化的域内路由可能频繁导致验证规则的更新，增大了通信开销也影响了源地址验证的准确性，并且要求全局部署，使协议的可扩展性受到制约.

基于加密认证的方法引入了一种端到端的加密认证机制，排除了网络拓扑、路由路径的影响，无需中间节点特殊处理. 加密由源自治域端添加认证源真实身份的标签完成. 报文转发至目的自治域端时检查报文携带标签，如果标签验证正确，即把标签从报文中去除并将报文转发给目的主机；如果标签验证不正确，就将报文丢弃. SPM[11] 是一种典型的基于加密认证的自治域端到自治域端的解决方案，每一对互为通信对端的自治域维护一对私密的、唯一的密钥来验证源地址的真实性，源端自治域通过添加密钥可保证源地址的真实性，目的端自治域通过检查密钥可验证源地址的真实性. 到达目的端自治域的报文密钥被验证正确后，即把密钥从报文中去除，若验证不正确，则将报文丢弃. SPM 可实现自治域粒度的真实源地址验证，使得部署 SPM 的自治域可以有效保护本域网络中的用户，具有部署激励. 然而，SPM 密钥的协商、管理和同步需要收发双方频繁进行通信，致使当网络繁忙或遭受 DoS/DDoS 攻击时，其验证性能大幅下降，这也构成制约其推广的软肋. 针对上述问题，APPA[12] 在 SPM 的基础上进行了有益的改进. APPA 的实现思想我们将在第 3 节中简要介绍.

互联网的路由和寻址是一个层次结构，要实现全网的真实源 IP 地址验证，依赖单一的方法，部署在单一层次和位置是不现实的[24]. 为了解决全网真实源 IP 地址问题，清华大学提出了基于真实 IPv6 源地址的网络寻址体系结构(SAVA)[25]，设计和实现了一种包括接入、域内、域间源地址验证 3 个层次的真实 IPv6 源地址网络寻址系统，分别在主机、IP 地址前缀和自治域粒度上保证源 IP 地址的真实性. 其中，域间源地址验证是 SAVA 体系结构中最困难和复杂的部分，根据自治域邻接关系，SAVA 设计了 2 种生成域间验证规则的机制：应用于相邻自治域间的基于路由的机制和应用在非相邻自治域间的基于签名的机制. SAVA 通过 IPv6 源地址验证，为解决下一代互联网的安全隐患提供了重要保证，成为可信任下一代互联网的重要技术基础. 目前，清华大学已在 IETF 完成一项 RFC 标准[26]，提交 3 项标准草案[27-29]，并以此为基础推动 IETF 成立专门工作组 SAVI，使中国参与 IETF 国际标准方面实现了新的突破，产生了重要的国际影响.

3　自治域间源地址验证方法概述

在基于加密认证的方法中，典型的是文献[12]的基于标签的域间真实源地址验证方法，其实现思想是：由部署验证机制的自治域作为成员单位组建一个信任联盟，联盟内每一对互为通信对端的成员

自治域 AS_X 和 AS_Y 都各自维护有一对分别用来生成和验证标签的状态机$\langle AS_X, AS_Y\rangle$和$\langle AS_Y, AS_X\rangle$(状态机的双向有序性),当 AS_X 作为源域时即数据报文源自 AS_X 发往 AS_Y,AS_X 的出口边界路由器依据状态机$\langle AS_X, AS_Y\rangle$生成确保源于本域的数据报文源地址真实性的标签并添加在报文扩展头中,目的域 AS_Y 的入口边界路由器则依据相同的状态机$\langle AS_X, AS_Y\rangle$来验证标签,若验证通过则判定源地址是真实可信的,即数据报文的确源自 AS_X,从而去除标签进一步转发,否则判定该源地址系伪造,数据报文予以丢弃;同样原理,当 AS_Y 作为源域 AS_X 作为目的域时,通信双方的边界路由器依据状态机$\langle AS_Y, AS_X\rangle$来生成和验证标签,从而实现源地址前缀的验证.

该方法的有效实施需要由联盟注册服务器、控制服务器以及边界路由器协同工作来完成,如图 1 所示. 在每一成员域内部,都配属有一台控制服务器,该服务器主要完成以下职能:与注册服务器通信,完成自身注册并获取联盟成员列表以及其它成员域的控制服务器地址列表;与其它控制服务器交换各自所辖的地址前缀信息并协商生成标签所需的状态机;控制本域的边界路由器,配置地址前缀与自治域的映射列表和进出方向的状态机列表,上述环节以下简称"验证规则部署". 在整个信任联盟内部,配属有一台联盟注册服务器,用于动态维护信任联盟全局成员的列表信息,管理和控制成员的加盟及退出,向控制服务器实时发布联盟成员信息. 上述环节以下简称"成员信息管理".

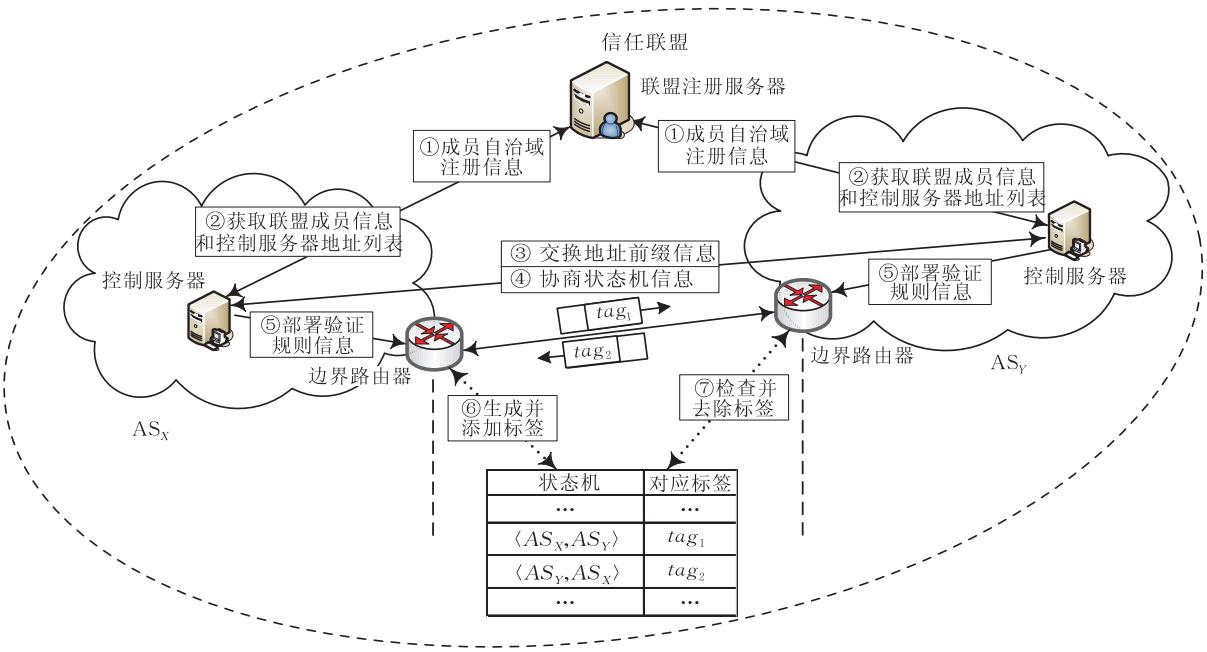

图 1 基于端到端轻量级标签的域间真实源地址验证方法

该方法完善了 SPM 方法的加密认证机制,解决了密钥的协商、管理和同步导致频繁通信的问题,降低了控制服务器之间的通信开销,在确保本域的地址不被伪造的同时还可验证其它来源地址的真实性,具有一定的部署激励. 但是,由于部署该方法的所有自治域同属一个信任联盟,为确保验证机制的有效运转,所有成员间必须建立全连接的状态机双向共享关系和前缀与自治域全局对应信息,由此导致边界路由器必须维护数量庞大的全局验证规则信息才能正确实施验证. 比如,当联盟成员数为 N 时,每一边界路由器需维护的状态机数量达到 $2(N-1)$ 个,状态机存储的空间复杂度达到 $O(N)$ 量级,状态机更新代价达到 $O(N^2)$ 量级. 大数量的状态机加重了路由器存储开销和更新延时,使得状态机的协商和同步难以控制,报文验证延时增大、效率降低,由成员变化带来的影响辐射整个联盟范围. 上述分析表明,导致传统的基于标签的域间真实源地址验证方法难以实现大规模部署的根本问题是:信任联盟体系结构的扁平化和单一化.

4 Hidasav 方法总体设计

针对上述问题,本文在文献[12]的基础上,提出了一种可自下而上分层级建立信任联盟的、基于轻

量级标签替换的自治域间真实源地址验证方法.本节将详细阐述本方法的设计思想以及验证机制.在给出详细的讨论前,首先列出本方法涉及的相关术语和定义,如表1所示.

