轻量级域间BGP路由安全网络方案研究

Research on Light eBGP Routing Security Network Scheme

熊礼霞，陈　燕，郜均翔，张　旭（中讯邮电咨询设计院有限公司，北京 100048）
Xiong Lixia，Chen Yan，Gao Junxiang，Zhang Xu（China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China）

摘　要：
首先阐述网络安全技术及域间BGP路由安全的发展现状，分析了现有防护方案（如业界BGPsec方案[1]）的核心问题——部署难度高、对现网设备改造要求高。提出了一种轻量级域间BGP路由安全网络方案，从协议扩展设计与业务处理流程2个方面，详细阐述了方案的总体思路、技术细节、应用场景及应用价值。旨在通过该轻量级方案，降低域间BGP路由安全防护的部署复杂度与现网改造成本，为域间路由安全防护提供可行路径。

关键词：
轻量级BGP安全；域间BGP；BGP安全
doi：10.12045/j.issn.1007-3043.2025.10.013
文章编号：1007-3043（2025）10-0071-05
中图分类号：TN914
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
Firstly，the development status of network security technology and eBGP routing security is elaborated，and the core problems of existing protection scheme（such as the industry BGPsec scheme）are analyzed，such as high deployment difficulty and high requirements for the transformation of existing network equipment. A light eBGP routing security scheme is proposed，and from two aspects：protocol extension design and business processing flow，it elaborates on the overall idea，technical details，application scenarios，and application value of the scheme. Through this light scheme，the deployment complexity and network transformation cost of eBGP routing security protection are reduced，providing a feasible path for inter domain routing security protection.

Keywords：
Light BGP security；eBGP；BGP security

引用格式：熊礼霞，陈燕，郜均翔，等. 轻量级域间BGP路由安全网络方案研究[J]. 邮电设计技术，2025（10）：71-75.

0 引言

网络安全是在计算机网络广泛应用和快速发展的背景下产生的关键内容。它已成为关系国家安全、社会稳定和广大人民群众切身利益的重要问题，业界通过建立不同的技术体系，从不同层面开展研究以促进全球网络安全技术的发展。我国也将提升网络安全保障能力放在国家战略高度。

网络安全技术的载体是网络设备。从逻辑层面划分，网络设备的安全功能对应在管理平面、控制平面和数据转发平面3个功能平面，其中，管理平面主要涉及与OAM（Operation，Administration，and Maintenance Technology）相关的功能，如SNMP、用户接入控制、日志等；转发平面主要涉及数据转发过程中的安全相关特性能力，如报文校正检验、攻击流量抑制等；控制平面负责运行各种协议信令，主要涉及各种路由协议的安全特性技术，如BGP、OSPF等。由于自2000年以来发生了诸多重大路由安全事故，控制平面的BGP安全成为通信领域近年来的热点研究课题。本文所提的轻量级域间BGP路由安全网络方案归属于控制平面的安全技术研究范畴。该方案通过验证和识别BGP路由发布过程中的非法前缀信息，实现网络安

收稿日期：2025-09-15

全防护。

1 BGP路由安全技术现状

一直以来,BGP安全事故频发,这迫使BGP协议不断更新和完善。目前,业界关于BGP安全的研究主要包括协议和业务2个层面。

a)BGP协议机制本身的安全提升。通过各种认证技术修补BGP协议的路由认证缺陷,例如采用MD5等提高对等体关系的安全认证方法。

b)通过第三方权威可信认证方式对域间路由进行验证和安全增强,例如RPKI(Resource Public Key Infrastructure)认证方案[2]。

1.1 技术标准化研究情况

BGP协议诞生于1989年的IETF会议期间[3],RFC1105是第1个正式发布的BGP国际标准。目前,BGP相关的功能扩展等IETF标准基本在IDR(Inter-Domain Routing)工作组讨论和发布。受全球路由安全事故的影响,2017年,IETF联合其他机构启动了安全域间路由(SIDR)的联合项目,专门针对BGP的路由攻击威胁。目前,在IETF有专门的SIDROPS(SIDR Operations)工作组,该工作组涉及的主要技术方案为RPKI、ROV(Origin Validation of BGP announcements)和BGPsec[4-7]。

国内标准组织主要为中国通信标准化协会(CCSA),其中TC8的研究范围涵盖信息通信网络与数据安全、融合新兴技术和业务安全等领域。其下设有8个工作组,分别针对不同的技术领域进行研究,工作组WG2主要负责网络安全技术手段等相关标准化工作,不过目前在TC3和TC1也有相关的路由安全技术研究项目。

