软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2020,31(1):208−227 [doi: 10.13328/j.cnki.jos.005867]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

区块链技术在域间路由安全领域的应用研究*

陈 迪[1,2,3], 邱 菡[1,2], 朱俊虎[1,2], 王清贤[1,2]

[1](中国人民解放军战略支援部队 信息工程大学,河南 郑州 450002)

[2](数学工程与先进计算国家重点实验室,河南 郑州 450002)

[3](中国洛阳电子装备实验中心,河南 洛阳 471003)

通信作者: 陈迪, E-mail: chendi-409@tom.com

摘 要: 互联网域间路由系统的安全问题一直备受关注.实现全网范围的互联网资源管理认证和可信跨域协作至关重要.区块链技术以其去中心化、防篡改、可追溯等天然属性,可作为域间网络资源认证与信任建立的基础.首先分析域间路由系统安全脆弱性及其影响,以及传统域间路由安全机制面临的部署困难、管理复杂、信任中心化等困境;然后,在简要介绍区块链技术基本理论的基础上指出区块链技术运用于域间路由系统安全的技术思路,并详述区块链技术应用于域间路由认证、域间智能管理和域间 DDoS 防御等方面的最新进展;最后,分析区块链应用于域间路由安全领域的优势,从性能与规模、兼容性与增量部署以及区块链自身安全问题这 3 个方面分析其问题与挑战,并对下一步研究进行展望.

关键词: 域间路由安全;区块链;互联网资源管理;路由认证

中图法分类号: TP393

中文引用格式: 陈迪,邱菡,朱俊虎,王清贤.区块链技术在域间路由安全领域的应用研究.软件学报,2020,31(1):208−227. http://www.jos.org.cn/1000-9825/5867.htm

英文引用格式: Chen D, Qiu H, Zhu JH, Wang QX. Research on blockchain-based interdomain security solutions. Ruan Jian Xue Bao/Journal of Software, 2020,31(1):208−227 (in Chinese). http://www.jos.org.cn/1000-9825/5867.htm

Research on Blockchain-based Interdomain Security Solutions

CHEN Di[1,2,3], QIU Han[1,2], ZHU Jun-Hu[1,2], WANG Qing-Xian[1,2]

[1](PLA Strategic Support Force, Information Engineering University, Zhengzhou 450002, China)

[2](State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450002, China)

[3](Luoyang Electronic Equipment Test Center of China, Luoyang 471003, China)

Abstract: Much attention has been paid to the security of interdomain routing system. It is crucial to achieve the origin validation of Internet resource and multi-domain collaboration. By virtue of the natural attributes of blockchain including decentralization, tamper-resistant, and traceability, blockchain technology can act as the basis of Internet resource certification and trust establishment among multiple Internet domains. Firstly, the vulnerabilities of interdomain routing system and the dilemma of existing interdomain security proposals are analyzed including difficulty in deployment, complexity in management, centralized trust mechanism, etc. Secondly, based on the introduction of the basic concept of blockchain, the technical ideals of blockchain-based interdomain security solutions are pointed out, and an up-to-date review of blockchain-based interdomain security solutions is conducted from 3 aspects: interdomain routing authentication, intelligent interdomain management, and DDoS defense and mitigation. Finally, the advantages of blockchain-based interdomain security solutions are summarized and corresponding challenges are analyzed from the perspectives of scalability,

* 基金项目: 国家自然科学基金(61502528, 61902447)
Foundation item: National Natural Science Foundation of China (61502528, 61902447)
收稿时间: 2019-02-23; 采用时间: 2019-05-09; jos 在线出版时间: 2019-08-09
CNKI 网络优先出版: 2019-08-12 12:08:18, http://kns.cnki.net/kcms/detail/11.2560.TP.20190812.1208.010.html

deployment, and security, and the development outlook of blockchain technology used in the field of interdomain routing security is highlighted.

Key words: interdomain routing security; blockchain; Internet number resource certification; route origin attestation

互联网域间系统是一个规模巨大的分布式自治系统,边界网关协议(border gateway protocol,简称 BGP)[1]负责在各自治域(autonomous system,简称 AS)传递网络可达信息,为互联网范围的域间互连互通发挥着重要作用.由于 BGP 的无条件信任机制以及自适应机制方面的缺陷,互联网域间系统面临众多由恶意攻击[2]或网络误配置[3]等因素触发的安全威胁(如前缀劫持、路由泄露),进而引发域间路由系统出现流量黑洞、级联失效等现象,严重影响互联网的稳定运行[4].各自治域之间错综复杂的商业关系和路由策略[5],使多域间信任建立和资源认证成为互联网域间路由系统安全的重、难点课题.

目前,有较高影响力和代表性的域间路由安全机制主要有 S-BGP[6]和 so-BGP[7].其主要思想是:利用一套用于证书发布和路由验证的公钥基础设施 PKI,建立多域间的认证信任机制,以应对 BGP 主要安全威胁.在这些工作的基础上,IETF 安全域间路由(secure inter-domain routing,简称 SIDR)工作组提出了资源公钥基础设施标准化架构 RPKI(resource public key infrastructure)[8],用于源路由授权认证 ROA(route origin authorization)[9]以及用于路径传播认证的 BGPsec[10],并在实际部署方面做出了很多努力.但最新调查显示[11],仅有 12%的网络运营商部署了 RPKI 的全部功能.71%的网络运营商表示,因其高昂的部署开销和有限的安全收益[12],不会在本地部署 RPKI.此外,这些基于 PKI 的安全机制还存在信任中心化的缺陷[13]:由于各自治域属于不同的国家和地区,利益与审查政策不尽相同,中心化信任机构的部署缺乏有效激励.即使花费了很大的代价完成部署,当高层的证书机构或网络注册机构被攻击后,域间路由安全依然无从保证[14].

因此,如何在不依赖中心化信任机制的前提下实现分布自治的多域间的信任建立、资源认证、多方协作,同时又能最大程度地保护 AS 间的商业关系和路由策略,成为解决域间路由安全困境的关键问题.区块链技术[15]因其去中心化、防篡改、可追溯性的天然属性,提供了一种可供选择的技术支撑.区块链技术是利用块链式数据结构来存储与验证数据、利用分布式节点共识算法来生成和更新数据、利用密码学方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算方式.区块链通过分布式节点验证和共识机制的支持,使得在一个分布式的网络中,任何两个节点可以达成无中介的信任.

近几年,网络安全领域的研究者开始探索如何运用区块链技术解决域间路由安全面临的难题,新的思路和方法不断涌现,如基于区块链的路由认证[16−21]、基于智能合约的域间智能管理[22,23]、基于区块链的 DDoS 攻击防御[24,25]等.区块链可以作为新一代互联网的分布式账本系统,对互联网上数据资产的整个生命周期事务进行分布式地记录、加密和认证,其安全性由区块链技术使用的密码学算法作为信任“背书”,经过验证后,每一次事务交互过程可永久保存在分布式数据库(区块)中,一旦验证完毕,它将是共享的、匿名的、防篡改的,并且易于查询.在各个自治域保留和执行本地的路由策略和商业关系规则的前提下,区块链可作为互联网各自治域间建立信任关系的共同信任基础设施,在此基础上开展域间多方协作,构建一个可信任、共建秩序的互联网域间路由系统.

本文的工作包括:

- 首先,从域间路由安全脆弱性的内在原因出发,总结了域间路由系统需要解决的安全问题和现有安全机制存在的缺陷;
- 然后,从域间路由认证、域间智能管理以及跨域 DDoS 攻击防御缓解这 3 个方面,着重对区块链技术应用于域间路由安全领域的研究进展进行了详细梳理和深入分析;
- 最后指出了基于区块链的域间路由安全解决方案的技术优势和亟待解决的问题,从性能、规模、安全性、兼容性等多角度分析其技术难点和研究挑战,并对该领域未来的研究进行展望.

希望能激发相关研究领域的新思路,给相关研究提供参考与帮助.

本文第 1 节分析域间路由系统脆弱性与典型域间路由安全机制面临的困境.第 2 节在简要介绍区块链技术

基本理论的基础上,指出其运用于域间路由安全领域的技术思路,并综述区块链应用于域间路由安全领域的最新进展.第 3 节对区块链应用于域间路由安全领域进行优势比较、挑战分析与前景展望.第 4 节给出全文总结.

1 域间路由系统安全现状

1.1 域间路由系统脆弱性分析

BGP 是 Internet 默认的外部网关协议,负责互联网中各个自治系统 AS 之间的互联互通,每个 AS 都由全局唯一的自治系统号 ASN(autonomous system number)所标识,由独立管理机构控制,使用不尽相同的路由策略.但由于 BGP 协议自身的安全缺陷[26],难以保证 AS 之间通信安全和路由信息的真实性,并且任意一个 AS 的突发错误或攻击都会通过 BGP 协议影响其他 AS 的行为与决策,使得域间路由系统面临严峻的安全威胁.近年来,BGP 安全事件层出不穷,包括前缀劫持、链路中断、路由泄露、数据平面 DDoS 攻击等.图 1 按时间顺序列出了近 10 年的 BGP 重要安全事件,这些安全异常事件对整个互联网的可用性和稳定性都造成了不同程度的影响.

Fig.1 Influential BGP security incidents in recent decade

图 1 近 10 年重要 BGP 安全事件

域间路由系统从逻辑上可分为控制平面和数据平面,其中,控制平面负责交换路由信息,管控路由设备;数据平面负责转发数据报文.其中都存在不同程度的安全脆弱性,分析触发 BGP 异常事件的内在原因有利于从根源上应对域间路由安全问题.下面对域间路由系统的主要威胁、安全缺陷、相应影响做出简要阐述.

物理中断是由自然灾害(如地震)、能源基础设施毁伤等事件引发的通信网络线缆中断,导致路由节点链路失效,目标网络不可达,流量重定向,进而在路由状态的反复震荡影响下造成域间路由系统的连锁故障.解决这类问题的主要思路为:一方面是增强基础设施的鲁棒性;另一方面是在域间路由系统,通过有选择地增加备选路径等方案,提高毁伤后的自愈能力和恢复速度.