表1　相关术语和定义对照表

中文	英文	缩写	释义
信任联盟	Trust Alliance	TA	部署了验证机制的成员集合
联盟注册服务器	Registration Server	RES	用以注册、管理联盟列表的服务器(一个信任联盟只配属一个RES)
控制服务器	AS Control Server	ACS	代表本域与联盟注册服务器及其它联盟成员通信的服务器,它还负责对本域所有边界路由器进行配置(在一个信任联盟内,每个联盟成员只配属一个ACS)
边界路由器*	AS Edge Router	AER	具有源地址验证功能的自治域边界路由器(实际中,每个成员自治域可能有多台AER)
联盟边界	Trust Alliance Edge	TAE	隶属于本级联盟且连接联盟外部网络的成员(TAE在联盟构建时会逐一预先确定)
联盟边界路由器*	Trust Alliance Edge Router	TAER	在联盟边界处连接联盟外部网络的出口路由器(实际中,每个TAE可能有多台TAER)
标签	Tag	Tag	添加在IP报文中用以检验源IP地址前缀正确性的字符串
本级联盟状态机	Local Alliance State Machine	LSM	某一子联盟内部成员间用以生成和验证标签序列的状态机(在不同场景中,该联盟可能是由自治域组成的单一联盟,也可能是由子联盟组成的多级联盟)
本级联盟状态机表	Local Alliance State Machine Table	LSMT	用于存储本级联盟状态机的信息表
全局状态机	Global Alliance State Machine	GSM	联盟全局范围内的不同层级联盟成员间用以生成和验证标签序列的状态机
全局状态机表	Global Alliance State Machine Table	GSMT	用于存储全局状态机的信息表
联盟映射状态机	Member vs. Alliance Mapping State Machine	MSM	联盟内某一成员个体与所属联盟整体映射的状态机(双向有序)
联盟映射状态机表	Member vs. Alliance Mapping State Machine Table	MSMT	用于存储联盟映射状态机的信息表

注：* 目前,“可信任下一代互联网关键技术及应用示范研究”课题组已委托设备制造商研制出试商用源地址验证设备AER/TAER,提出了相应的技术规范和标准,并组织技术团队对设备软、硬件进行了系统测试和验收.

4.1　设计目标

本方法的总体设计目标是:遵从系统设计的开放性、简单性原则[30],立足实际网络体系结构,能够分层级构建信任联盟,能够在不同自治域间协调工作,从终端用户的角度使信任联盟的层次化结构趋于透明,它们无需关心验证机制的实现即可受益,从系统设计的角度则需做到异常行为状态可监测、结果可评估、过程可控制[31],以尽量少的通信、存储和处理开销,获得最大限度的验证实效,维护自治域粒度的信任关系和不良行为控制,形成一个高性能的信任系统.具体而言,本方法在实施和技术层面应该包括以下一组设计目标:

(1)优化性能.验证方法应该简单轻权,以尽可能小的路由器存储空间、计算资源和通信开销,获得较高的真实源地址的安全保障[32],不影响交换路由信息和降低路由收敛速度,不给自治域间的高速通信带来明显影响.

(2)安全机制可扩展.验证方法的效能应该与部署规模成正比,能够增强现有规模信任联盟网络主动预防和积极抵御多种攻击、威慑的能力,尽可能地将不信任的访问操作遏制在源端,而且这种能力能够随着机制部署规模的扩大而相应增长,使网络的安全机制具有健壮性和可扩展性,同时还可为其它多种网络应用服务提供安全支持(组播准入控制等)[33].

(3)支持增量部署.验证方法能够提供自治域间端到端的安全服务,必须立足实际网络拓扑结构和域间路由决策机制,验证设备(RES和ACS)的引入既不触及核心网络(设备)也不对边缘网络(设备)做任何改变,无需终端用户和中间节点(报文转发途经的部署或未部署验证机制的节点)特殊处理,只需通过带外接入的方式部署在联盟成员网络边缘,无需进行域间路由协议扩展,对路由协议的稳定性没有负面影响,能够以较小的部署复杂度提供足够充分的信任保障.

(4)松耦合.验证方法的实现能够有效排除实际网络中域间路由变化及非对称路由的影响,不依赖自治域间的邻接关系,部署验证机制的各个自治域相互独立,允许各域依据实际情况(隶属关系、自身策略、网络结构和经济、政治、军事利益)灵活构建多层级的信任联盟;同时还允许各自治域内部灵活实现更细粒度的真实源地址验证,域内外验证系统相互独立,最大限度地保证验证的准确性、严密性和

灵活性.

4.2 基本思想

本方法采用一种基于轻量级标签替换的自治域端到自治域端的加密认证机制,通过自下而上的分层,将部署了本方法的所有自治域(AS)划分为多层级信任联盟,每一层级联盟可以作为成员(抽象为一个系统整体)参加更高层级的联盟,使得整个信任联盟系统构成一种具有源地址验证功能的、层次化的体系结构.我们将在第 5.1 节中给出体系结构的详细阐述.

在数据层面,与扁平化结构中单一的数据通信场景相比,在层次化的信任联盟体系结构中,通过分层数据通信场景被扩展为 3 类:

(1)单一信任联盟数据通信,某一最低层级信任联盟内成员 AS 互为通信对端,报文仅在该联盟内部网络中交互.在此类数据通信场景中,源地址验证过程无需标签替换,只需依据该最低层级联盟状态机,采用传统的验证机制即可有效实现源地址验证;

(2)跨信任联盟数据通信,隶属于不同层级信任联盟的 AS 互为通信对端,数据报文需要在跨越联盟的网络中交互.在此类数据通信场景中,处在不同层级联盟中的源 AS 和目的 AS 间无需通过建立状态机双向共享,而是通过引入 TAE 和联盟映射状态机来实现源地址验证.其原理是:数据报文由源 AS 端 AER 依据联盟映射状态机生成并添加确保源地址真实性的第一个标签,建立最初的信任关系,报文沿着路由协议决策的域间路由正常转发的过程中,在途经第一个 TAE 时,由该处的 TAER 根据联盟映射状态机表和全局状态机表将标签替换成数据报文转发途经的更高层级联盟的标签后向本级联盟外部网络转发,如果报文穿越多个更高层级的联盟,则多次执行上述过程由 TAER 充当跨联盟数据报文交互的"中继代理",完成自下而上的逐级标签替换,延续报文源地址真实性的信任关系,当报文送达目的 AS 所在的各级联盟的 TAE 时,相应地由每一层级的 TAER 对报文进行自上而下的逐级标签替换,直至将数据报文转发至目的 AS 所在最低层级联盟的 TAE,由该处的 TAER 根据联盟映射状态机表进行最后一次标签替换,当报文到达目的 AS 端时由 AER 依据联盟映射状态机进行标签检验和去除,完成源地址验证,验证机制的实现我们将在 5.2 节详细阐述;

(3)非信任联盟数据通信,信任联盟中的 AS 与其它非信任联盟 AS 间进行的数据通信.在此类数据通信场景中无需源地址验证也不涉及标签的任何操作.

在控制层面,本方法借鉴了文献[12]中有关控制层面和数据层面的处理机制,同样需要由 RES、ACS 以及路由设备协同工作来完成验证策略的协商和决策,生成相应的验证控制规则和指令,控制数据报文的验证动作.所不同的是,在我们提出的层次化体系结构中,RES 和 ACS 被赋予新的职能.每一联盟内部均需配属一台 RES,在对下完成本级联盟的成员信息管理的同时,对上还须与其它各层级联盟的 RES 交互成员列表;参与信任联盟的每一自治域均配属一台 ACS,对下须完成本级联盟范围的验证规则部署,对上须与其它层级联盟建立通信,参与更高层级联盟的验证规则部署;ACS 还须接收 AER/TAER 的运行状态汇报.需要说明的是伴随上述过程的实施,所有 TAE 会同时明确自身"中继代理"的职能,TAE 的 ACS 会相应完成对 TAER 的配置.

4.3 安全机制

为有效抵御针对验证规则部署和成员信息管理过程的窃听、截获和破解等安全威胁,增强验证机制的健壮性,本方法着重考虑了以下 4 点设计:(1)状态机的周期自动更替机制.为每一个状态机设置了启用和到期时间,在到期时间来临之后,互为通信对端的源域和目的域必须同步自动完成新旧状态机更替,确保了生成的标签在一定周期内的时效性、唯一性和可靠性,降低了 ACS 之间的通信开销;(2)时间同步.要求 RES 通过 NTP 协议定期向各成员 ACS 发送时间校准报文,由 ACS 实时校准本域 AER/TAER 的时间,同时在各 AER/TAER 上设置一个共享时间片,规定在该时间片内,刚刚到期的标签与新的标签均被认为是有效的,从而确保各成员 AER/TAER 之间的时间同步,进而实现状态机的同步;(3)安全信道.立足现有域间链路,采用开启 TCP 拦截和 Diffie-Hellman 协议结合的方式,通过 TCP 连接建立起验证规则信息交互的安全信道;(4)TAER 工作模式.允许 TAER 在进行标签替换的同时可依据网络安全等级灵活设置工作模式(直接替换模式或替换并验证模式).

5 体系结构与实现

本节介绍层次化信任联盟的体系结构,并通过实例讨论验证涉及的控制层面和数据层面的处理流程.

5.1　体系结构

层次化的域间源地址验证方法允许联盟管理机构依据实际情况，灵活选取不同的划分原则和组合模式构建层次化的信任联盟体系结构. 首先以 AS 为单位成员，将部署本方法的所有 AS 按照相同属性聚合成多个最低层级信任联盟，然后再以这些最低层级信任联盟为单位成员，依据一定的划分原则聚合成更高层级的信任联盟，由此自下而上地不断以同一层级的信任联盟为单位嵌套式聚合，直至形成一个最高层级信任联盟，如图 2 所示. 在层次化的信任联盟体系结构中，进行标签添加、替换和检验的主体是边界路由器，它们区分为 2 类：AER 和 TAER. AER 位于最低层级信任联盟内部，无需进行标签替换，其职责是添加数据报文的第一个标签和完成最后一次标签验证，只需维护最低层级信任联盟成员数量级的状态机有序对和前缀-自治域对应关系等验证规则信息而无需掌握全局情况；TAER 位于联盟边界是连接不同层级联盟的桥梁和纽带，其职责是在跨联盟数据通信时完成数据报文标签的逐级替换，由于处理过程涉及多个层级的信任联盟，因此每一层级的 TAER 必须掌握全局验证规则信息.