1.2 BGP路由安全问题分类

BGP协议运行在网络设备的控制面,主要负责找到最优路由,以实现报文转发到目的网络及设备。基于已发生的BGP路由安全事件分析,目前国际组织IETF将路由安全问题分为以下6种类型。

a)从上游ISP(Internet Service Provider)接收的路由泄露给其他上游ISP。

b)从非转接(横向)ISP接收的路由泄漏给其他非转接(横向)ISP。

c)从上游ISP接收的路由泄漏给非转接(横向)ISP。

d)从非转接(横向)ISP接收的路由泄漏给上游ISP。

e)更改路由前缀的合法来源,重新发布路由。

f)发布内部或更具体明细路由(前缀信息),造成属于其他合法来源部分内容被更改。

上述6种类型都源于路由信息的泄漏。其中,前面4种类型只涉及信息泄漏,被称为“路由泄漏”,后面2种类型还存在路由被篡改的问题,通常又被称为“路由劫持”[8]。

1.3 现有方案及问题分析

目前,跨域BGP路由安全技术方向主要包括RPKI、BGPsec和自治系统供应上授权(Autonomous System Provider Authorization,ASPA)。业界仍旧针对现有方案存在的问题进行不断的分析和优化完善。

RPKI是由IETF主推的,目前应用最为广泛的BGP路由验证方案。RPKI是一个以区域互联网注册管理机构(Regional Internet Registry,RIR)为中心的集中式分层结构的基础设施,在其内部存储着路由源授权(Route Origin Authorization,ROA)。AS节点的ROA由该AS的上级机构所签发,将经过认证的IP前缀与该AS的节点编号相绑定,并允许该AS节点向其他AS节点宣告其拥有该IP前缀。BGP路由器在需要进行路由验证时,会依据ROA进行IP前缀与宣告AS对应关系的验证,即路由源验证ROV。如果验证成功,则依据该宣告更新路由信息;否则丢弃该宣告,防止该IP前缀被劫持。RPKI部署方式相对简单,对BGP恶意攻击或误操作所造成的影响也有不错的防御能力,因此被IETF广泛推广,进而成为BGPsec等BGP路由验证方案的基础。但是,由于ROA的发放与更新都是人工审核,RPKI存在更新速度较慢且会产生误操作的隐患。同时,RPKI采用了集中式分层结构,在ROA部署灵活性和可扩展性上均可进一步增强[4-7]。

BGPsec是基于RPKI和ROV的BGP路径验证方案。BGPsec要求宣告AS path的AS节点在包含IP前缀和源、目的AS的宣告上签名,以便目的AS节点验证该AS path的宣告者。当目的AS节点收到该宣告时,会基于RPKI的ROV对该签名进行验证,以确认该宣告AS path的真实性。当目的AS节点向后续节点继续宣告AS path时,其会在新的宣告报文后面继续附上自己的签名来辅助后续AS节点进行验证。由于报文中同时携带有之前每一跳的签名信息,目的节点同时可以对整条AS path进行验证,以确保AS path的真实性。BGPsec的逐跳验证AS path的策略可以有效防止虚假

的AS宣告，保证AS path的真实性。但是由于BGPsec逐跳验证的特性，对于AS path上部分部署的情况，会导致验证每跳信息的签名链断裂，难以完整验证整条AS path的安全性。

ASPA是基于AS间商业关系的BGP路径验证方案。ASPA要求客户AS（Customer AS）维护一个列表并对列表签名，列表中记录有该客户AS的AS编号和其所对应的一组供应商AS（Provider AS）的AS编号。客户AS的列表会存储到分布式的ASPA数据库中，用以在验证AS path宣告时进行辅助验证。当AS收到其他AS的AS path宣告时，它可以根据无谷（valley-free）原则（如图1所示，供应商AS 2向另一个供应商AS 4传输时，不应经过该供应商AS的客户AS，即AS 3），结合ASPA数据库中所记录的客户—供应商关系对AS path进行验证，以验证该路径的真实性。ASPA是基于商业关系对AS path进行验证的，它从新的角度对BGP路径进行验证。但是，由于AS商业关系的公开，AS间商业关系泄露也成为隐患，ASPA仍需在保护商业隐私上有所提升[9-10]。