操作失误是域间路由安全中不可忽略的关键因素,许多大规模安全事件的原因并非恶意攻击,而是由个别网络运营商的错误配置引发.这是因为愈加复杂的网络拓扑、路由策略和 AS 之间的协作关系,使 BGP 策略设置与路由配置操作繁琐,需考虑商业关系、流量工程、可扩展性与审查政策等多重因素.BGP 的错误配置主要有两种类型:一类是源配置错误,比如某个 AS 错误地通告了不属于自己的网络前缀地址,当该错误通告被其他 AS 根据最长前缀匹配等路由策略接受时,会对域间路由系统造成与前缀劫持同样的影响;还有一类是出站错误配置,即错误地发送了不符合路由策略[27]或协商好的商业规则的路由通告,当该错误通告被其他 AS 根据客户优选、无谷底等路由策略接受并传播时,就会发生路由泄露事件.例如,2017 年 8 月 26 日,Google 意外地将从其 peer 获取的路由信息泄露给其 provider,因此变成了一个中转 AS[28],其后果是大量用户(尤其是日本用户)的网速急剧下降甚至彻底无法连接网络.BGP 操作失误引发异常的根本原因,也源于域间路由系统在控制层面缺乏 AS 之间协作认证机制的缺陷.

数据平面发起的攻击利用了域间路由系统在数据平面的安全脆弱性:控制平面和数据平面使用同样的物理媒介,数据平面的会话拥塞必然引起控制平面的拥塞.因此,当攻击者仅使用数据流量进行攻击时,也会造成 BGP 路由对等体之间逻辑链路断链.利用 BGP 自适应机制缺陷,一种方式为攻击者针对关键路由节点进行报文

注入,使路由器过载造成关键路由节点失效;另一种方式攻击者通过精心选择攻击链路,如远程拒绝服务 ZMW 攻击[29]、跨平面会话终止(coordinated cross plane session termination,简称 CXPST)攻击[30]等,造成关键路由链路失效,进而导致 BGP 会话重置,大量更新报文洪泛,AS 路径急剧增长,关键 BGP 会话在断开与重建中周而复始不断切换,网络拓扑急剧震荡,相邻的路由节点在震荡过程中过载崩溃,造成域间路由系统的级联失效,地区和国家范围内的大规模域间路由系统崩溃[31].

控制平面发起的攻击利用域间路由系统在控制平面的安全脆弱性:相邻 BGP 路由器交互域间路由信息过程中的无条件信任.这种缺失认证的无条件信任会被恶意节点利用,伪造并通告虚假或不符合路由策略的域间路由信息,当 BGP 路由器接收到消息时,默认该消息来自合法对等实体且内容真实完整.当 BGP 消息中的多出口分辨器属性(multi-exit discriminators,简称 MED)、IP 网络前缀、AS 商业关系、网络拓扑信息、AS 路径(AS_path)属性等关键信息被攻击者冒用、窃取、篡改、删除或重放时,就会造成虚假路由信息的传递与扩散.典型的控制平面攻击包括前缀劫持、路由泄露、AS 路径更改攻击,错误路由通告被相邻节点根据最长前缀匹配原则、最短路径优先、客户优选等路由策略接受后,会引发流量重定向,进而会造成窃听攻击或流量黑洞等安全事件[32].例如:2015 年 11 月 6 日,印度运营商 BHARTI Airtel 生成并通告了数以千计的不属于本地的外来 IP 地址前缀[33],造成流量重定向和路由泄漏,导致 2 000 多个自治域网络故障,对印度、中国、美国、日本、沙特等国家影响长达 9 小时;2017 年 12 月 12 日,俄罗斯某 AS 在 6 分钟内通过前缀劫持的方式,将多个知名网络机构(包括 Google、Apple、Facebook、Microsoft 等)的流量重定向到本地,然后再重新将流量送至合法目的地址以达成窃听攻击[34].当重定向流量集中于某 AS 节点造成路由节点/链路过载崩溃后,还会引发路由震荡,进而造成域间路由系统的级联失效现象.

基于上述分析,图 2 展示了触发 BGP 异常的原因、相应安全威胁以及对域间路由系统产生的影响.

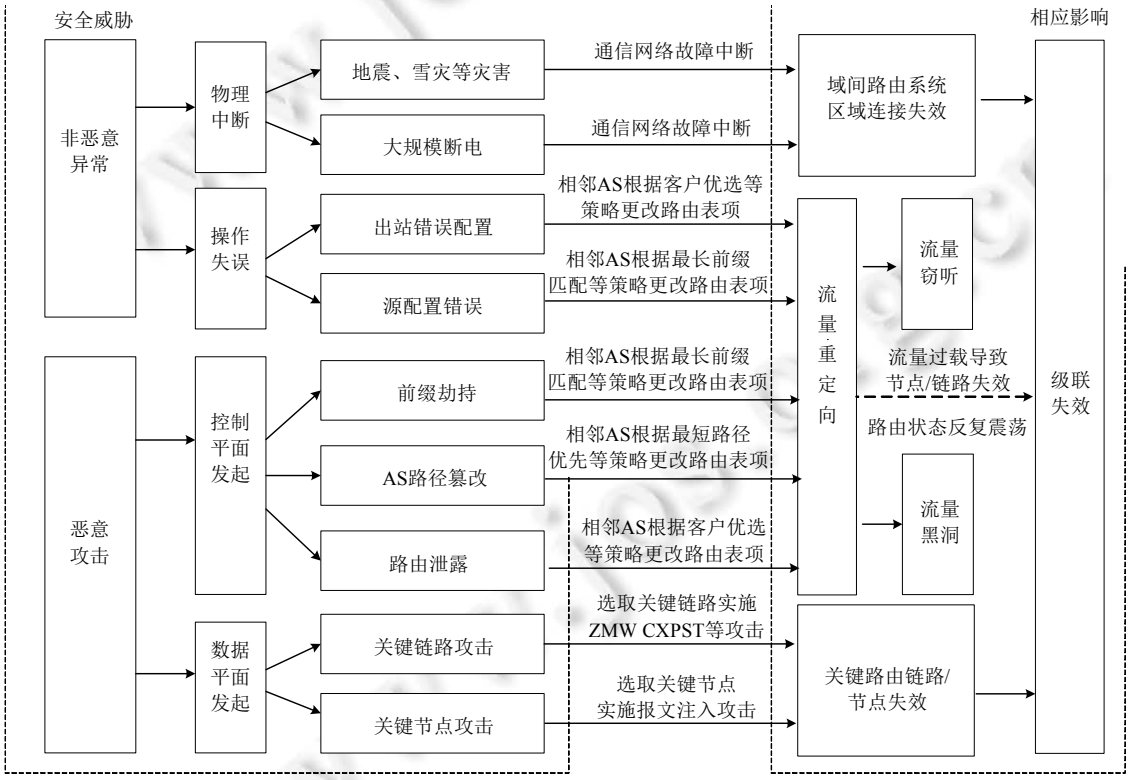

Fig.2 Impact of BGP security vulnerabilities on inter-domain routing system

图 2 BGP 安全缺陷对域间路由系统的影响

域间路由系统安全的关键问题之一是:在保留各自治域本地路由策略和商业关系隐私的前提下,在域间建立认证与信任.RFC 4360 指出[35]:要保证域间路由系统的安全,依赖于 BGP 传递信息的网络参与者必须具有从信息源头开始的信任传递关系.然而,由于越来越多分布自治的网络连接到互联网,这种信任建立的难度越来越高.很多研究者围绕这个问题提出了解决方案,下一小节将对其中典型方法做出简单的梳理与阐述,对其局限性做出分析与总结.

1.2 典型域间路由安全机制

当前,针对域间路由安全提出的解决方案主要有两类:一是通过基于数字签名、安全证书和加密技术的安全机制,弥补 BGP 协议认证缺失的缺陷[36];二是利用现网数据分析、网络主动探测等方式,对域间路由异常事件进行检测、定位和缓解[37].虽然检测与缓解技术目前具有较高的实用性,但现网数据仍存在区域和时间维度的局限性[38],漏报与误报依然无法避免,且难以预防安全事件的发生.从长远意义考虑,域间路由系统依然需要更加完善的前摄性防御机制,其中最重要的问题之一是路由认证,包括 AS 通告 IP 前缀的合法授权认证以及 BGP 路由消息中 AS-path 属性的完整性认证.

S-BGP[6]是最早提出的 BGP 安全机制解决方案之一,利用数字签名和公钥证书来验证通告的路由信息.S-BGP 借鉴了现有的互联网资源(IP 地址和 ASN)层次下发结构,建立了一套完整的且与之并行运行的 PKI 体系.将互联网数字分配机构(the internet assigned numbers authority,简称 IANA)作为根信任点,逐级下发到地区性互联网注册机构(regional internet registry,简称 RIR),直到互联网服务提供商(Internet service provider,简称 ISP).S-BGP 对 IP 前缀与 AS 授权、AS-path 路径、BGP 更新报文完整性、BGP 路由通告授权等关键信息都提供了认证功能,但由于 S-BGP 计算开销较大,路径收敛时间长,并未得到广泛的采用.So-BGP[7]是在 S-BGP 的基础上提出的更为轻量级的解决方案,通过设计分别负责认证 AS 身份、IP 地址块授权和 AS 拓扑连接真实性验证的 3 类证书来实现路由认证.域间路由验证(interdomain route validation,简称 IRV)[39]方案基于覆盖网络的思想,提出了一个连接各 AS 的分布式查询系统来验证 BGP 路由信息的方案,AS 可以指定一个 IRV 数据库,对其网络状况和路由信息的授权合法性进行查询验证.

受 S-BGP 等方案启发,IETF 的 SIDR 工作组在 2012 年提出了首个资源公钥基础设施标准化架构 RPKI[8],遵循现有 IP 地址前缀和 ASN 层次分配下发的流程,提供基于数字签名和安全证书的路由合法授权源认证 ROA[9]的功能,并进行了局部的部署.图 3 展示了 RPKI 的层次授权验证结构设计.