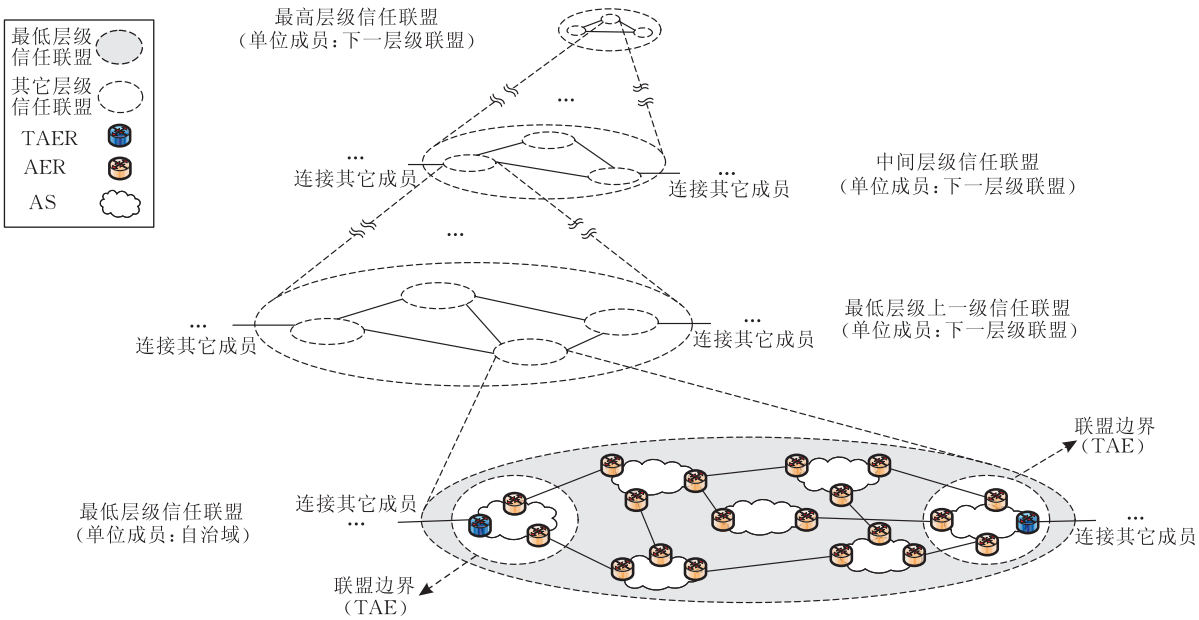

图 2　基于标签替换的域间真实源地址验证方法构建的层次化的信任联盟体系结构

5.2　验证机制实现

下面选取图 2 中的最低层级和其上一级的两层级信任联盟体系结构为例，说明 AER/TAER 如何进行基于标签替换的域间真实源地址验证过程，如图 3 所示. 在以下的讨论中，最低层级信任联盟分别表示为 Sub-TA_1、Sub-TA_2、Sub-TA_3 等，其上一级信任联盟表示为 TA，$\langle AS_X, Sub\text{-}TA_Y\rangle$ 二元组表示成员 AS_X 个体与最低层级联盟 Sub-TA_Y 整体对应的联盟映射状态机，$\langle Sub\text{-}TA_X, Sub\text{-}TA_Y\rangle$ 二元组表示在 TA 中源端成员 Sub-TA_X 与目的端成员 Sub-TA_Y 对应的状态机，$\langle Sub\text{-}TA_X, AS_Y\rangle$ 二元组表示最低层级联盟 Sub-TA_X 整体与成员 AS_Y 个体对应的联盟映射状态机，tag_1 表示由 $\langle AS_X, Sub\text{-}TA_Y\rangle$ 生成的标签，tag_2 表示由 $\langle Sub\text{-}TA_X, Sub\text{-}TA_Y\rangle$ 生成的标签，tag_3 表示由 $\langle Sub\text{-}TA_X, AS_Y\rangle$ 生成的标签，AER_AS_* 表示最低层级信任联盟中某一成员 AS_* 的 AER，TAER_AS_* 表示某一联盟边界 AS_* 中的 TAER，TAER 在进行标签替换时工作模式设置为直接替换模式. 图 3 中，不同灰度的实心圆分别表示 AER 和 TAER，各圆间的连接线标识了各个自治域间建立的 BGP 会话，同时也表示 BGP 决策的从源到目的自治域的域间路由路径. 在以下实例中，RES、ACS 和 AER/TAER 已完成了成员信息管理和验证规则部署等各项初始化阶段工作程序，进入稳定工作状态. 这里，着重说明跨联盟数据通信时数据层面的处理过程，其余 2 种通信场景不再赘述.

1. 源域 AS_X 的 AER_AS_X 收到域内用户发来的数据报文，根据地址前缀与自治域的映射列表对源地址和目的地址依次检查，判定数据报文源地址属于本域（AS_X）、目的地址属于对等联盟 Sub-TA_3 中成员 AS_Y，随即启动如下处理策略：查询 MSMT，定位状态机 $\langle AS_X, Sub\text{-}TA_2\rangle$，生成并添加 tag_1，向本域外部网络转发.

2. 报文转发至中间节点 AS_M 时，该节点根据地址前缀

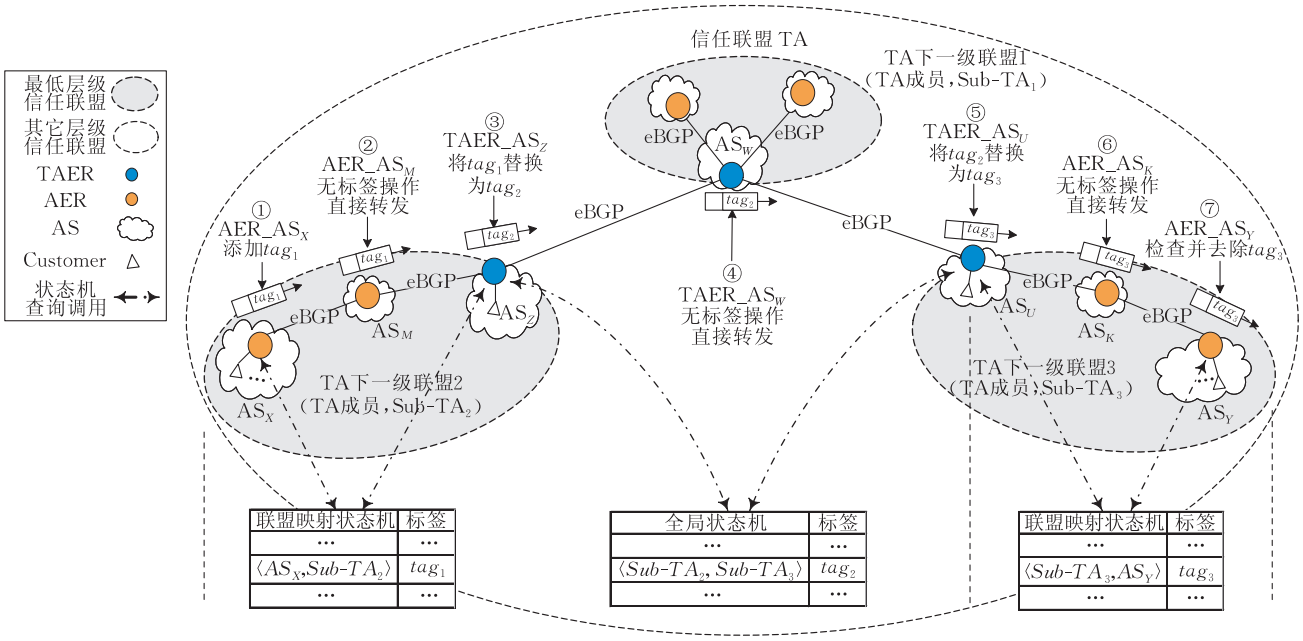

图 3 基于标签替换的域间真实源地址验证方法验证过程

与自治域的映射列表对源地址和目的地址依次检查，当发现报文源地址不属于本域时即停止检查，不对报文做任何处理直接按照目的地址转发至下一跳.

3. 报文转发至路由路径上的第 1 个 TAE 即本级联盟 Sub-TA_2 与外部网络的“中继代理”AS_Z（所有 TAE 事先就已明确自身“中继代理”的职能）处完成第一次标签替换，$TAER\_AS_Z$ 处理策略如下：根据地址前缀与自治域的映射列表对源地址和目的地址依次检查，查询 MSMT 找到对应状态机〈AS_X，$Sub\text{-}TA_2$〉，去除标签 tag_1，紧接着查询 GSMT，定位状态机〈$Sub\text{-}TA_2$，$Sub\text{-}TA_3$〉，生成并添加 tag_2，向本级联盟外部网络转发.

4. 报文转发至中间节点 AS_W 时，该节点不对报文做任何处理，直接按照目的地址转发至下一跳.

5. 报文转发至路由路径上源端所在联盟 Sub-TA_3 的 TAE 即 AS_U 处完成第 2 次标签替换，$TAER\_AS_U$ 处理策略如下：根据地址前缀与自治域的映射列表对源地址和目的地址依次检查，查询 GSMT 找到对应状态机〈$Sub\text{-}TA_2$，$Sub\text{-}TA_3$〉，去除标签 tag_2，紧接着查询 MSMT，定位状态机〈$Sub\text{-}TA_3$，AS_Y〉，生成并添加 tag_3，完成最后一次标签替换，向本级联盟内部网络转发.

6. 报文转发至中间节点 AS_K 时，该节点不对报文做任何处理，直接按照目的地址转发至下一跳.

7. 目的域 AS_Y 的 AER_AS_Y 收到数据报文，根据地址前缀与自治域的映射列表对源地址和目的地址依次检查，判定数据报文源地址属于对等联盟 Sub-TA_3 中成员 AS_X 目的地址属于本域 AS_Y，随即启动如下处理策略：查询 MSMT，定位状态机〈$Sub\text{-}TA_3$，AS_Y〉，验证并去除 tag_3，向本域内部网络转发. 至此，域间真实源地址验证过程结束，过程中一旦检测到非法报文则立即丢弃.