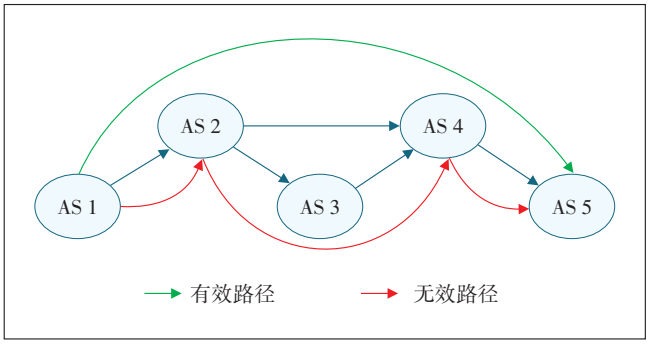

图1　valley-free原则示意

上述3种现有方案是当前业界重点关注和研究的方案，但在以下3个方面仍需进一步优化。

a）可部署性：BGPsec部分部署会导致信任链断裂，使安全性大幅降低。

b）路由策略和商业隐私保护：ASPA会公开AS间商业信息和路由策略。

c）跨平面验证：上述BGP路径验证方案仅能验证宣告的正确性，对于流量是否按宣告路线缺乏验证。

因此，需要在上述主流BGP路径验证方案的基础上设计出一个兼具灵活性和可部署性的方案。该方案能够对BGP路径宣告进行逐跳验证并实现隐私保护，同时能够实现跨平面验证的BGP路径验证。

2 轻量级域间BGP路由安全网络方案

2.1 方案总体思路

通过在BGP update消息中新增一个可选过渡属性（BGP设备可以识别和处理此属性，也可以不识别但传递通告此属性）——Path_Attribute，采用轻量级密码标签对路由前缀、当前AS和下一跳AS信息进行加密验证。同时，该方案不修改AS_PATH属性，兼容现有BGP部署，且可以降低部署率要求，实现一种可增量部署的域间路由验证机制[11]。

2.2 方案详细设计

2.2.1 新增Path_Attribute

方案在BGP Update消息中新增一个全局的可选过渡属性——Path_Attribute，用于携带所发布路由的AS信息、下一跳的AS信息和IP路由前缀，并利用私钥进行编码处理，将得到的加密信息作为路由验证的关键数据，其封装格式如图2所示。