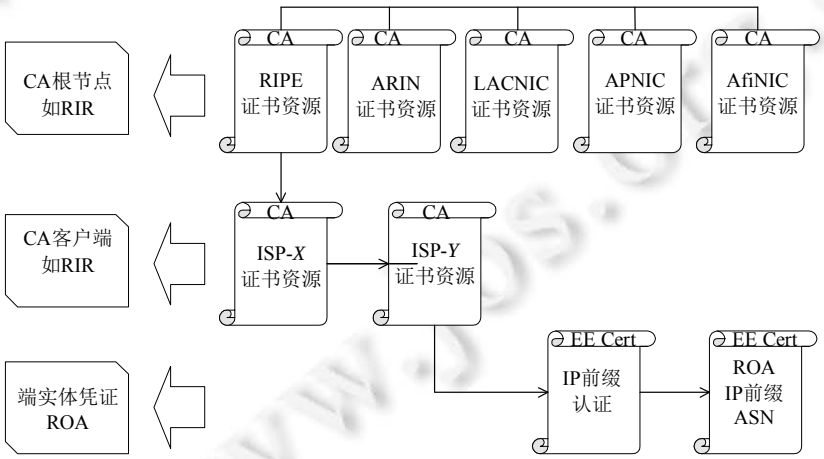

Fig.3 Administrative resource allocation hierarchy of RPKI

图 3 RPKI 资源管理分配层级

5 个 RIR 作为根信任证书颁发机构(certificate authority,简称 CA),可以形成从根节点 CA 到某 AS 或 ISP 加

密验证的信任链,其中,CA 负责授权 IP 地址块和为 ASN 分配有效性证书;终端实体(end-entity,简称 EE)为这些 IP 地址块之间授权传递提供中转;路由源认证(route origin authorization,简称 ROA)将 IP 前缀和路由源 AS 的 ASN 绑定在一起;分布式存储系统用于存储和提供签名的对象(如 ROA),并且每个 CA 定期发布证书撤销列表(certificate revocation list,简称 CRL)以撤回无效的证书.为了防止 AS 路径修改,提出了基于 RPKI 架构的 BGPsec[10],用于保证路由通告所经过的一系列 AS 路径的真实性.如图 4 所示:每个路由器利用自己的证书给从上一跳路由接收到的 ASN 信息进行签名认证,并作为路由消息的一部分继续转发.为了防止授权路由器进行重放攻击,BGPsec 需要定期的密钥更新.受限于部署规模和开销的限制,以及部署过程中所需的多方合作,RPKI ROA、BGPsec 在全球内应用的范围还很有限[40].

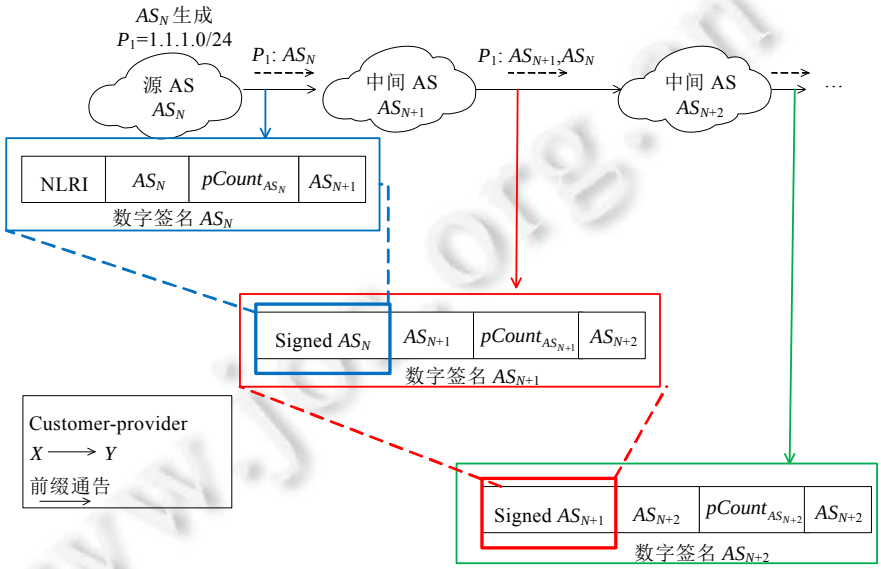

Fig.4 BGPsec path validation with forward signing

图 4 基于转发签名的 BGPsec 路径认证

上述方法在域间路由安全领域研究中发挥了重要的作用,但它们仍然存在未解决的安全隐患,并且均存在部署困难、管理复杂以及所依赖的信任基础架构信任中心化等问题.

- 部署困难:RPKI 等解决方案需要在全球范围内部署才能发挥作用,这不仅要解决所有要保护的安全对象的存储问题以及在全球范围内的时间同步问题,还需要多方积极配合.由于所有的 ISP 都需要在 CA 注册并接受管理,但为不同的自治域建立一个共信的权威中心,从政策层面来讲十分困难.最新调研[11]显示,71%的网络运营商不愿意在本地网络中部署 RPKI 作为前摄性防御机制,主要原因在于 RPKI 部署范围有限,协议机制复杂,处理开销较大,而带来的安全收益却不大.有很多工作[41,42]研究了全球 RPKI 部署的规模、分布式资源库同步与时延等问题,但这些工作并没有对全球 RPKI 的规模、功能、资源库大小、安全证书数量等指标达成共识;
- 管理复杂:RPKI 等方案需要复杂的管理操作.发放证书、确定证书有效期、证书撤销等管理操作都需要各级证书颁发机构 CA、注册机构 RA 以及证书发布系统的多方协同,会占用带宽资源,导致网络收敛时间变慢等问题,引发负面的效果.例如:一旦密钥更新,就需要从上至下对所有的证书重新签名;为了完成证书撤销的操作,需要签名方和验证方之间使用复杂的特定协议交互,处理 CRL 并进行公示;
- 信任基础架构信任中心化:RPKI 等基于 PKI 体系的防御方案信任中心化特性阻碍了其部署和应用进程,而现有的信任体系对于上层 CA 等权威中心的行为没有充分的记录和监管,CA 可以任意撤回下游的认证,也可能删除和修改其可认证的对象(如签名方、ROA 等).这种信任中心化会引起垄断问题,不

能抵御出于国家、机构等利益由 CA 所发起的恶意行为,也难以在全球互联网范围内保证认证信息的一致性.另外,RPKI 体系是一个中心化的树形结构,具有单点失效的缺陷,即使花费了很大的代价部署了类似 RPKI 的网络安全架构,当高层的 CA 等安全基础设施被攻击后,整个网络依然会陷入瘫痪.

基于上述分析,表 1 列出了当前典型域间路由安全机制未解决的安全隐患、部署情况与需求及其信任机制.

Table 1 Comparison of typical inter-domain routing security mechanisms

表 1 典型域间路由安全机制比较

解决方案	未解决的安全隐患	部署情况	部署需求				信任机制		
			额外硬件	额外架构	更改 BGP	公开 AS 关系	证书	数字签名	加密
S-BGP	路由泄露;PKI 安全隐患	未部署	可能	√	×	×	√	√	√
SoBGP	信任网络中恶意行为;路由泄露	未部署	可能	√	√	√	√	×	×
IRV	不支持 IP 源认证;伪造 IRV 数据库	未部署	√	√	×	部分	×	可能	可能
RPKI&ROA	不支持 AS 路径验证;RPKI 的安全隐患	部分部署	×	√	×	×	√	×	×
BGPsec	不支持 IP 源认证;RPKI 的安全隐患	未部署	可能	√	√	×	√	√	×

综上,针对传统域间路由安全机制的不足,迫切需要一个去中心化、易于管理、支持增量部署并能够有效激励网络运营商部署的域间路由信任方案,以保证网络资源分配和管理的真实性、一致性以及可追溯性.近年来出现的区块链技术给域间路由安全的研究者提供了新的解决思路,下文将重点阐述和分析近年来区块链技术在路由安全领域的应用.

2 区块链在域间路由安全领域的应用

区块链技术应用于域间路由安全的研究较新,本节首先简述区块链技术,然后从基于区块链的路由认证、域间智能管理系统和 DDoS 攻击防御这 3 个方面综述该领域的发展现状,并分析总结这些方案尚未解决的问题.

2.1 区块链技术及其应用于域间路由安全领域的总体思路

区块链技术[15]是一种按照时间顺序将数据区块以链条的方式组合成特定数据结构,并以密码学方式保证其不可篡改、不可伪造的去中心化共享总账,能够安全存储简单的、有先后关系、能在系统内验证的数据.在区块链中,数据存储在链式结构相连的数据区块中,每个区块分为区块头和区块体两部分:区块头中包含前一个区块的哈希值、时间戳等信息;区块体包含一系列由交易方对其进行数字签名的交易记录.新区块按照时间顺序添加在前一个区块的后面,逐渐形成一个拥有时间维度的链条,能够记录所有交易的分布式账本,从而保证数据的真实性和可追溯性.

共识机制是区块链技术的关键技术之一.当节点通过异步通信方式组成网络集群时,这种异步网络默认是不可靠的[43],那么在这些不可靠主机之间复制状态需要采取共识机制,以保证每个节点的状态达成最终一致性.由于区块链是一种分布式去中心化的架构,各节点需要对分布式账本中的记账权和记账顺序达成一致,以确定网络中的记账(生成新区块)节点,保证数据的一致性与正确性.现有的主流区块链共识机制包括基于算力比拼的工作量证明(proof of work,简称 PoW)和基于资产比拼的权益证明(proof of stake,简称 PoS):PoW 需要大量的资源消耗,共识机制达成周期较长;PoS 易于造成资产集中化和中心化.在此基础上,许多其他共识机制被提了出来,如除了考虑用户拥有的资产,还考虑用户重要度和可信度的重要度证明(proof of importance,简称 PoI)[44]、在以太坊上开发中的 Casper[45]等.

设计一个区块链系统架构,可针对特定的用户需求和应用场景选择或者定制最合适的区块链类型.区块链严格定义上被划分为 3 种类型:公有链、私有链和联盟链.公有链是对所有人公开,用户不需要注册和授权就能够匿名访问网络和区块,任何人都可以自由加入和退出网络,并参与记账和交易,通过密码学算法保证交易的安全性和不可篡改性,在陌生的网络(非安全)环境中,建立互信和共识机制.联盟链仅限于联盟成员,因其只针对成员开放全部或部分功能,所以联盟链上的读写权限以及记账规则都按联盟规则来定制.私有链对单独的个人或实体开放,仅在私有组织,比如公司内部使用,私有链上的读写权限、参与记账的权限都由私有组织来制定.这 3

种类型的区块链去中心化程度和对应的能耗开销和交易速率都是由高到低的.

区块链技术最早应用于比特币加密交易系统,除比特币以外,区块链还可以作为一个分布式账本系统被应用到注册、转移和确认各种不同类型的资产及合约,这些资产和合约统称为智能资产和智能合约.这也带动了以以太坊(Ethereum)为代表的第二代区块链(区块链 2.0)技术的迅速发展,第二代区块链中的资产可以是有形资产,也可以是无形资产,资产的智能化转移是通过区块链和智能合约来实现的.智能合约是各种资产的数字化协议,决定标的资产在哪里、所有权以及将如何处理.与普通合同不同,智能合约的核心是利用算法程序或脚本来替代人,在资产交易不被篡改的前提下去执行合约,实现在非信任的参与者之间自动执行合约中的协议条款.执行智能合约的程序和脚本存储在区块链上,保证了合约内容不被篡改.以太坊是第二代区块链运行智能合约及其应用的基础平台,任何智能合约应用,也被称为去中心化应用(blockchain decentralized application,简称DApp),都可以运行在以太坊平台上,也可以基于以太坊进行定制开发.在以太坊区块链上没有中间机构,不存在宕机、欺诈或第三方干扰的可能.