6 有效性分析与性能评价

本节首先分别分析了 Hidasav 对于状态机存储开销和更新代价的优化以及对于单位数据报文验证开销的影响，接着进行了实验评估.

6.1 有效性分析

假设在扁平化的信任联盟中，加入联盟的 AS 总数为 N，那么，每个 AER 所需维护的状态机列表规模是 $S_{AER}=2(N-1)$，并设其对应的集合为 C_F；在层次化的信任联盟中，所有部署 Hidasav 的 AS 组建信任联盟 $TA(N,L)$，N 是加入信任联盟的 AS 总数，L 是 $TA(N,L)$ 的层级总数（$1<L<\lfloor\log_2 N\rfloor+1, L\in Z$）. 令 m_i 表示 $TA(N,L)$ 中第 i 层级子联盟共有 m_i 个（$1<m_i\leq\lceil\sqrt[L-1]{N}\rceil$，$m_i\in Z$ 且均匀），p_{ij} 表示第 i 层中第 j 个子联盟 $Sub\text{-}TA(N,L)_{ij}$ 中的成员个数，（$1\leq i\leq L$，$1\leq j\leq m_i$，$1<p_{ij}\leq\lceil\sqrt[L-1]{N}\rceil$，$i,j,p_{ij}\in Z$）为了易于描述和反映 $TA(N,L)$ 的层次关系，将 $TA(N,L)$ 抽象为一棵高 L 的树 $\mathbb{T}$，其中每个节点表示一个信任联盟，所有叶子节点代表联盟的成员数的总和即为加入信任联盟的 AS 总数 N，如图 4 所示. $TA(N,L)$ 中每个 AER 所需维护的状态机列表规模是 $\overline{S}_{AER}$，并设其对应的集合为 C_{AER}；每个 TAER 所需维护的状态机列表规模是 $\overline{S}_{TAER}$，并设其对应的集合为 C_{TAER}.

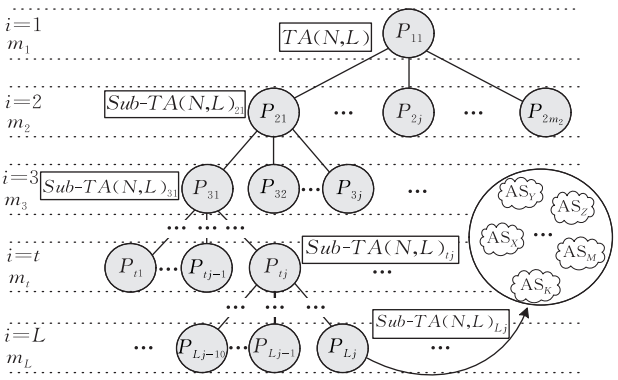

图 4　𝕋树层次化的体系结构(该树型结构反映了层次化信任联盟的等级关系和成员构成)

6.1.1　合理规划、均匀构建层次化的信任联盟

(1)状态机存储开销

合理规划是指联盟管理机构必须允许自治域依据隶属关系、路由策略、网络结构、数据通信统计分析和经济、政治、军事利益等现实情况自主决策加入不同的子信任联盟,灵活构建多层级的信任联盟.合理规划的目的是既确保互访数据通信频度较大的自治域聚类整合在同一子联盟内部,最大限度地简化子联盟内部管理的验证规则信息,同时又能保证隶属不同子联盟的自治域间的互联互通,而且应当尽可能既区分出层次又不至于造成层级过多引入标签替换开销增大的负面影响.

均匀构建是指 $TA(N,L)$中的所有层级联盟规模一致即从上到下每一层联盟均分为 m 个子联盟.由此,𝕋为一棵高为 L、具有 N 个叶子节点的满 m 叉树$\mathbb{T}_{\mathbb{F}}$,AER 维护的状态机量级缩减为式(1)所示:

$$\overline{S}_{\mathrm{AER}}=2(\lceil N/m^{L-1}\rceil-1)+2 \tag{1}$$

因为 L、m 远小于 N 且均为正整数,那么 $\lceil N/m^{L-1}\rceil\ll N$ 必然成立,所以分层后 AER 维护的状态机数量远小于未分层时的状态机数量如式(2)所示.

$$\overline{S}_{\mathrm{AER}}=2(\lceil N/m^{L-1}\rceil-1)+2\ll S_{\mathrm{AER}}=2(N-1) \tag{2}$$

对于 TAER,在本级联盟内部它维护着本级 AS 与对等节点间的状态机有序对,当作为本级联盟沟通外部其它联盟的中继时,它还需维护本级联盟与对等节点间的状态机有序对.不失一般性,可以推断当多个不同层次的信任联盟的 TAE 发生重叠时,该 TAE 处的 TAER 就必然在多个层级的信任联盟中分别履行 TAER 的职能.那么,考虑最极端的情况即 $TA(N,L)$中的某个路由器在多个不同层次的信任联盟中兼是 TAER,记为 $\mathrm{TAER}_{\max}$,其状态机列表规模记为 $\overline{S}_{\mathrm{TAER,max}}$.显然 $\mathrm{TAER}_{\max}$ 需要存储的状态机数量最为庞大,其列表规模由 3 部分组成:一是在最低层级联盟中 $\mathrm{TAER}_{\max}$ 所属的 AS 与对等节点间的状态机有序对;二是在自下而上的多层级联盟中 $\mathrm{TAER}_{\max}$ 所属的成员与对等节点间的状态机有序对;三是在自下而上的多层级联盟中 $\mathrm{TAER}_{\max}$ 所属的每一个联盟的联盟映射状态机,如式(3):

$$\overline{S}_{\mathrm{TAER,max}}=2\lceil N/m^{L-1}\rceil+2(L-1)m-4L \tag{3}$$

根据第 4 节中阐述的层次化的验证机制和标签替换规律,L 的取值应当尽可能兼顾既有效区分出层次、缩减 AER/TAER 的状态机数量又不至于造成层级过多而导致标签替换的开销增大的负面影响,因此 m 从上至下一定满足数值没有激增且尽量保持均匀.由此,可以推断对于取值范围内的任意的 L 和 m 当 N 达到一定数量级时总有且至少有一组 L 和 m 能够使得 $2\lceil N/m^{L-1}\rceil+2(L-1)m-4L$ 最小.于是,对式(3)求导,可得当 $m=\sqrt[L]{N}$ 时式(3)达到最小值.也就是说,当采用这样的分层原则和构建方法,TAER 维护的状态机数量是最小的,如式(4):

$$\overline{S}_{\mathrm{TAER,max}}=2L\sqrt[L]{N}-4L\ll 2(N-1) \tag{4}$$

因为 $1<L<\lfloor\log_2 N\rfloor+1, L\in Z$,所以式(4)必然成立.根据集合论,仍然可以推导出任何 $AER\in TA(N,L)$ 或 $TAER\in TA(N,L)$ 对应的 C_{AER} 或 C_{TAER} 都是 C_F 的子集即 $C_{\mathrm{AER}}\subset C_F$, $C_{\mathrm{TAER}}\subset C_F$.

同时,由于状态机的双向共享特性,状态机列表规模直接决定了其存储开销和更新代价,结合上述分析,由式(2)和(4)可知,相对于传统的扁平化的验证方法,当采用 Hidasav 方法均匀构建层次化的信任联盟时,状态机信息的存储开销和更新代价可得到有效缩减,如表 2 所示.

表 2　状态机信息的存储开销和更新代价对照表(均匀)

验证机制	联盟规模	验证设备	状态机存储开销	状态机更新代价
APPA	N	AER	$O(N)$	$O(N^2)$
Hidasav	N	AER	$O(N/m^{L-1})$	$O((N/m^{(L-1)})^2)$
		TAER	$O(N^{1/L})$	$O((N^{1/L})^2)$

(2)单位数据报文验证开销

为了便于分析,表 3 给出了分析过程需要用到的变量定义及说明.

表 3　相关变量定义及符号说明表

变量	释义
t_{SM}	状态机查询单位开销
t_{PRE}	IP 前缀和所属自治域对应关系查询单位开销
t_{OPE}	添加/去除标签操作单位开销
S_{PRE}	信任联盟全局 IP 前缀数
$\overline{S}_{\mathrm{PRE}}$	最低层次信任联盟 IP 前缀数,是 S_{PRE} 的子集

当以文献[12]方法构建扁平化信任联盟时,其单位数据报文最大验证开销 $Cost_{\max}F$ 是:

$$Cost_{\max}F=S_{AER}\cdot t_{SM}+2(S_{PRE}\cdot t_{PRE}+t_{OPE})=2(N-1)\cdot t_{SM}+2S_{PRE}\cdot t_{PRE}+2t_{OPE} \quad (5)$$

当以 Hidasav 方法构建层次化的信任联盟时,涉及标签验证和处理的数据通信场景由单一信任联盟数据通信和跨联盟数据通信 2 种组成,假设单一信任联盟数据通信和跨联盟数据通信所占比例分别为 p 和 $1-p$,那么,单位数据报文最大验证总开销为 $Cost_{\max}H.u=Cost_{\max}H.u._{STA}\cdot p+Cost_{\max}H.u._{CTA}\cdot(1-p)$.

这里以图 3 为例,分别在单一信任联盟数据通信和跨联盟数据通信 2 种场景中对单位数据报文验证开销进行分析:

(i)单一信任联盟数据通信单位数据报文验证开销

$$Cost_{\max}H.u._{STA}=2\lceil N/m^{L-1}\rceil\cdot t_{SM}+2\bar{S}_{PRE}\cdot t_{PRE}+2t_{OPE}\ll Cost_{\max}F=2(N-1)\cdot t_{SM}+2S_{PRE}\cdot t_{PRE}+2t_{OPE} \quad (6)$$

因为 $\lceil N/m^{L-1}\rceil\ll N$,$\bar{S}_{PRE}\ll S_{PRE}$,可得式(6)必然成立.即在单一信任联盟数据通信场景中,以 Hidasav 方法均匀构建层次化信任联盟,能够减小单位数据报文验证开销.