图2　新增Path_Attribute封装格式

a）标识（1字节）：设定值为0b11010000，表示此属性为可选过渡的，是此路由的部分属性。

b）类型（1字节）：待定，待IANA组织分配。

c）加密信息长度（2字节）：表示加密信息的字段字节长度值。

d）加密信息（长度可变）：携带上一个AS号、当前AS号和下一跳AS，路由IP及加密相关信息的编码信息，具体格式如图3所示。

加密信息字段中各字段的定义和功能如下。

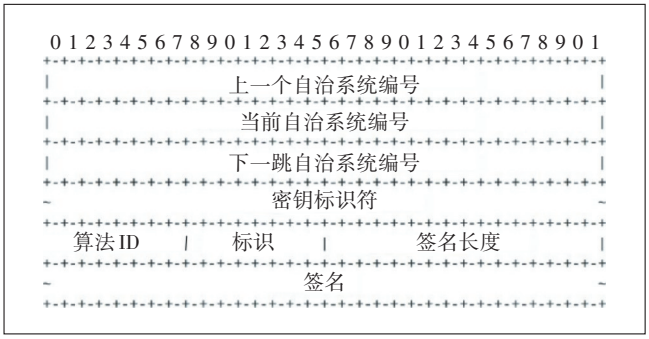

图3　加密信息字段格式

a）自治系统编号字段。采用4字节方式。

b）密钥标识符。定义为20字节，在RPKI路由认证系统中，此信息用作唯一的签名验证公钥。

c）算法ID字段。作为加密算法的索引或标识信息。

d）标识字段。暂未使用（全0）。

e）签名长度字段。长度为2字节，数值为签名字段的字节数。

f）签名字段。长度可变，其内容为路由前缀和3个自治系统编号的信息加密编码。

2.2.2 路由验证处理流程

部署此方案的路由器设备，收到携带新增Path_Attribute的BGP Update消息后，需要进行3个操作处理。

a）验证AS_Path属性，以确认路由路径的合法性。

b）在BGP控制面进行路由优选，此操作与标准BGP处理流程一致。

c）更新Path_Attribute信息，并继续发布BGP Upate到下一跳设备。

图4所示为一个BGP Update携带新增Path_Attribute进行域间路由安全验证的协议信息。

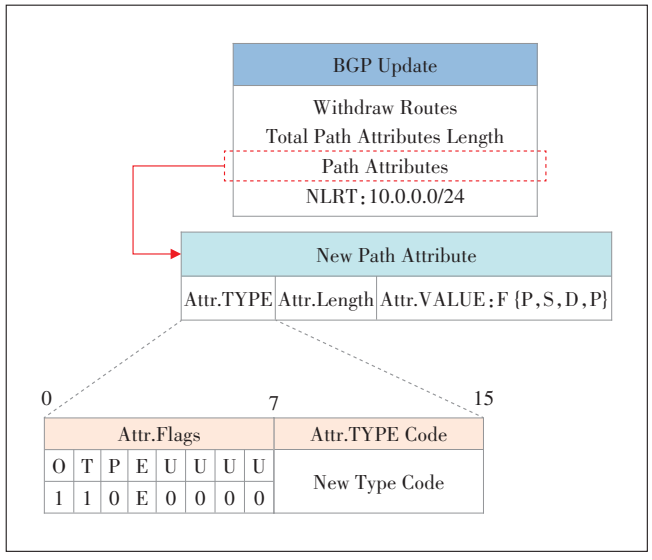

图4　携带新增Path_Attribute的BGP信息示例

假设存在3个自治域：A（AS 65001）、B（AS 65002）、C（AS 65003）。当BGP Update信息从A传给B后，再由B发布到C，用于加密验证的Path_Attribute从A开始产生，在B中进行验证和处理，之后B将新的验证信息再发布给C，C并不需要验证A到B的路径，即此方案中的验证和发布仅基于上一个自治域的路径，不需要验证之前的所有路径，如图5所示。

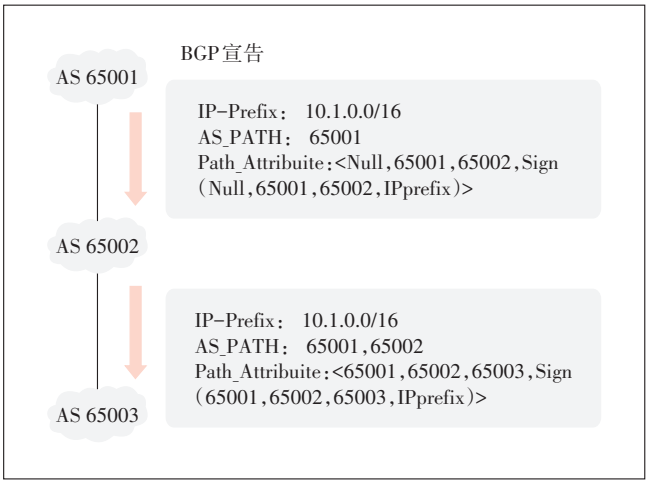

图5　路由通告示例

当B接收到Update消息时，从中提取用于路由验证的Path_Attribute属性信息，使用密钥标识符字段查找公钥，并使用算法ID中指定的算法来计算签名。如果计算得出的签名与封装中的签名匹配，则验证从A到B路由具有合法性。

如果B中的设备未部署该方案相关的功能，那么它在传播BGP路由时，只需将BGP Update转发给其邻居即可。如果下一个自治域中部署了此方案相关的功能，那么新的验证过程会重新建立。

2.3 方案验证测试

首先，构造一个包含多个AS域的模拟网络环境。在每个AS域中，随机构造不同的邻居数，根据邻居数从大到小将构造的多个AS进行排序。

然后，按照从小到大设置模拟网络环境里的设备功能部署率。根据上述的AS排序，依次选择一定数量的ASBR设备进行功能部署。例如，当部署率为0时，所有设备均不部署此方案；当部署率为0.1%时，选择AS排序中前0.1%的AS，并对其ASBR设备进行功能部署，以此类推。

最后，进行运行仿真测试。比如部署率为0，基于应用互联网数据分析中心（center for applied Internet data analysis，CAIDA）公开数据库中的路由发布数据，对BGP updates消息进行攻击仿真，测试获取攻击成功率。将部署率设置为0.1%，同样进行BGP updates消息的攻击仿真，测试获取攻击成功率。以此类推，进行多组不同部署率下的测试，获取多组测试数据。通

过观察和研究在不同部署率下网络被成功攻击的概率，评估该方案的可行性和可靠性，并分析测试结果的理论依据（见图6）。

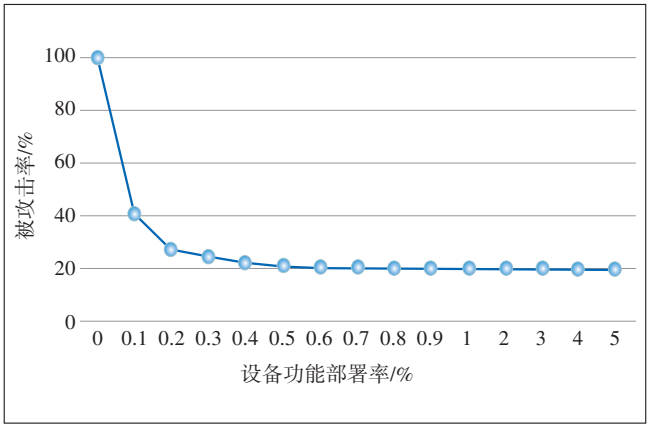

图6　不同设备功能部署率下的被攻击机率

3 应用场景分析

在运营商网络中，城域网、骨干网及数据中心等不同网络之间都会涉及BGP协议的应用。通过在路由发布消息中添加签名认证，并且不依赖逐跳部署的方式，便能够以最小的代价和增量升级方式实现路由安全的防护和保障。运营商跨域网络示意如图7所示。