近几年,研究者开始将区块链技术用于解决域间路由安全中路由认证和多域间信息共享与协作的问题.文献[16]首次提出了 Internet Blockchain 方案,将区块链技术用于网络控制层面和互联网资源的可信管理.其总体思路是将互联网中的资源,如 IP 地址、DNS 域名、自治域 ASN 看作不可复制的资产,将其分配、下发、转交等操作及 BGP 通告过程看作互联网交易事务,用区块链进行去中心化不可篡改的记录,以确保真实性、可追溯性、可验证性.

在 Internet Blockchain 的启发下,研究者开展了基于区块链技术的 IP 地址授权合法认证[17,19,20]、BGP 路径认证[16]、现有安全机制密钥管理下发[21]、域间智能管理[22,23]以及 DDoS 防御机制设计[24,25]等多个方向的探索.这些研究的思路主要包括利用区块链去中心化、防篡改的信任机制,解决目前现有域间路由安全机制中信任中心化的垄断问题;利用区块链匿名、信息分布式共享的特性,解决目前域间路由系统各自治域信息独立、缺乏协同的问题;利用以太坊智能合约支持资产智能化转移的功能,实现多自治域间智能管理的功能,解决BGP操作配置复杂、错误配置概率较大的问题.

上述解决问题涉及到在第 1.1 节中阐述的操作失误问题、控制平面认证问题以及数据平面威胁,其中很多工作已完成原型系统实现和初步性能测试.虽然目前的方案仍未成熟,但可以激发域间路由安全研究的新思路.

2.2 利用区块链技术解决域间路由认证

利用区块链技术解决域间路由认证,近期研究工作的思路是利用区块链去信任、去中心化的优势,完成与传统方案 RPKI&ROA、BGPsec 等方案类似的功能,主要包括基于区块链的 IP 地址授权合法认证和基于区块链的路由认证两个方面.

2.2.1 基于区块链的 IP 地址授权合法认证

在区块链分布式去中心化特性的启发下,不少研究者发现了 IP 地址和区块链中代币之间的共同之处:可转让、可分、不能同时分配给多个参与者.为了对互联网数字资源(如 IP 地址、ASN)进行管理和分配,可以将各自治域拥有的IP地址前缀子网资源视作区块链中的资产,利用区块链的特性,建立比现有IP前缀分配管理系统更为灵活、简洁的信任模型和管理体系.

Xing 等人在文献[17]中提出了 BGPcoin,一种基于以太坊的互联网资源管理解决方案,利用智能合约实现 IP 地址和 ASN 两种网络资源的授权认证,防止前缀劫持类的安全威胁.BGPcoin 用链上的公共账本记录所有网络资源所有权变化的交易事务,并支持对其使用情况进行追溯,从而保证网络数字资源所有权和租用权的监管.BGPcoin 由两个主要的组件组成:一是规定系统协议,并作为区块链资源管理接口的智能合约;二是与智能合约交互的客户端,用于用户进行资源检索.其智能合约的功能分为两类——资源交易记录和资源检索,且都兼具网络地址聚合的存储与更新.如图 5 所示,BGPcoin 在 IANA、RIR、ISP 等 5 种类型的网络实体完成网络 IP 地址的注册、分配、下发和撤回,以及 ASN 的注册、分配和更新.文献[18]扩展了 BGPcoin,增加了 ROA 认证功能.该工作利用 RIR 公开数据库等现网数据中的 IP 地址和 AS 的注册和分配信息,复现了网络资源注册、分配和下发的过程;搭建了以太坊本地仿真网络,验证了 BGPcoin 的性能与可扩展性;并在以太坊官方测试网络

Ropsten 中模拟了资源交易事务以验证可行性.但由于现有测试网络中对账户余额的限制,其仿真实验规模有限,无法判别其在实际使用中争取记账权的时间消耗和在实际互联网复杂情况下的运行情况.

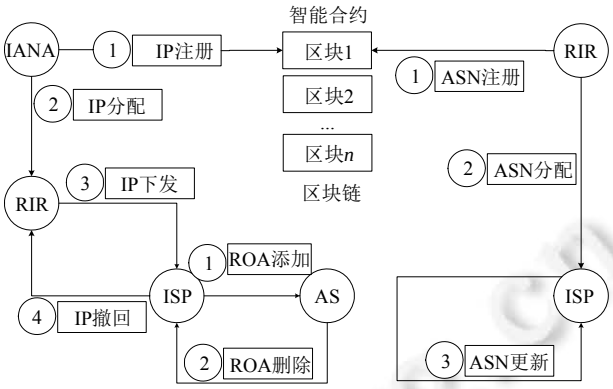

Fig.5 Workflow of BGPcoin

图 5 BGPcoin 的工作流程

Paillisse 等人提出了 IPchain[19],利用区块链来保证 IP 地址从 IANA 到 RIR 再到 ISP 和客户端逐级下发分配的真实性和可追溯性.基于以下原因,IPchain 使用了 PoS 共识机制对 IP 地址进行管理:第一,拥有更多 IP 地址资源的机构通常都有互联网维护相关的业务,更希望网络能够正确、安全地运行,应该有更大概率的记账权;第二,拥有更多 IP 地址资源的机构通常没有动机出售或转交自己的 IP 地址资源,基于 PoS 共识机制的 IPchain 面临的收购安全隐患较小,即,攻击者会从其他主体那里购买大量代币来获得更多的对区块链的控制权的概率较小;第三,PoS 不需要特殊的硬件支持和高昂的算力开销,这降低了该类应用使用区块链进行共同协作的门槛.图 6 展示了 IPchain 工作流的一个例子:当路由器 $R1$ 在链上写入自己的合法前缀后,该路由通告在网络传播时被中间某恶意路由器修改了该前缀的所有权,当路由器 $R3$ 接收到 150/8 to $R2$ 的通告后,可以在区块链中进行核对,确认该前缀是否的确是 $R2$ 的合法前缀.在此应用情景中,该通告即被视为无效通告.该工作实现了开源的原型系统,搭建了支持与软件路由器覆盖网络(open overlay router,简称 OOR)[46]交互的私有区块链.在已发表的 RFC 草案[47]中,对 IPchain 用于 IP 前缀分配下发的适用性和可行性进行了分析,并指出,利用 PoS 共识机制可以在保证安全性的前提下节省存储开销.但 IPchain 中 PoS 共识机制决定了拥有更多网络资源的实体会拥有更多的区块链控制权,这意味着 IANA 等当前 IP 地址资源管理机构有可能几乎拥有整个区块链的控制权,有悖于区块链应用于网络资源管理去中心化的初衷,也存在着对上层资源提供者的信任问题,以及链上信任中心化与分布式控制之间的权衡问题.

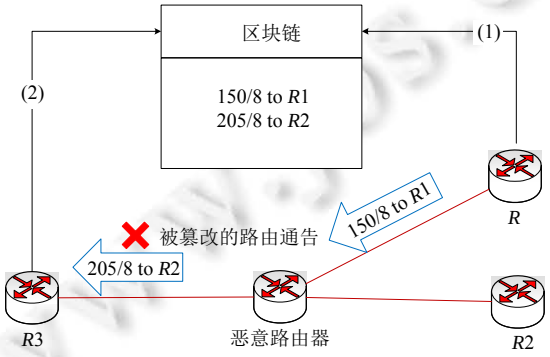

Fig.6 Sample usage scenario of IPchain

图 6 IPchain 的使用情景

Stefano 等人利用以太坊中的智能合约实现了用于 IP 地址管理的分布式自治组织(distributed autonomous organization,简称 DAO)[20],称其为 InBlock,对 IP 地址分配与管理开展实验.其中,收费机制模仿了现有 RIR 的收费方式,任何给 InBlock 提交了虚拟货币的实体,可以请求分配和保留地址.费用机制的引入,也可以阻止一些资产恶意囤积和浪费行为.InBlock 利用分布式的共识来达到非中心化的信任管理,并利用合适的物质激励来保护 IP 地址等资源,提供了一种分布式、自动化、不可逆、防篡改、公开可用并且匿名化的 IP 分配机制,并可作为一个权威的数据库来保证路由系统的安全.考虑到绝大多数 IPv4 地址已被分配,该工作目前仅从 IPv6 地址空间中选取了部分地址用于分布式互联网资源管理实验,但其工作对下一步验证收费机制和安全风险等问题的研究具有启发和借鉴意义.

表 2 总结了目前基于区块链的 IP 地址管理方法的共识机制、实现方式、实验规模、性能测试等情况.BGPcoin 分别在以太坊本地仿真网络和官方测试网络 Ropsten 中开展了实验,实验规模为 70 000 交易量,区块确认时间平均为 25s,吞吐量平均能达到每秒 5 个交易;IPchain 实现了基于 PoS 共识机制的私有链原型系统,使用云设备中部署在世界各地的 9 个虚拟机,复现了遵循“IANA-RIR-ISP-端用户”层次结构的 IP 过程,实验规模达到 200 000 交易量,其中,区块确认时间为 60s,吞吐量约为每秒 6 个交易;InBlock 在以太坊现有链开展了部分 IPv6 地址的实验,实验规模为 24 000 交易量,其区块确认时间与吞吐量分别为 18s 和平均每秒 10 个交易.

Table 2 Summary of blockchain-based IP origin authentication methods

表 2 基于区块链的 IP 地址授权认证机制总结

工作名称	共识机制	实现方式	实验规模(*k* trans)	性能测试结果	
				区块确认时间(s)	吞吐量(trans/s)
BGPcoin	PoW	本地仿真网络/Ropston	70	25	5
IPchain	PoS	原型系统	200	60	6
InBlock	PoW	以太坊现有链	24	18	10

2.2.2 基于区块链的路由认证

IETF 的 SIDR 工作组将 BGP 的路由认证分解为两个问题:一是 AS 源认证,即 AS 是否拥有通告某一 IP 前缀的合法授权;二是 AS 路径的完整性,即 BGP 路由报文中携带的 AS-path 信息是否与实际传播的路径一致.前者代表了真实性,后者代表了完整性.近期,一些研究工作尝试将区块链技术运用于解决域间路由安全中的路由认证问题,利用区块链技术来提供类似 RPKI 中 ROA 和 BGPsec 的功能,利用区块链的去中心化的优势解决 PKI 系统中信任根节点的垄断问题,使用多重签名真实、完整地记录所有的历史交易事件.