(ii)跨联盟数据通信单位数据报文验证开销

$$Cost_{\max}H.u._{CTA}=(\bar{S}_{AER}+4m-2)\cdot t_{SM}+2(S_{PRE}+\bar{S}_{PRE})\cdot t_{PRE}+6t_{OPE}=(2\lceil N/m^{L-1}\rceil+4m-2)\cdot t_{SM}+2(S_{PRE}+\bar{S}_{PRE})\cdot t_{PRE}+6t_{OPE} \quad (7)$$

根据分析发现,层次化后在跨联盟数据通信场景中,单位数据报文验证开销的组成中有关状态机处理的开销部分有较大幅度缩减,而跨联盟过程中涉及的标签替换开销以及地址前缀和所属自治域对应关系查询开销均有较小幅度的增加,此时的单位数据报文验证开销受 L,m 和 p 数值大小因素制约.综合评估,通过合理规划即信任联盟层次较小以及互访数据通信频度较大的自治域聚类整合在同一子联盟内部,能够实现 p 和 m 值较大、L 和 $(1-p)$ 较小,总能够使得 $Cost_{\max}H.u\ll Cost_{\max}F$ 成立.

6.1.2 合理规划、非均匀构建层次化的信任联盟

(1)状态机存储开销

非均匀构建是指 $TA(N,L)$ 中的不同层级或同一层级联盟间规模不完全一致,各联盟可以根据不同的划分原则和构建方法适当地、灵活地组织联盟规模.此时,$TA(N,L)$ 可抽象为一棵高为 L 的一般树$\mathbb{T}$.AER 的状态机列表规模缩减为 $2p_{Lj}$,因为 p_{Lj} 远小于 N,所以分层后的状态机数量远小于未分层时的,如式(8)所示.

$$\bar{S}_{AER}=2(p_{Lj}-1)+2\ll S_{AER}=2(N-1) \quad (8)$$

对于 TAER,在本级联盟内部它维护着本级 AS 与对等节点间的状态机有序对,当作为本级联盟沟通外部其它联盟的中继时,它还需维护本级联盟与对等节点间的状态机有序对.不失一般性,可以推断当多个不同层次的信任联盟的 TAE 发生重叠时,该 TAE 处的 TAER 就必然在多个层级的信任联盟中分别履行 TAER 的职能.那么,考虑最极端的情况即 $TA(N,L)$ 中的某个路由器在每一层级联盟中都是 TAER,记为 $TAER_{max}$,其状态机列表规模记为 $\bar{S}_{TAER.max}$.显然 $TAER_{max}$ 需要存储的状态机数量最为庞大,其构成同 6.1.1 节中(1)中所述,如式(9)所示.

$$\bar{S}_{TAER.max}=4\sum_{i=1}^{L}(p_{ij}-1)<4\sum_{i=1}^{L}p_{ij},\ p_{1j}=p_{11} \quad (9)$$

其中,$\sum_{i=1}^{L}p_{ij}$ 表示 $TAER_{max}$ 所在的所有层级联盟的成员数总和,根据第 4 节中阐述的层次化的验证机制和标签替换规律,L 的取值应当尽可能兼顾既有效区分出层次、缩减 AER/TAER 的状态机表项又不至于造成层级过多而导致标签替换的开销增大的影响,因此 m_i 和 p_{ij} 从上至下一定满足数值没有激增且尽量保持均匀.由此,可以推断对于取值范围内的任意的 L 和 p_{ij} 当 N 达到一定数量级时总有且至少有一个 $4\sum_{i=1}^{L}p_{ij}\ll 2(N-1)$ 必然成立,于是式(9)可表示为式(10):

$$\bar{S}_{TAER.max}=4\sum_{i=1}^{L}(p_{ij}-1)\ll 2(N-1) \quad (10)$$

根据集合论,仍可推导出任何 $AER\in TA(N,L)$ 或 $TAER\in TA(N,L)$ 对应的 C_{AER} 或 C_{TAER} 都是 C_F 的子集即 $C_{AER}\subset C_F$,$C_{TAER}\subset C_F$.

同时,由于状态机的双向共享特性,状态机列表规模直接决定了其存储开销和更新代价,分别令 p_{Lj_max} 表示 AER 所在的规模最大的某一最低层级联盟的成员总数,p_{lj_max} 表示 $TAER_{max}$ 所在的规模最大的某一层级联盟的成员总数,显然 $p_{Lj\_max}\ll N$,$p_{lj\_max}\ll N$,结合上述分析,由式(8)和式(10)可知,相对于传统的扁平化的验证方法,当采用 Hidasav 方法非均匀构建层次化的信任联盟时,状态机信息的存储开销和更新代价仍可得到有效缩减,如表 4 所示.

表 4　状态机信息的存储开销和更新代价对照表(非均匀)

验证机制	联盟规模	验证设备	状态机存储开销	状态机更新代价
APPA	N	AER	$O(N)$	$O(N^2)$
Hidasav	N	AER	$O(p_{Lj\_\max})$	$O(p^2_{Lj\_\max})$
		TAER	$O(p_{lj\_\max})$	$O(p^2_{lj\_\max})$

(2) 单位数据报文验证开销

当以 Hidasav 方法非均匀构建层次化的信任联盟时，涉及标签验证和处理的数据通信场景中单位数据报文最大验证总开销为 $Cost_{\max}H.un=Cost_{\max}H.un._{\mathrm{STA}}\cdot p+Cost_{\max}H.un._{\mathrm{CTA}}\cdot(1-p)$.

这里以图 3 为例，分别在单一信任联盟数据通信和跨联盟数据通信 2 种场景中对单位数据报文验证开销进行分析：

(i) 单一信任联盟数据通信单位数据报文验证开销

$$\begin{aligned}Cost_{\max}H.un._{\mathrm{STA}}=&\\ &2p_{Lj}\cdot t_{\mathrm{SM}}+2\overline{S}_{\mathrm{PRE}}\cdot t_{\mathrm{PRE}}+2t_{\mathrm{OPE}}\ll Cost_{\max}F\\ &=2(N-1)\cdot t_{\mathrm{SM}}+2S_{\mathrm{PRE}}\cdot t_{\mathrm{PRE}}+2t_{\mathrm{OPE}}\end{aligned}\tag{11}$$

因为 $p_{Lj}\ll N$，$\overline{S}_{\mathrm{PRE}}\ll S_{\mathrm{PRE}}$，可得式(11)必然成立. 即在单一信任联盟数据通信场景中，以 Hidasav 方法均匀构建层次化信任联盟，能够减小单位数据报文验证开销.

(ii) 跨联盟数据通信单位数据报文验证开销

$$\begin{aligned}Cost_{\max}H.un._{\mathrm{CTA}}=&(\overline{S}_{\mathrm{AER}}+4m_L-2)\cdot t_{\mathrm{SM}}+\\ &2(S_{\mathrm{PRE}}+\overline{S}_{\mathrm{PRE}})\cdot t_{\mathrm{PRE}}+6t_{\mathrm{OPE}}\\ =&(p_{Li}+p_{Lj}+4m_L-2)\cdot t_{\mathrm{SM}}+\\ &2(S_{\mathrm{PRE}}+\overline{S}_{\mathrm{PRE}})\cdot t_{\mathrm{PRE}}+6t_{\mathrm{OPE}}\end{aligned}\tag{12}$$

同 6.1.1 节中(2)(ii)中分析发现，层次化后在跨联盟数据通信场景中，单位数据报文最大验证开销的组成中有关状态机处理的开销部分有较大幅度缩减，而跨联盟过程中涉及的标签替换开销以及地址前缀和所属自治域对应关系查询开销均有小幅增加，此时的单位数据报文验证开销受 L、p_{Lj} 和 p 数值大小因素制约. 综合评估，通过合理规划即信任联盟层次较小以及互访数据通信频度较大的自治域聚类整合在同一子联盟内部，能够实现 p 较大，L、p_{Lj} 和 $(1-p)$ 较小，总能够使得 $Cost_{\max}H.un\ll Cost_{\max}F$ 成立.