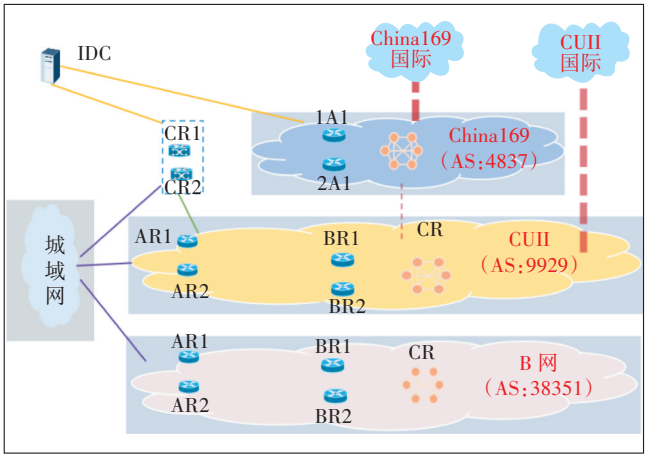

图7　运营商跨域网络示意

4 结束语

以BGPsec为代表的现有路由路径验证机制对部署率有较高要求，难以兼容部分部署的演进过程。本方案致力于研究域间路由分布式信任机理，将域间路由通告的路径验证过程映射为信任根建立和分布式信任传递过程。基于轻量级密码标签，设计相应的分布式、增量式部署的域间路由路径验证机制，改善当前方案对于部署率的过高要求，提升路由路径验证机制的可部署性和实用价值。

参考文献：

[1] LEPINSKI M，SRIRAM K. BGPSEC protocol specification：RFC8205 [S/OL]. [2025-02-24]. https://www.rfc-editor.org/rfc/rfc8205.

[2] 马迪. RPKI概览[J]. 电信网技术，2012(9)：30-33.

[3] REKHTER Y，LI T，HARES S. A border gateway protocol 4 (BGP-4)：RFC 4271[S/OL].[2025-02-24]. https://www.rfc-editor.org/rfc/rfc4271.

[4] DURAND A. Resource public key infrastructure (RPKI) technical analysis：OCTO-014[R/OL].[2025-02-24]. https://www.icann.org/en/system/files/files/octo-014-02sep20-en.pdf.

[5] KRISTOFF J，BUSH R，KANICH C，et al. On measuring RPKI relying parties[C]//Proceedings of the ACM Internet Measurement Conference. Virtual Event：Association for Computing Machinery，2020：484-491.

[6] COOPER D，HEILMAN E，BROGLE K，et al. On the risk of misbehaving RPKI authorities[C]//Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks. College Park：Association for Computing Machinery，2013：1-7.

[7] LEPINSKI M，KENT S. An infrastructure to support secure Internet routing：RFC 6480[S/OL]. [2025-02-24]. https://datatracker.ietf.org/doc/rfc6480/.

[8] 张沛，张晗，黄小红，等. 互联网域间路由安全监测与防御[M]. 北京：北京邮电大学出版社，2023.

[9] AZIMOV A，USKOV E，BUSH R，et al. A profile for autonomous system provider authorization [R/OL]. [2025-02-24]. https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-profile-20.

[10] AZIMOV A，BOGOMAZOV E，BUSH R，et al. BGP AS_PATH verification based on autonomous system provider authorization (ASPA) objects[R/OL].[2025-02-24]. https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-23.

[11] XU K，WANG X，LIU Z，et al. FC-BGP protocol specification[R/OL].[2025-02-24]. https://www.ietf.org/archive/id/draft-sidrops-wang-fcbgp-protocol-00.html.

作者简介：
熊礼霞，毕业于南京邮电大学，高级工程师，硕士，主要从事数据通信网络研究工作；陈燕，毕业于悉尼大学，工程师，硕士，主要从事数据通信网络研究工作；郜均翔，毕业于宁夏大学，工程师，硕士，主要从事数据通信网络研究及云网产品研究应用相关工作；张旭，毕业于郑州大学，工程师，硕士，主要从事数据通信网络研究工作。