Internet Blockchain[16]中阐述了用于提供了 AS 源认证的功能的一种交易事务类型.图 7 展示了 IP 地址分配的创世区块交易事务流程,将互联网注册机构的区块链地址作为输入,将授权或租用给该机构的 IP 地址与该机构的区块链地址绑定作为输出.

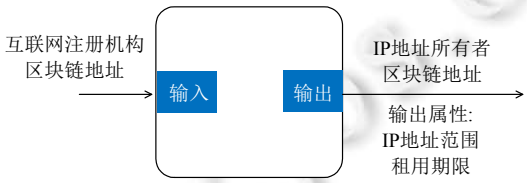

Fig.7 Genesis transaction for IP address allocation

图 7 IP 地址分配的创世交易事务

图 8 展示了用区块链记录将一个多宿主地址授权给 AS_1 和 AS_2,并通告其 IP 前缀的路由源认证过程.这种交易事务类型在 Internet Blockchain 中称为 ROA 事务.这样,网络对等体就可以验证网络资源的有效性并防止资源的双重分配.例如,当 IP 前缀地址 25.0.0.0/8 之前已经由地址 *B* 的注册处分配给 *A* 地址,则将该地址分配给 *A* 地址以外的其他地址的交易事务就会失败.根据当前网络资源分配的需求,每次交易都附带一个交易标签,用于

指示当前资源是否可以转交给其他的实体.比如一个注册机构可以重设关联 ISP 的 IP 前缀的交易事务标签,防止 ISP 将该 IP 前缀转交给其他机构.为了适应当前网络资源大多是被某些机构租用的应用需求,还支持在资源转交的交易中添加租用期限,当租用期满后,网络资源所属权将被归还给原所有者.在 Xing 等人最新的工作[18]中,增加了 ROA 的功能,增加了用于注册和验证 ASN 和 IP 地址块从属关系的子合约,允许任何一个 BGP 路由器直接从本 AS 内的以太坊客户端查询 IP 地址网络前缀与 ASN 的合法授权关系,从而避免多源冲突.

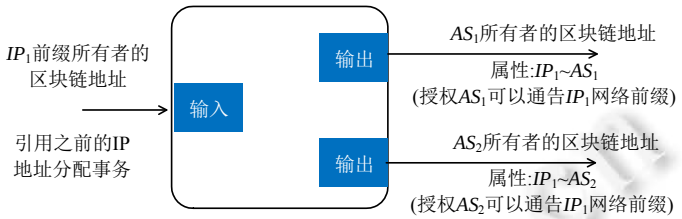

Fig.8 ROA transaction from a multi-homed site

图 8 多宿主地址的路由源认证交易事务

Internet Blockchain 定义了提供类似 BGPSec 的路径认证功能的交易类型.当 BGP 路由器在 BGP 更新报文中通告对应某个 IP 子网前缀的 AS-path 时,创建一个 BGP 通告事务.每一个 BGP 通告都将从上游 AS 路径作为该事务的输入,继续传播 BGP 更新消息的目的下游 AS 作为输出,这些下游 AS 在传播该更新报文时都将前面的 ASN 添加至 AS-path 序列中.同时还支持相应的 BGP 撤回操作,可根据需求撤回之前通告的路由信息.图 9 展示了使用该交易事务类型完成路径认证的过程.假设 AS_1 首先给 AS_2、AS_3 通告了 IP 前缀 IP_1 并创建了一个 BGP 通告事务,将 IP 前缀 IP_1 的 ROA 事务作为自己的输入,发送给 AS_2 和 AS_3.接下来,如果 AS_2 将这条路径通告给 AS_4,就会创建一个新的 BGP 通告事务,将从 AS_1 收到的交易事务内容作为输入,AS_4 作为输出.当 AS_4 在 BGP 更新报文中通告 AS_4-AS_1-IP Prefix IP_1,则其对等实体很容易验证出 AS_4 不能通过 AS_1 向 IP 前缀 IP_1 发送数据包.这是因为在 AS_1 在链上公布的交易事务信息中,只列出了 AS_2 和 AS_3 作为 IP 前缀 IP_1 的接收者,并不包括 AS_4.虽然 Internet Blockchain 提出了路由认证的思想和方案,但并没有对其进行具体实现,目前也没有区块链用于路由认证的具体测试性能结果.

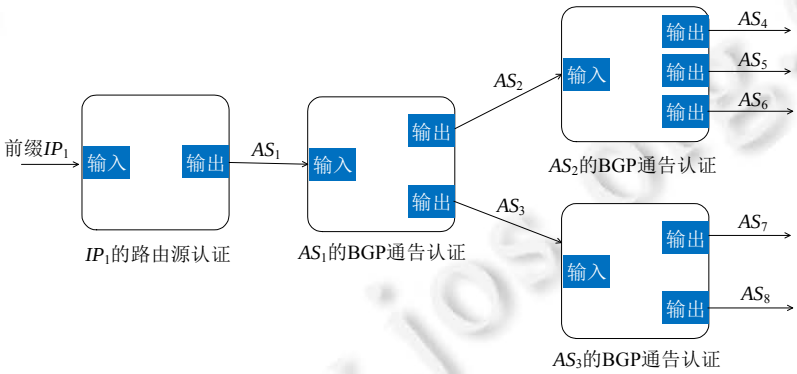

Fig.9 BGP advertisement transactions

图 9 BGP 通告交易事务

文献[21]中,基于区块链技术设计了一个信任管理系统 SBTM(secure blockchain trust management),将基于区块链的 PKI 系统 Certcoin[48,49]用于现有域间路由安全机制(如 S-BGP,So-BGP)的证书管理下发具体操作中.SBTM 并没有提出新的安全协议,只是利用区块链为现有用于域间路由认证的安全机制密钥管理和增量部署提供了一种信任管理机制.但该设计方案存在区块链自身认证与防篡改功能与现有安全机制功能设计上的冗余,且文献[21]只给出了初步的性能和可行性分析.

2.3 基于区块链的域间智能管理

为了解决在第 1.1 节中所分析的影响域间路由安全的操作失误类型异常,一些研究工作开始尝试融合区块链技术开展分布式域间智能管理,为各自治域之间提供智能域间协作、路由更新、故障恢复解决方案.

文献[22]设计了一种智能域间代理来辅助人工操作和配置,以完成域间自治管理,提出了一种域间自治架构 A2RD(autonomous architecture over restricted domains),文献[50]进一步给出了其技术细节.图 10 展示了 A2RD 的设计架构,A2RD 通过对由网络操作员、工程师、研究者撰写的各类 IETF 或 IRTF 标准化文档形成的训练数据集进行语义学习,形成知识库,为本地自治域智能管理提供指导.每个 AS 可根据自己的意愿在本地配置 A2RD,为了让不同自治域的智能代理共享知识库,提高它们沟通协作的安全性和智能性,使用区块链为各自治域的 A2RD 提供域间知识库的共识存储平台,称其为 IIBlockchain(Internet infrastructure blockchain),在每个域部署的 A2RD 智能代理基于区块链交互加密和认证信息.如图 10 所示,链上的区块中记录了每个 A2RD 智能代理的内部数据及其所在 AS 的环境参数,这些信息的交互使得各自治域可以在保留自治权的情况下开展协同合作.虽然该工作分析了 IIBlockchain 的区块空间规模和实现算法的时间复杂度,但并未给出具体的测试结果,也没有对其智能决策结果进行准确性评估.

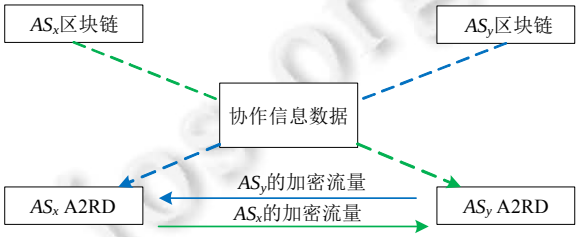

Fig.10 IIBlockchain architecture implemented over AS_x and AS_y domains

图 10 AS_x 和 AS_y 之间实现的 IIBlockchain 架构

Raphael 等人在文献[23]中借助区块链去中心化信任的属性,设计了一种灵活、透明的多域间网络服务生命周期管理体系架构,支持端到端可分片的服务级一致协议(service level agreement,简称 SLA),并实现了 DApp 开源原型系统,如图 11 所示.

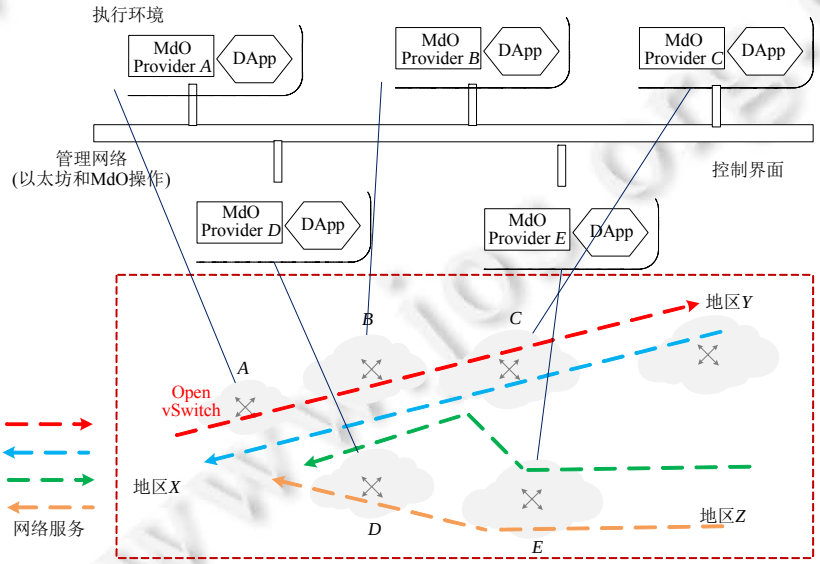

Fig.11 Demo scenario of the MdO/DApp prototype

图 11 MdO/DApp 原型系统演示场景

在该原型系统中使用了一系列开源组件(如以太坊、OVS、Neo4j、Ryu/OpenFlowv1.3、ARIA/TOSCA),实现了基于身份管理机制智能合约的 DApp,用于远程多重管理域间协作(multi-domain orchestrator,简称 MdO),使得只有得到授权的实体才能在 MdO 中完成特定任务.此外,利用区块链可以记录在网络服务生命周期中事件的工作流,从而能够对互联网资源的部署、配置及监测过程中的交互过程保持追溯状态.利用定制的智能合约,可以完成基于网络服务状态的事件触发(如流量过载等)以及协作式 MdO 行为.虽然该工作目前仍处于概念验证的实验阶段,但其对于面向多域间网络服务生命周期管理的开源区块链网络设计组件的实现,涵盖了基于事件触发的交互组件、对数据平面的综合考虑、AS 之间的商业协议关系等,进一步激发了对域间多重管理技术的讨论、研究与实现[51,52].