6.2　实验评估

6.2.1　状态机存储开销评估

(1) 实验 1. 根据 Hidasav 方法均匀构建信任联盟时状态机的优化验证. 图 5(X 轴为线性坐标，Y 轴为对数坐标)显示了{$L=4$, $m=5$}, {$L=5$, $m=5$},

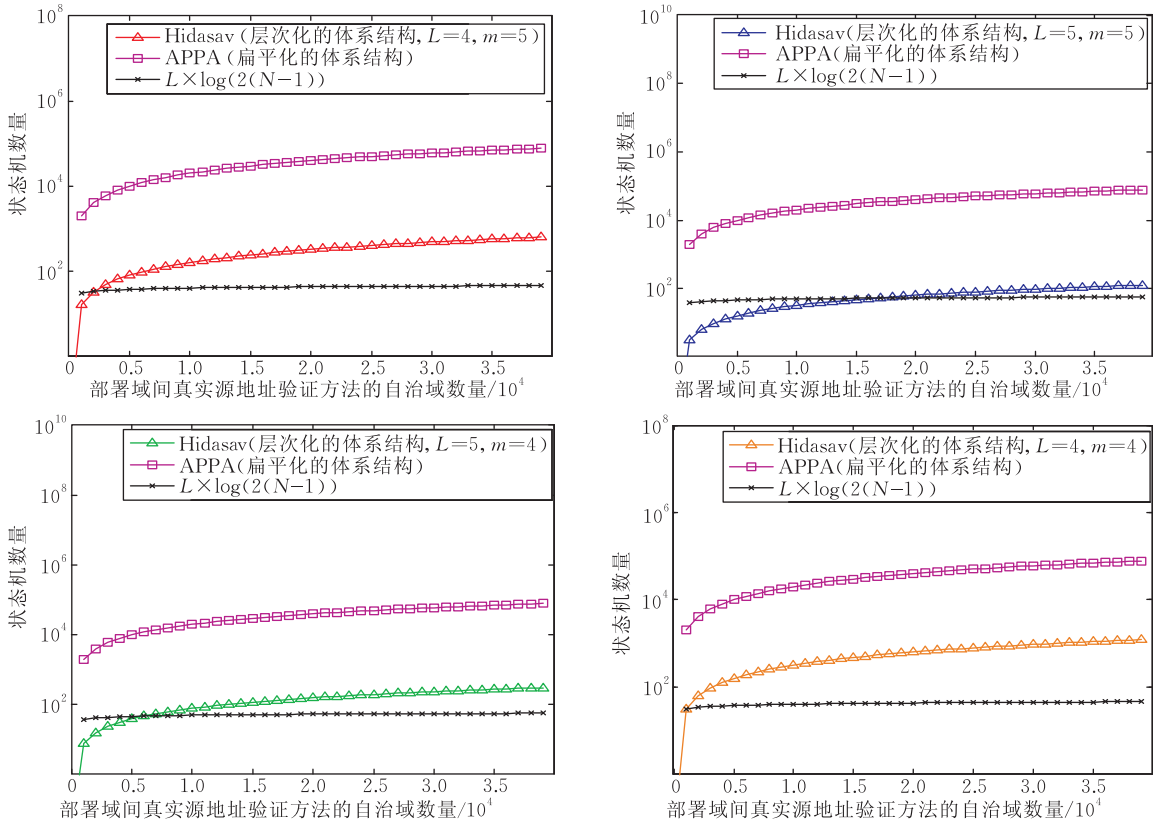

图 5　采用均匀方法构建的层次化信任联盟中边界路由设备 AER 维护状态机开销

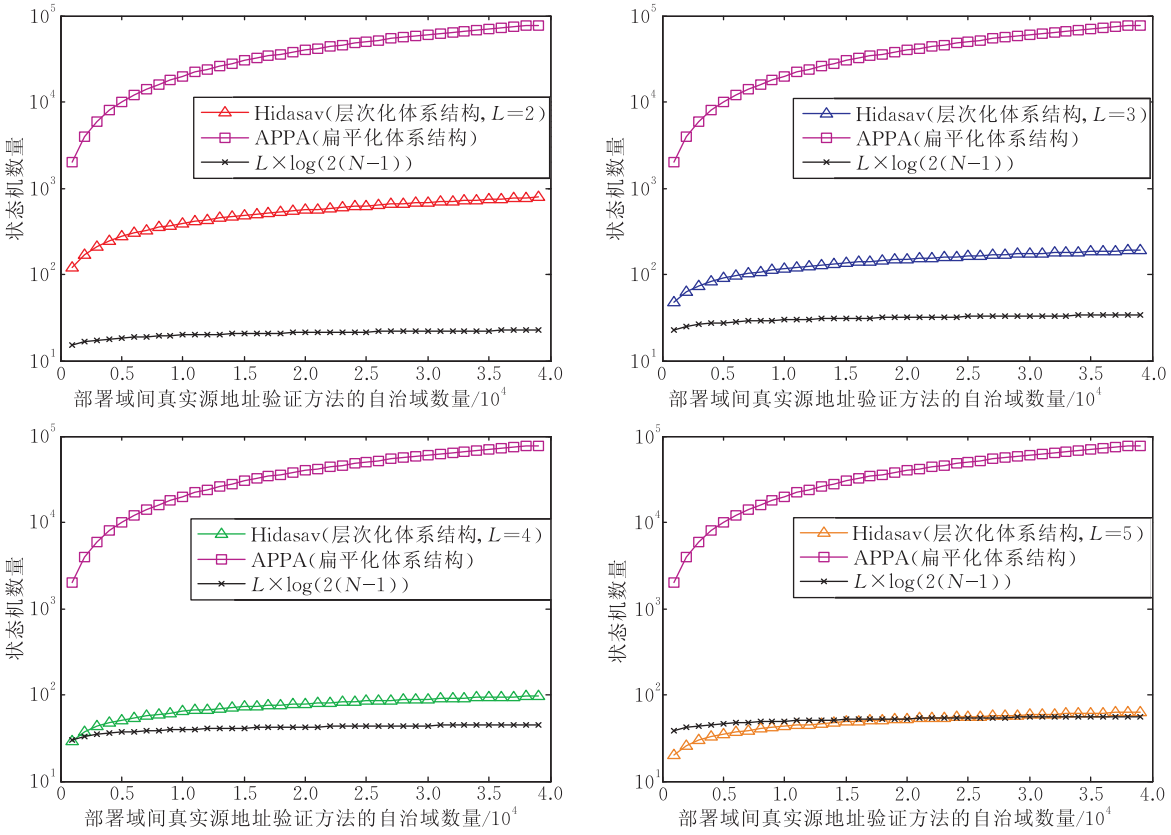

图 6 采用均匀方法构建的层次化信任联盟中边界路由设备 TAER 维护状态机开销

$\{L=5, m=4\}$,$\{L=4, m=4\}$时边界路由器 AER 状态机的数量级,图 6(X 轴为线性坐标,Y 轴为对数坐标)显示了当$\{L=2, m=\sqrt[2]{N}\}$,$\{L=3, m=\sqrt[3]{N}\}$,$\{L=4, m=\sqrt[4]{N}\}$,$\{L=5, m=\sqrt[5]{N}\}$时边界路由器 TAER 状态机的数量级. 图 5、图 6 中的实验结果表明,采用文献[12]的方法构建扁平化的信任联盟时,边界路由器维护的状态机数量随着联盟规模的增大呈较大幅度的快速增长,当联盟成员数量达到 5000 时,状态机就已接近 10^4 数量级,而采用 Hidasav 方法均匀构建层次化的信任联盟,边界路由器维护的状态机数量均得到了有效缩减,状态机存储空间复杂度也由 $O(N)$ 量级降低为 $O(N^{1/L})$ 量级. 可以看出对于 AER,即使在最大规模的信任联盟中,状态机的数量平均还不到 10^3 数量级,与文献[12]中的 10^5 对比,平均优化幅度达到 93%. 对于 TAER,因为联盟规模的扩展而带来的状态机增长明显放缓,并且随着 L 值的增大缩减的幅度也不断增大,当 $L<5$ 时,状态机数量的优化幅度平均达到了 10^3 数量级,当 $L=5$ 时,状态机数量增长函数演变成了近似对数函数接近 10^2 数量级,状态机维护开销平均优化幅度达到 95%.

(2) 实验 2. 根据 Hidasav 方法非均匀构建信任联盟时状态机的优化验证. 目前,清华大学主持建设的真实 IPv6 源地址验证体系结构已在 CNGI-CERNET2 网络上部署、运行和测试,并有多家国内外机构、运营商和设备制造商参与实现,国内主要有 CERNET2①、中国电信、中国移动等,国际上主要有 TEIN3②、GÉANT2③、APAN-JP④、KREONet2⑤. 上述机构都拥有多个全局独立的自治域编号,共同为本文实验 2 提供了一个多自治域的实验环境. 实验在 CNGI-CERNET2 网络运行管理中心的 Aladdin 网络流量监测系统上进行了数据采集和分析,如图 7 数据显示:较之访问 NGI(国际下一代互联网)的流量(浅),CNGI 内部用户的互访流量约占 90%(深);较之访问 CNGI 的流量(浅),CERNET2 内部用户的互访流量约占 92%(深).

基于层次化的验证机制和标签替换规律,结合上述分析,认为将 CNGI 和 CERNET2 构建为 2 个

① CERNET2,第二代中国教育和科研计算机网. http://www.cernet2.edu.cn
② TEIN3,第三代跨欧亚信息网络. http://www.tein3.net
③ GÉANT2,第二代泛欧洲教育和科研数据网络. http://www.geant2.net
④ APAN-JP,亚太高等计算机网络日本站. http://www.jp.apan.net/NOC/
⑤ KREONet2,第二代韩国研究环境开放网络. http://noc.kreonet.net

不同层级的信任联盟可合理实现区分层次和标签替换开销的权衡，并构建了全球下一代互联网信任联盟，如图 8 所示.