2.4 基于区块链的DDoS攻击防御和缓解

对于在第 1.1 节中阐述的域间路由系统在数据平面面临的安全威胁,分布式拒绝服务(distributed denial of service,简称 DDoS)是其主要攻击手段之一,攻击者可利用 DDoS 攻击使域间路由系统关键节点/链路失效,进一步导致域间路由系统震荡和级联失效.现有的 DDoS 防御机制缺乏应对攻击的资源可协调性和灵活性,区块链和智能合约等新技术的出现,可以使攻击信息以分布式自动化的方式进行共享.

Rodrigues 等人设计了一种基于智能合约和区块链技术的新型架构,提供了更为灵活、有效的多域间 DDoS 缓解方案[24].利用区块链和智能合约的分布式架构,在各个自治域之间自动并分布式地共享攻击信息(如 IP 地址的黑名单和白名单)并达成全局共识,实现在多个自治域之间完成灵活、有效 DDoS 攻击缓解目标.该架构可以作为现有 DDoS 防御系统的补充安全机制,替代构建专有注册机构和其他分布式机制在多域间共享信息.目前,该架构使用 SDN 网络作为用例,能够在多域间以更快速的方式开展流量识别与验证,以缓解 DDoS 攻击.但该工作并不局限于在 SDN 网络中使用,且能够支持与现有导出攻击信息的检测监控工具兼容,将攻击信息在链上公开发布.图 12 展示了该系统的应用场景:AS *C* 中的 Web 服务器正在遭受来自其他域(AS *A*,AS *B*,AS *C*)中设备的 DDoS 攻击,如果利用非协作式的缓解方法,该 Web 服务器只能依赖于本地的防御机制,但由于在多数情况下攻击流量源的距离较远,攻击流量在传播中会在很多 AS 中过载.利用基于智能合约的协作式防御机制,当 Web 服务器被攻击时,被攻击的用户或 AS 可以将攻击者的 IP 地址等信息在智能合约中存储下来,签署该智能合约的所有 AS 都会收到需被封锁的地址,并通过流量分析和目标地址验证来确认攻击的真实性,进而根据本地域的安全策略和机制自动触发缓解策略.文献[25]中提出了新型硬件部署方法 BloSS(blockchain signaling system),简化了在协作网络 DDoS 防御系统发送 DDoS 攻击信号的过程,建立了在多域间协同防御 DDoS 攻击的经济激励,并降低了协作的运营成本.

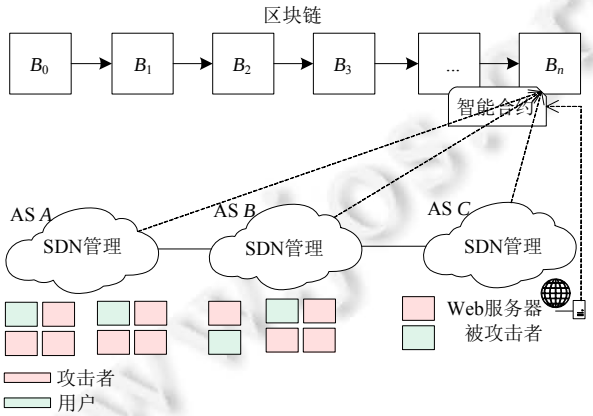

Fig.12 Application scenario of blockchain-based architecture for collaborative DDoS mitigation

图 12 基于区块链的多域协作 DDoS 缓解架构应用情景

与 IETF 提出的跨域协作 DDoS 防御协议 DOTS(DDoS open threat signaling)协议和基于特定协议的 DDoS

防御系统比较,基于区块链和智能合约的 DDoS 防御缓解技术作为一个天然的分布式架构,不需要在多域间建立专用注册机构和其他分布式的协同机制或协议.但由于对于大规模攻击,智能合约的规模和开销较大,只适用于小规模或中等规模的攻击,文献[24]只给出了该系统的设计方案,并未进行实际部署和实验验证.这种基于区块链技术的域间协作,可为域间路由数据平面的攻击溯源提供新的研究思路.

3 问题挑战与研究展望

如本文第 2.3 节的分析,传统域间路由前摄性防御机制存在着部署困难、管理复杂以及所依赖的信任基础架构信任中心化等问题.基于区块链的域间路由安全方案能够在去中心化、防篡改、交易透明等条件下,提供与 RPKI 等传统方案类似的功能,解决了传统方案存在的部分问题,但由于区块链的引入,也带来了一些新问题和新挑战.本节首先分析了基于区块链的域间路由安全方案的技术优势,然后分析了其在性能与开销、兼容性与增量部署、区块链自身安全性方面新的问题与挑战,最后对该方面的研究工作进行展望.

3.1 区块链应用于域间路由安全领域的优势

与传统的域间路由前摄性防御机制相比,基于区块链的域间路由安全方案的优势主要体现在管理自动化和信任基础架构去中心化两个方面.

(1) 管理自动化

传统的域间路由前摄性防御机制采用集中式管理和人工管理方式,对网络管理员的要求较高,可能存在网络资源的多重分配,也不易进行域间协同完成诸如防范 DDoS 攻击、故障恢复等任务.基于区块链的分布式信任架构可以规避集中式证书管理的复杂操作和单点失效问题,降低管理操作占用的带宽资源;基于区块链的网络资源分布式认证技术,可以确认网络资源的唯一所有权;IIBlockchain 等基于分布式智能代理和智能合约的域间管理方案,可以使各自治域进行自动化协同,完成事件触发、智能资源分配和更新路由等任务;基于智能合约和区块链,可以在没有专有可信注册机构和其他分布式协同机制和协议的情况下,在各自治域间自动共享攻击信息,协同完成域间 DDoS 防御与缓解等任务.

(2) 信任基础架构去中心化

如第 1.2 节的分析,在诸如 SoBGP、SBGP 等基于 PKI 的域间防御机制中,采用中心化的证书认证体系,可信实体完成从分布式资源库中收集对象,在可信资源库中进行日志记录,利用密码算法完成 IP 地址前缀、路由源、路径认证,并向 BGP 边界路由器输出认证结果供其进行路由决策.这些方法存在着信任基础架构信任中心化和管理复杂等问题,一旦发生权威中心的行为不可信、被第三方恶意攻击、网络资源的多重分配等情况,会造成域间防御机制失效,给整个域间路由系统的稳定运行带来巨大的影响.此外,这种传统防御机制提供的资源认证大多是利用资源库来存储属于自己加密管理的资源对象,但在这些资源库中并不能做到对所有 IP 前缀、AS 路径等资源完成精准的映射.由于这些资源库的管理缺乏监管,还有可能会引发镜像攻击[53],或是在下发分配资源中的循环依赖问题[13].

基于区块链技术,可以构建不依赖单一可信实体的分布式信任体系,形成一种基于去中心化信任基础架构的域间路由安全方案.这种方案解决了传统方案的部分缺陷,其优势如下:第一,可以避免单点失效的风险,健壮性和抗攻击性较强;第二,采用基于时序增长的链式哈希加密方法,形成可追溯防篡改的链上时序事务记录,对域间路由系统中网络资源及交易过程进行分布式记录、存储、协作及维护,提供基于历史交易的信任机制,从而避免权威机构的不当行为带来的安全隐患;第三,不需要对信任机构管理、证书管理等一系列复杂管理过程,提供了更为灵活、易于管理的信任机制;第四,基于区块链技术,提供了精准的资源所有权认证,即在每一次资源分配下发的过程中都建立了明确的资源所属权,从而避免了传统方案存在的镜像攻击、资源下发分配中的循环依赖等问题.

3.2 基于区块链的域间路由安全方案存在的问题和挑战

作为一个新兴的研究领域,区块链应用于域间路由安全的研究和工程实践都处于起步阶段,本节从性能与

开销问题、兼容性与增量部署问题以及区块链自身安全问题这 3 个方面对该领域的问题和挑战进行了分析.

3.2.1 性能与开销问题

从目前区块链应用于域间路由安全的研究和实践来看,能否构建一个互联网规模并拥有足够带宽和存储资源的区块链,是一个重要的可行性问题.因为区块链支持的交易速率受限于网络规模和区块大小,时间和空间开销等可扩展性问题成为必不可少的考虑因素.

- 时间开销

比特币区块链区块的大小被限制在1MB,起初该设置主要是为了防止DoS攻击,避免少数矿工的恶意行为,但这样大小的区块所能承载的交易数非常有限.当前,比特币交易的一次确认时间平均大约是 10min,只能在每秒完成 3~7 个交易.相较于比特币区块链较低的交易效率和较长的确认时间,目前在以太坊中区块创建时间为13.6s,平均每秒可以处理 7~20 个交易.根据 BGP 不稳定报告[54],截至 2019 年 1 月,域间路由系统的每天 BGP 大量路由更新(BGP churn)数量从 2016 年到 2018 年底一直稳定在 170 000 个左右,即每秒平均前缀更新为 2 个;但在 2018 年底的最后几周,达到了每天 700 000 个的峰值,即每秒平均前缀更新为 8 个.可以看到:目前,现有的比特币区块链提供的交易时延和吞吐量不能满足域间路由系统的性能需求,但以太坊区块链对于达到处理域间路由系统峰值更新需求的目标具有较大潜力.

值得关注的是,近期有许多研究正在试图解决区块链的交易速率和可扩展性问题.比如:Bitcoin-NG[55]可以用于节省挖矿竞争的时间;侧链(sidechain)和闪电网络微支付渠道(payment channel)为主区块链的交易迁移提供了启发式解决方案,可以依托主链实现 DNS 和 BGP 事件交易记录分别存储;更多的共识机制,如 PoS、DPoS、重要性证明 PoI[44]、Casper[45]等,可以为根据域间路由系统可扩展性需求定制的私有链安全解决方案提供支撑.

- 空间开销

区块链随着时间不断增长,带来了潜在的可扩展性问题.目前,成熟的区块链(如比特币区块链)需要超过100GB 的存储空间,预计在 2034 年,比特币区块链的规模将达到 900GB.考虑 AS 与/24 前缀 IP 地址块映射的区块链规模达到将近 600GB,只记录 IP 前缀和 BGP 路由表增长的情况,在 20 年内规模将达到约 40GB,与 BGP 路由更新的增长接近一致[47].

简单地删除或归总历史交易会降低基于 PoW 共识机制的区块链安全性,因为其安全性依赖于生成区块的算力.其他的共识机制(如 PoS,DPoS 等)不依赖于算力,所以空间存储策略并不降低其安全性.最简单、直观的处理方式即链上存储空间达到某一规模,可以将旧交易归总为一个子集.设计定制的专用私有链也可以解决区块链的空间存储问题.例如:基于区块链的 DNS 的分布式命名系统 Namecoin[56]将域名和值的映射直接存储在区块链中,提供了分布式域名解析管理功能;然而,Namecoin 的域名的最大长度是 64 字节,这会导致区块链的增长速度过快.Blockstack[57]在 Namecoin 的基础上进行了改进,使用逻辑分层结构,自下向上分为区块链层、路由层和存储层;区块链层仅用于为用户在系统上的操作(如注册和更新域名等)达成共识,路由层负责区域文件散列值到区域文件路径的映射,存储层存放着加密的用户数据.Blockstack 这种将命名系统逻辑与共识机制分离的设计不仅增强了数据存储能力,还使得逻辑层能够独立地演进和扩展,具有较重要的借鉴意义.

3.2.2 兼容性与增量部署问题

与 RPKI 等方案类似,基于区块链的域间路由安全方案如果在全网范围内部署,将会是一个规模浩大的工程,并且会对互联网的稳定性产生影响.因此,这些方案与现有域间路由协议的兼容性与增量部署问题是将要面临的重要挑战.

- 兼容性问题

如果要利用区块链记录 BGP 更新通告,需要解决与现有 BGP 协议的兼容性问题.如何在保证现有 BGP 正常运转的前提下,对其中的更新通告进行接近同步的记录和认证,是基于区块链的域间路由安全方案可行性的关键问题.Internet Blockchain[16]提出了一种解决方案,为了保证通告交易正常记录和 BGP 更新消息正常传播,每个 AS 在进行 BGP 通告时,使用区块链交易消息取代更新消息.如图 13 所示:在 BGP 路由器前面加入一个转换器,将发出的BGP更新转换为通告交易消息的形式发送给相邻的AS,并在链上完成公布和记录,相邻AS再把

收到的通告交易消息转换为 BGP 更新消息,以供 BGP 路由器处理.用这种方式,现有 BGP 协议无需做出改变.由于两种消息模式都提供相同的语义信息,因此在转换过程中没有信息损失.然而,区块链发布区块是周期性的,而 BGP 需要实时处理输入的消息,如何达到快速收敛,使得 BGP 更新报文消息与区块链通告基本能够保持同步,仍然是需要解决的关键问题.

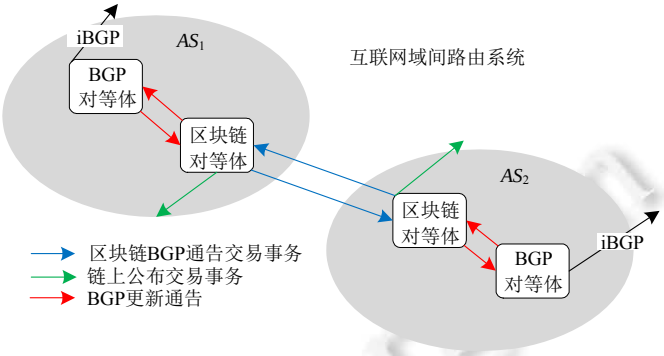

Fig.13 Integrating BGP update with BGP advertisement transactions

图 13 BGP 更新与通告集成交易事务

- 增量部署问题

域间路由安全机制需要全网协作才能完成,不可能一蹴而就,因此,增量部署是基于区块链的域间路由安全方案部署的关键途径,其部署过程可以从保护的资源范围和地理范围两个维度进行.

- 从资源保护类型的维度,可以渐进式地开展资源保护:首先,可以提供类似 RPKI 的记录和认证 IP 地址所有权和源路由的功能;进而提供类似 BGPSec 的记录和认证 AS 路径和 BGP 更新通告的功能;最后,提供类似 DNSsec 的域名安全等功能;
- 从地理范围的维度,基于区块链的域间路由安全方案可以首先部署在使用 BGP 提供网络可达性信息的 SDN 控制器对等实体中,在企业内部或云内部设立 BGP 交易的分布式账本,然后可以扩展到多个协作的互联网交换中心(Internet exchange point,简称 IXP)或软件定义的互联网交换中心(software defined Internet exchange,简称 SDX)[58]之间,最后扩展到整个互联网.

3.2.3 区块链自身安全问题

虽然区块链技术自提出以来,展现了广阔的应用前景,但区块链自身还存在很多安全问题.

使用工作量证明 PoW 的区块链 1.0 和区块链 2.0 共同的安全问题有 51%攻击[59]、私钥安全[60]、双花攻击[61]、交易事务隐私泄露[62]等.区块链 2.0 还面临智能合约和以太坊虚拟机(Ethereum virtual machine,简称 EVM)设计缺陷导致的安全脆弱性[63,64]问题.PoS 共识机制也存在一系列安全风险及隐患,如无利害攻击(nothing at stake)风险[65]、远程攻击(range attack)[66]、参与度不足以及垄断问题等.此外,区块链底层用于交换信息的 P2P 网络结构也存在遭受 DDoS 攻击、交易洪泛、路由攻击等风险.

虽然目前区块链技术还不够成熟,其共识机制和交互过程依然面临诸多安全隐患,但已有大量的工作研究和解决区块链中的安全问题,新的共识机制和解决方案层出不穷.针对域间路由安全的具体需求,可以设计定制隐私度和安全性较高的私有区块链;此外,在金融系统中,参与者会为了自己的私人财产积累,不惜以较大的代价进行攻击,而互联网生态系统却不同于金融系统,在互联网系统中的大多数参与者都希望能够达成一致、有序的安全网络环境,攻击者是少数实体,这也降低了基于区块链域间路由的安全风险和隐患.

3.3 区块链应用于域间路由安全领域研究展望

虽然区块链技术应用于域间路由安全仍然面临许多问题与挑战,但区块链去中心化、防篡改、可追溯等天然属性给域间路由网络资源信任管理提供了新的思路和方法.区块链领域提出的新型共识机制为针对域间路

由系统应用情景的私有链提供了更多可能;区块链用于数字货币交易的功能为改进现有网络收费机制提供了新的解决思路;在网络层次扁平化、端到端服务不断增长的新网络环境中,区块链技术提供了更多应用潜能.本节给出了在该领域的研究中,关于共识机制设计、以新型收费机制激励部署、在网络应用中更多潜能方面的一些思考和展望.

- 定制化的共识机制设计:从域间路由系统的应用场景和需求出发,可以考虑设计更加定制化的区块链,尤其是其中的共识机制设计.现有的许多共识机制[44,45,55]在记录资源交易的同时还考虑了网络节点的交易量和交易对象,进而评估节点的重要度和可信度.这些共识机制的设计思想可以借鉴到域间路由系统安全设计中,在网络资源交互和路由更新的同时,评估各 AS 域的可信度,并加入相应的奖惩机制.例如,文献[67]借鉴 PoW 工作量证明的思想,引入了互联网资源证明(proof of networking,简称 PoN)的概念,将持有的网络资源,如带宽、计算校验和 BGP 对等体的数量等作为衡量标准.采用这种共识机制的设计,只要半数以上的网络资源掌握在非恶意的网络参与者中,域间网络的安全就基本可以得到保证.这一方向的研究仍处于起步阶段,仍然有许多值得研究和探索的问题;
- 以新型收费机制激励部署:区块链的产生起源于数字货币,在基于区块链的域间路由安全方案中,可以考虑关联数字货币,使网络服务付费更加便捷、安全,并激励网络运营商和网络使用者参与到方案的部署中.网络运营商提供的是网络资源和信息传输服务的租赁,是这些服务的供给侧,它们可以考虑将这些服务供给及其收费结合到区块链交易中,并根据需求侧的具体需求和使用情况进行定制化收费.例如,可以根据用户以往流量转发的具体情况对其进行收费.已有的实验结果[18,20]表明:采用以太坊对网络资源管理的开销,比传统方式互联网管理的开销低;并且可以通过在进行网络资源交易时,增加需求侧的记账奖励并降低其按需服务的费用,使供给侧和需求侧都有更多参与记账和验证的愿望,以促进基于区块链技术的域间路由安全方案的增量部署;
- 在网络应用中的更多潜能:当下互联网环境不断演变,愈来愈多的大型内容分发网络——对等基础设施、网络交换点 IXP、定制化的跨域网络服务,使得网络层次趋于扁平化发展,面临着更多新型威胁,在域间乃至全球范围内部署具有联动功能的安全机制的需求也越来越迫切.基于区块链的域间路由安全方案,除了能够提供类似 RPKI、BGPSec 和 DNSSec 的功能之外,还具备现有传统安全架构无法提供的潜在功能.例如,可以将细粒度的流式路由指令与 BGP 通告交易相结合,为其流量转发提供可信服务;利用区块链节点的信用度评估作为域间路由系统中客户 AS 选择其上游服务提供 AS 的依据,提供更加可信可靠的路由策略;根据商业需求,利用智能合约定制端到端可分片的 SLA,实现自动化的多域管理与决策等.区块链的可编程属性使得基于区块链的网络资源管理和域间路由安全机制有更多待挖掘的潜能,可以为新型网络的资源管理的自动化、智能化提供重要的技术支撑;同时,SDN、NFV 等新型网络的不断发展,为区块链在域间路由安全中的应用与部署提供了更为广阔的发展空间.

4 结束语

域间路由安全对于整个互联网稳定运行至关重要.区块链技术因其分布式、防篡改、可追溯等特点,为多自治域间的地址资源分配、路由认证、智能管理等需求提供了“去信任中心化”、“有共识”的技术基础和新的研究思路与解决方案.本文梳理了域间路由安全脆弱性与传统域间安全机制的瓶颈与不足,综述了区块链技术应用于域间路由认证、域间智能管理、域间 DDoS 攻击防御和缓解等域间路由安全领域的研究,分析了基于区块链的域间路由安全方案的优势及其在性能与规模、兼容性与增量部署和区块链自身的安全方面的问题和挑战,并展望了该领域的研究和发展.本文希望能为区块链应用于域间路由安全研究领域的下一步研究工作提供参考与启发.