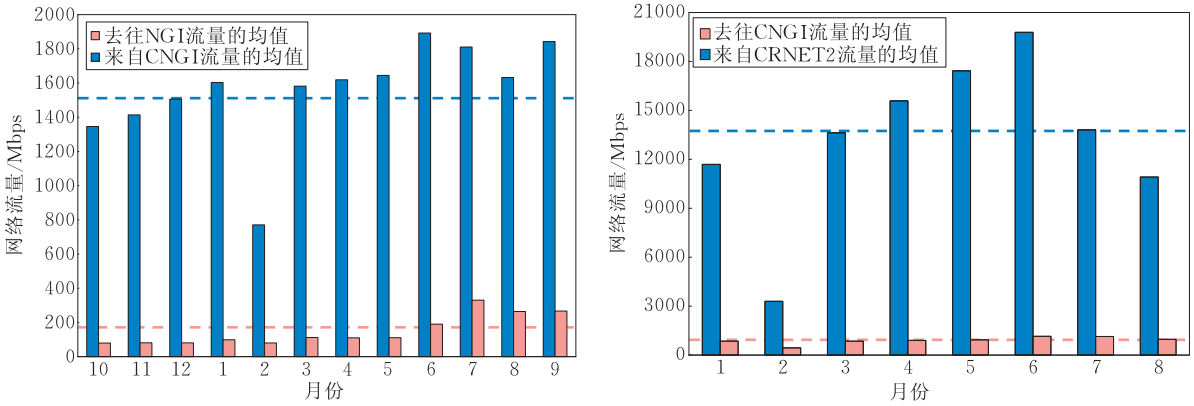

图 7　CNGI-6IX 和 CNGI-CERNET2 主干网入/出站流量统计(CNGI-6IX：09.10～10.09，CNGI-CERNET2：10.01～10.08)

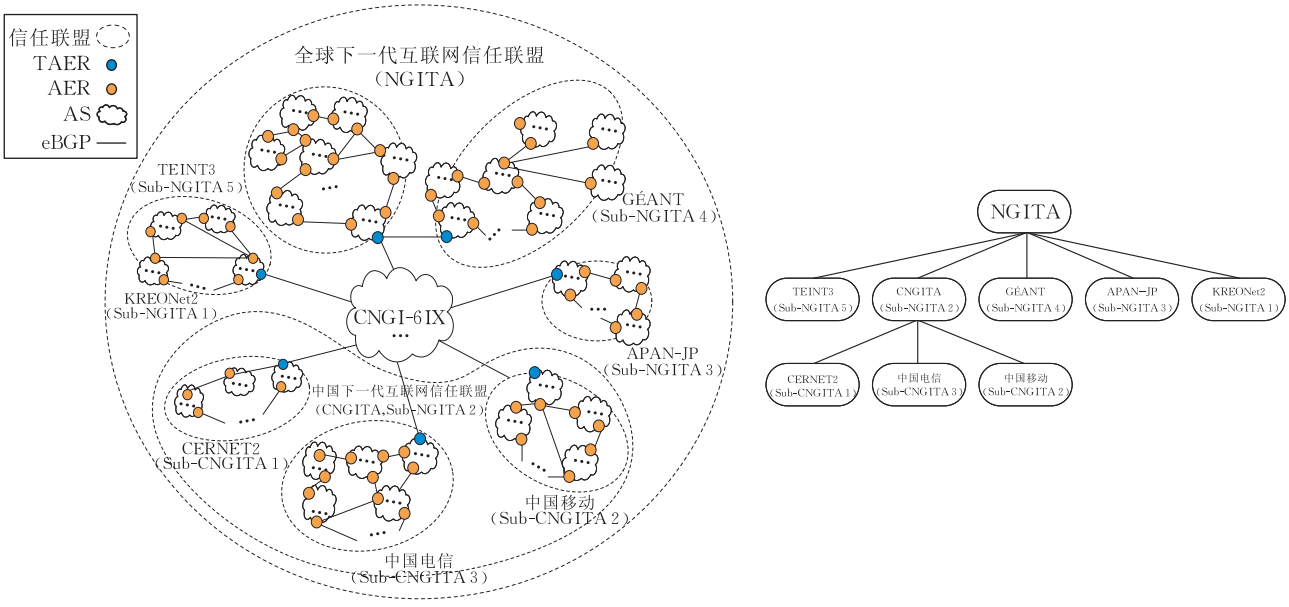

图 8　全球下一代互联网信任联盟的体系结构和层次关系

表 5 显示了根据 Hidasav 方法非均匀构建层次化的信任联盟时，AER/TAER 维护的状态机数量均得到了有效缩减，与文献[12]的方法对比，状态机的存储开销最大缩减了 94%，最小也缩减了 74%，平均缩减幅度达到 85%；状态机的更新开销也缩减了 95%以上，优化明显，达到了实验预期的效果.

表 5　扁平化结构和层次化结构中边界路由设备状态机存储和更新开销对比

机构名称	AS	扁平化体系结构		层次化体系结构							
		AER 状态机数量	状态机更新开销	AER 状态机数量	优化幅度/%	状态机更新开销	优化幅度/%	TAER 状态机数量	优化幅度/%	状态机更新开销	优化幅度/%
CERNET2	25+	448	448^2t	48	90	48^2t	98	58	87	58^2t	98
中国移动	45+	448	448^2t	88	80	88^2t	96	98	78	98^2t	95
中国电信	55+	448	448^2t	108	76	108^2t	94	118	74	118^2t	93
TEIN3	20+	448	448^2t	38	92	38^2t	99	48	89	48^2t	98
GÉANT2	34+	448	448^2t	66	85	66^2t	98	76	83	76^2t	97
APAN-JP	32+	448	448^2t	62	86	62^2t	98	72	84	72^2t	97
KREONet2	14+	448	448^2t	26	94	26^2t	99	36	92	36^2t	99

注：数据来源于 CNGI-CERNET2 NOC；t 表示状态机更新单位时间.

6.2.2 单位数据报文验证开销评估

(1)实验 1.根据 Hidasav 方法均匀构建信任联盟时单位数据报文验证开销的优化验证.图 9 显示了{$p=0.4, m=12$},{$p=0.5, m=16$},{$p=0.6, m=20$},{$p=0.7, m=24$},{$p=0.8, m=28$},{$p=0.9, m=32$}时采用 Hidasav 方法均匀构建 2 层级信任联盟时单位数据报文的验证开销.实验结果表明,采用文献[12]方法构建扁平化信任联盟时,单位数据报文的验证开销伴随联盟规模的扩大增长较快,平均增幅达到联盟规模增幅的 2 倍;当采用 Hidasav 方法均匀构建层次化的信任联盟时,单位数据报文验证开销的增幅明显放缓,并且随着 p 和 m 的增大而逐渐减小,较之文献[12]方法,当{$p=0.4, m=12$}时单位报文验证开销缩减较小,为 35.5%,当{$p=0.9, m=32$}时缩减较大,达到 87.6%,分析 6 组实验数据,单位数据报文验证开销平均缩减达到 62.1%.

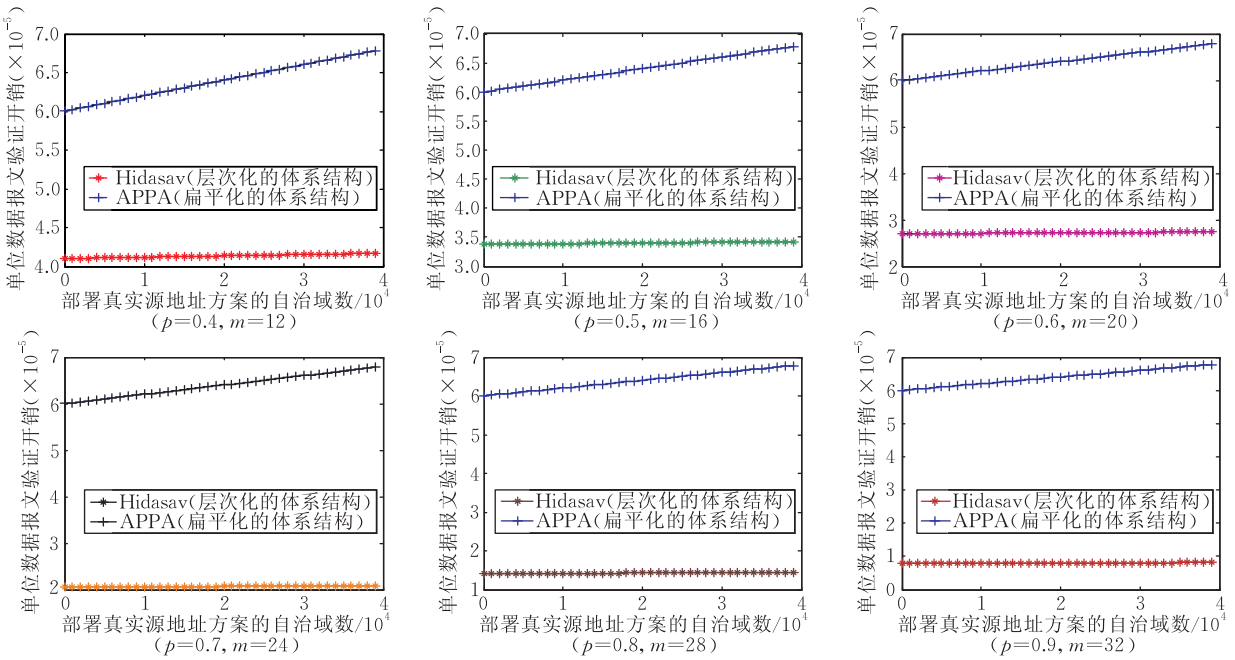

图 9 采用均匀方法构建的层次化信任联盟中单位数据报文验证开销

(2)实验 2.根据 Hidasav 方法非均匀构建信任联盟时单位数据报文验证开销的优化验证.基于 6.2.1 节中的实验 2,选取 CNGI 信任联盟中的 CERNET2 子信任联盟进行评估,其中跨联盟数据通信场景通信对端为中国电信信任联盟.实验在 CNGI-CERNET2 网络运行管理中心的 Aladdin 网络流量监测系统上进行了数据采集和分析,此时 $p=0.92$(如图 7 所示),CNGI 信任联盟内成员数 $N=448+$,CERNET2 子联盟 $P_{21}=25+$,中国电信子联盟内成员数 $P_{23}=55+$(如表 5 所示),属于 CERNET2 子联盟内的前缀为 $\overline{S}_{PRE}=52+$,属于 CNGI 信任联盟的前缀 $S_{PRE}=437+$.实验数据显示,与文献[12]的方法对比,在 CNGI-CERNET2 网络环境下,采用 Hidasav 方法非均匀构建信任联盟时,验证过程中:由分层引入的标签操作开销仅为 $0.23\cdot t_{OPE}$,而前缀和状态机的处理操作开销则分别缩减了 79%和 81%,单位数据报文验证开销平均优化幅度为 74%,达到了实验预期效果,如表 6 所示.

表 6 扁平化和层次化信任联盟中单位数据报文验证开销对照表

验证机制	单位数据报文验证		
	验证开销复杂度	验证开销	优化幅度/%
APPA	$O(N+S_{PRE})$	$248\cdot t_{SM}+874\cdot t_{PRE}+2\cdot t_{OPE}$	—
Hidasav	$O[p\cdot(P_{21}+\overline{S}_{PRE})+(1-p)\cdot(\overline{S}_{PRE}+S_{PRE})]$	$53\cdot t_{SM}+174\cdot t_{PRE}+(2+0.23)\cdot t_{OPE}$	74

7 结论及下一步工作

与现有的基于标签的域间源地址验证方法对比,本方法立足实际网络环境,可灵活构建层次化的多级信任联盟体系结构,通过分层和引入“中继代理”TAE,将每一层级联盟和外界网络隔离,无需协议扩展,不依赖域间的邻接关系,在确保路由协议的稳

定性和域间高速通信的情况下，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，实验证明该方法通过规划联盟层次和聚类整合，有效缩减了边界路由设备的状态机存储、更新开销和单位数据报文验证开销. 下一步将在 CNGI-CERNET2 网络上进行试验部署和可靠性测试，为大规模工程部署做准备. 同时，在本文研究的基础上，还将立足不同的实际网络环境进一步开展有关构建层次化信任联盟体系结构方法的研究.

参　考　文　献

[1] Moore D, Voelker G, Savage S. Inferring Internet denial-of-service activity. ACM Transactions on Computer Systems, 2006, 24(2): 115-139

[2] Elliott J. Distributed denial of service attacks and the zombie ant effect. IT Professional, 2000, 2(2): 55-57

[3] Evan C, Farnam J, Danny M. The zombie roundup: Understanding, detecting, and disrupting botnets//Proceedings of the USENIX Security Symposium SRUTI 2005. Cambridge, USA, 2005: 39-44

[4] Golbeck J, Hendler J. Reputation network analysis for Email filtering//Proceedings of the Conference on Email and Anti-Spam (CEAS). California, USA, 2004, 44: 54-58

[5] Wang H, Jin G, Shin K G. Defense against spoofed IP traffic using hop-count filtering. ACM Transactions on Networking, 2007, 15(1): 40-53

[6] Moore D, Voelker G, Savage S. Inferring Internet denial-of-service activity. ACM Transactions on Computer Systems, 2006, 24(2): 115-139

[7] Santiraveewan V, Pempoontanalarp Y. A graph-based methodology for analyzing IP spoofing attack//Proceedings of the 18th International Conference on Advanced Information Networking and Application (AINA'04). Fukuoka, Japan, 2004: 227-231

[8] Lee K, Kin J, Kwon K H et al. DDoS attack detection method using cluster analysis. Expert System with Applications, 2008, 34(3): 1659-1666

[9] Computer Emergency Response Team (CERT), TCP SYN flooding and IP spoofing attacks. http://www. cert org/advisories/CA-1996-21. html, 2000. 11. 29

[10] Ferguson P, Senie D. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. RFC 2827, 2000. http://www.ietf. org/rfc2827.txt?number=2827

[11] Bremler-Barr A, Levy H. Spoofing prevention method//Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Virginia, USA, 2005, 1: 536-547

[12] Shen Y, Bi J, Wu J P et al. A two-level source address spoofing prevention based on automatic signature and verification mechanism//Proceedings of the IEEE Symposium on Computers and Communications (ISCC). Tarrytown, NY, USA, 2008: 392-397

[13] Savage S, Wetherall D, Karlin A et al. Practical network support for IP traceback. ACM SIGCOMM Computer Communication Review, 2000, 30(4): 295-306

[14] Belenky A, Ansari N. IP traceback with deterministic packet marking. IEEE Communication Letters, 2003, 7(4): 162-164

[15] Snoeren A, Partridge C, Sanchez L et al. A hash-based IP traceback. ACM SIGCOMM Computer Communication Review, 2001, 31(4): 3-14

[16] Bellovin S, Leech M, Taylor T. ICMP traceback messages. IETF Internet Draft, draft-ietf-itrace-04, 2003, 8

[17] Lee H, Thing V, Xu Y et al. ICMP traceback with cumulative path, an efficient solution for IP traceback. Information and Communications Security. Berlin: Springer, 2003,2836: 124-135

[18] Park K, Lee H. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets. ACM SIGCOMM Computer Communication Review, 2001, 31(4): 15-26

[19] Li J, Mirkovic J, Wang M et al. SAVE: Source address validity enforcement protocol//Proceedings of the IEEE INFOCOM. Washington: IEEE, 2002, 3: 1557-1566

[20] Ferguson P, Senie D. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. IETF, RFC2827. 2000, 5

[21] Cisco Systems, Inc. Unicast reverse path forwarding. Cisco IOS Software Releases. 11. 1. 2007

[22] Jin C, Wang H. Hop-count filtering: An effective defense against spoofed DDoS traffic//Proceedings of the ACM CCS, 2003: 30-41

[23] Baker F. Requirements for IP version 4 routers. IETF RFC 1812. 1995, 6

[24] Wu J P, Xu K. Next generation internet architecture. Journal of Computer Science Technology, 2006, 21(5): 726-734

[25] Wu J, Ren G, Li X. Source address validation: Architecture and protocol design//Proceedings of the 15th IEEE International Conference on Network Protocols (ICNP). Beijing, China, 2007: 276-283

[26] Wu J, Bi J, Li X et al. A source address validation architecture (SAVA) testbed and experiences. IETF Internet RFC5210. 2008, 6

[27] Wu J, Ren G, Bi J et al. A first-hop source address validation solution for SAVA. IETF Internet Draft, draft-wu-sava-solution-firsthop-eap-01. 2008, 7

[28] Wu J, Bi J, Ren G et al. Source address validation architecture (SAVA) framework, IETF Internet Draft, draft-wu-sava-framework-01, 2007, 6

[29] Wu J, Bi J, Li X et al. SAVA testbed and experiences to date, IETF Internet Draft, draft-wu-sava-testbed-experience-06, 2008, 5

[30] Lin Chuang, Lei Lei. Research on next generation Internet architecture. Chinese Journal of Computers, 2007, 30(5): 693-711(in Chinese)
(林闯, 雷蕾. 下一代互联网体系结构研究. 计算机学报, 2007, 30(5): 693-711)

[31] Lin Chuang, Ren Feng-Yuan. Controllable, trustworthy and scalable new generation Internet. Journal of Software, 2004, 12(2): 1815-1821(in Chinese)
(林闯, 任丰原. 可控可信可扩展的新一代互联网. 软件学报, 2004, 12(2): 1815-1821)

[32] Wu Jian-Ping, Liu Ying, Wu Qian. The research progress on theory of next generation Internet architecture. Science in China, 2008, 38(10): 1540-1564(in Chinese)
(吴建平, 刘莹, 吴茜. 新一代互联网体系结构理论研究进展. 中国科学, 2008, 38(10): 1540-1564)

[33] Wu Jian-Ping, Wu Qian, Xu Ke. Research and exploration of next-generation Internet architecture. Chinese Journal of Computers, 2008, 31(9): 1536-1548(in Chinese)
(吴建平, 吴茜, 徐恪. 下一代互联网体系结构基础研究及探索. 计算机学报, 2008, 31(9): 1536-1548)

LI Jie, born in 1979, Ph. D.. His research interests include the architecture and key technology of next generation Internet, inter-domain IP source address validation solution.

WU Jian-Ping, born in 1953, Ph. D., professor, Ph. D. supervisor. His research interests include the architecture and key technology of next generation Internet, network protocol engineering.

XU Ke, born in 1974, Ph. D., professor, Ph. D. supervisor. His research interests include the architecture and key technology of next generation Internet, switch and router architecture.

CHEN Wen-Long, born in 1976, Ph. D.. His research interests include network protocol and network architecture.

Background

Next generation internet is highly concerned with the issue of trustworthy. Principally, the foundation of trustworthy is authenticated source IP address. However, IP source address spoofing is used in many attacks and the scale is increasing fast in the Internet, such as some DDoS/DrDoS attacks. IP source address spoofing would have profoundly negative implications for the Internet unless IP spoofing is stopped. In the last decade, many inter-domain authenticated source address validation solutions have been proposed to prevent IP address spoofing, such as SPM and APPA. However, as the demands on the size, functionality, performance and other aspects of keeping increasing, the current defense mechanisms are almost not available to the trust alliance for the hierarchical architecture. It leads to the flat structure of the trust alliance. With the increasing of the trust alliance size, the costs of validation grow up quickly. It has hampered the development of technology of inter-domain authenticated source address validation and none of them has been widely deployed. This paper first looks into the current state of inter-domain authenticated source address validation solution and thoroughly evaluates the current state of these solutions, then proposes a hierarchical inter-domain authenticated source address validation solution named Hidasav. Based on tag replacement and layer partition, Hidasav constructs a hierarchical structure of trust alliance without negative influence on actual network. It aims of several optimizing objects as follow, the number of the state machine, the difficulty of synchronization, the cost of per-packet tag operation and the cost of handle strategy, which is still a big challenge to existing solutions. It further analyzes and discusses the conclusion that can guarantee that every packet received and forwarded holds an authenticated source IP address. The experiment in CNGI also indicates that Hidasav can obtain the design goals of the architecture are hierarchical, lightweight, loose coupling, "multi-fence support" and incremental deployment.

This project is sponsored by the National Scientific and Technological Support Program during the 11th Five-Year Plan Period under grant No. 2008BAH37B02, the National Basic Research Program of China (also called 973 Program) under grant No. 2009CB320501 and the National High-Tech Research and Development Program of China (also called 863 Program) under grant Nos. 2008AA01A326, 2009AA01A334.