References:

[1] Rekhter Y, Li T, Hares S. A border gateway protocol 4 (BGP-4). 2006. https://tools.ietf.org/html/rfc4271

[2] Nordström O, Dovrolis C. Beware of BGP attacks. ACM SIGCOMM Computer Communication Review, 2004,34(2):1−8. [doi: 10.1145/997150.997152]

[3] Ratul M, Wetherall D, Anderson T. Understanding BGP misconfiguration. ACM SIGCOMM Computer Communication Review, 2002,32(4). [doi: 10.1145/633025.633027]

[4] Li S, Zhuge JW, Li X. Study on BGP security. Ruan Jian Xue Bao/Joumal of Software, 2013,24(1):121−138 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4346.htm [doi: 10.3724/SP.J.1001.2013.04346]

[5] Giotsas V, Luckie M, Huffaker B. Inferring complex as relationships In: Proc. of the 2014 Conf. on Internet Measurement Conf. ACM Press, 2014. 23−30. [doi: 10.1145/2663716.2663743]

[6] Kent S, Lynn C, Seo K. Secure border gateway protocol. IEEE Journal on Selected Areas in Communications, 2002,18(4):582−592. [doi: 10.1109/49.839934]

[7] White R. Securing BGP through secure origin BGP (soBGP). Business Communications Review, 2003,33(5):47.

[8] Lepinski M, Kent S. An infrastructure to support secure internet routing. RFC 6480, 2012.

[9] Lepinski M, Kent S, Kong D. A profile for route origin authorizations (ROAs). RFC 6482, IETF, 2012.

[10] Lepinski M, Sriram K. BGPSEC protocol specification. RFC 8205, 2017.

[11] Sermpezis P, Kotronis V, Dainotti A, Dimitropoulos X. A survey among network operators on BGP prefix hijacking. ACM SIGCOMM Computer Communication Review, 2018,48(1):64−69. [doi: 10.1145/3211852.3211862]

[12] Sharon G. Why is it taking so long to secure internet routing? Queue, 2014,12(8):20−33. [doi: 10.1145/2668152.2668966]

[13] Cooper D, Heilman E, Brogle K, Reyzin L, Goldberg S. On the risk of misbehaving RPKI authorities. In: Proc. of the 12th ACM Workshop on Hot Topics in Networks. ACM Press, 2013. 16. [doi: 10.1145/2535771.2535787]

[14] Gilad Y, Cohen A, Herzberg A, Schapira M, Shulman H. Are we there yet? On RPKI's deployment and security. In: Proc. of the Network and Distributed System Security Symp. 2017. [doi: 10.14722/ndss.2017.23123]

[15] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. https://bitcoin.org/bitcoin.pdf

[16] Hari A, Lakshman TV. The Internet blockchain: A distributed, tamper-resistant transaction framework for the Internet. In: Proc. of the ACM Workshop on Hot Topics in Networks. ACM Press, 2016. 204−210. [doi: 10.1145/3005745.3005771]

[17] Xing Q, Wang B, Wang X. Poster: BGPcoin: A trustworthy blockchain-based resource management solution for BGP security. In: Proc. of the 2017 ACM SIGSAC Conf. on Computer and Communications Security. ACM Press, 2017. 2591−2593. [doi: 10.1145/3133956.3138828]

[18] Xing QQ, Wang BS, Wang XF. BGPcoin: Blockchain-based Internet number resource authority and BGP security solution. Symmetry, 2018,10(9):408. [doi: 10.3390/sym10090408]

[19] Paillisse J, Ferriol M, Garcia E, Latif H, Piris C, Lopez A, Kuerbis B, Rodriguez-Natal A, Ermagan V, Maino F, Cabellos A. IPchain: Securing IP prefix allocation and delegation with blockchain. arXiv:1805.04439, 2018. https://arxiv.org/abs/1805.04439

[20] Angieri S, Garciamartinez A, Liu B, Yan Z, Wang C, Bagnulo M. An experiment in distributed Internet address management using blockchains. arXiv:1805.04439, 2018. https://arxiv.org/abs/1805.04439

[21] de La Rocha Gómez-Arevalillo A, Papadimitratos P. Blockchain-based public key infrastructure for inter-domain secure routing. In: Proc. of the Int'l Workshop on Open Problems in Network Security (iNetSec). Rome, 2017. 20−38.

[22] Braga J, Silva JN, Endo PT, Ribas J, Omar N. Blockchain to improve security and knowledge in inter-agent communication and collaboration over restrict domains of the Internet infrastructure. arXiv:1805.05250, 2018. https://arxiv.org/abs/1805.05250

[23] Rosa RV, Rothenberg CE. Blockchain-based decentralized applications meet multi-administrative domain networking In: Proc. of the ACM SIGCOMM 2018 Conf. on Posters and Demos. ACM Press, 2018. 114−116. [doi: 10.1145/3234200.3234217]

[24] Rodrigues B, Bocek T, Lareida A, Hausheer D, Rafati S, Stiller B. A blockchain-based architecture for collaborative DDoS mitigation with smart contracts. In: Proc. of the IFIP Int'l Conf. on Autonomous Infrastructure, Management and Security. Cham: Springer-Verlag, 2017. 16−29. [doi: 10.1007/978-3-319-60774-0_2]

[25] Rodrigues B, Bocek T, Stiller B. Enabling a cooperative, multi-domain DDoS defense by a blockchain signaling system (BloSS). In: Proc. of the 42nd IEEE Conf. on Local Computer Networks 2017 (LCN 2017). 2017.

[26] Murphy S. BGP security vulnerabilities analysis. RFC 4272, 2006.

[27] Gao LX, Rexford J. Stable Internet routing without global coordination. ACM SIGMETRICS Performance Evaluation Review, 2000,9(6):307−317. [doi: 10.1145/339331.339426]

[28] BGPmon Blog. BGP leak causing Internet outages in Japan and beyond. 2017. https://bgpmon.net/bgp-leak-causing-internet-outages-in-japan-and-beyond/

[29] Zhang Y, Mao ZM, Wang J. Low-rate TCP targeted DoS attack disrupts Internet routing. In: Proc. of the 14th Annual Network & Distributed System Security Symp. (NDSS 2007). San Diego: The Internet Society, 2007. 1−15.

[30] Schuchard M, Mohaisen A, Kune DF, Hopper N, Vasserman EY. Losing control of the Internet: Using the data plane to attack the control plane. In: Proc. of the Network and Distributed System Security Symp. (NDSS 2011). San Diego, 2010. 726−728. [doi: 10.1145/1866307.1866411]

[31] Qiu H, Li YF, Lan JL, *et al*. Research on cascading failure attack and detection of inner-domain routing system. Scientia Sinica Informationis, 2017,47:1715−1729 (in Chinese with English abstract). [doi: 10.1360/N112016-00259]

[32] Mitseva A, Panchenko A, Engel T. The state of affairs in BGP security: A survey of attacks and defenses. Computer Communications, 2018,124:45−60. [doi: 10.1016/j.comcom.2018.04.013]

[33] BGPmon blog large scale BGP hijack out of India. 2015. https://bgpmon.net/large-scale-bgp-hijack-out-of-india/

[34] BGPmon blog popular destinations rerouted to Russia. 2017. https://bgpmon.net/popular-destinations-rerouted-to-russia/

[35] Rekhter Y, Sangli SR. BGP extended communities attribute. RFC 4360, 2006. https://tools.ietf.org/html/rfc4360

[36] Siddiqui MS, Montero D, Serral-Gracia R, Masip-Bruin X, Yannuzzi M. A survey on the recent efforts of the Internet standardization body for securing inter-domain routing. Computer Networks, 2015,80:1−26. [doi: 10.1016/j.comnet.2015.01.017]

[37] Al-Musawi B, Branch P, Armitage G. BGP anomaly detection techniques: A survey. IEEE Communications Surveys & Tutorials, 2017,19(1):377−396. [doi: 10.1109/COMST.2016.2622240]

[38] Orsini C, King A, Giordano D, Giotsas V, Dainotti A. BGPStream: A software framework for live and historical BGP data analysis. In: Proc. of the 2016 Internet Measurement Conf. ACM Press, 2016. 429−444. [doi: 10.1145/2987443.2987482]

[39] Goodell G, Aiello W, Griffin T, Ioannidis J, McDanial P, Rubin A. Working around BGP: An incremental approach to improving security and accuracy of interdomain routing. In: Proc. of the Internet Society Symp. on Network Distributed Systems Security (NDSS), Vol.23. 2003.

[40] Wählisch M, Schmidt R, Schmidt TC, Maennel O, Uhlig S, Tyson G. RiPKI: The tragic story of RPKI deployment in the Web ecosystem. In: Proc. of the 14th ACM Workshop on Hot Topics in Networks. ACM Press, 2015. 11. [doi: 10.1145/2834050.2834102]

[41] Osterweil E, Manderson T, White R, McPherson D. Sizing estimates for a fully deployed RPKI. Technical Report, 1120005 version 2. Verisign, 2012.

[42] Bruijnzeels T, Muravskiy O, Weber B. RPKI repository analysis and requirements. 2013. draft-tbruijnzeels-sidr-repo-analysis-00

[43] Fischer MJ, Lynch NA, Paterson MS. Impossibility of distributed consensus with one faulty process. Journal of the Association for Computing Machinery, 1985,32(2):374−382. [doi: 10.1145/3149.214121]

[44] NEM.io Foundation. NEM tech reference. Technical Report, 2018. https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf

[45] Buterin V, Grith V. Casper the friendly finality gadget. Networking and Internet Architecture, 2017. 1710.09437.

[46] Rodriguez-Natal A, Paillisse J, Coras F, Lopez-Bresco A, Jakab L, Portoles-Comeras M, Maino F, *et al*. Programmable overlays via OpenOverlayRouter. IEEE Communications Magazine, 2017,55(6):32−38. [doi: 10.1109/MCOM.2017.1601056]

[47] Paillissé J, Rodriguez-Natal A, Ermagan V, Maino F, Cabellos A. An analysis of the applicability of blockchain to secure IP addresses allocation, delegation and bindings. IETF Draft-Paillisse-Sidrops-Blockchain-01, 2017.

[48] Fromknecht C, Velicanu D. CertCoin: A NameCoin based decentralized authentication system. Technical Report, 6.857 Class Project, Massachusetts Institute of Technology, 2014.

[49] Fromknecht C, Velicanu D. A decentralized public key infrastructure with identity retention. Technical Report, 803, Massachusetts Institute of Technology, 2014.

[50] Braga J, Silva JN, Endo PT, Omar N. A summary description of the A2RD project. arXiv:1808.09293, 2018. https://arxiv.org/abs/1808.09293

[51] Nakashima H, Aoyama M. An automation method of SLA contract of Web apis and its platform based on blockchain concept. In: Proc. of the 2017 IEEE Int'l Conf. on Cognitive Computing (ICCC). IEEE, 2017. 32−39. [doi: 10.1109/IEEE.ICCC.2017.12]

[52] Alowayed Y, Canini M, Marcos P, Chiesa M, Barcellos M. Picking a partner: A fair blockchain based scoring protocol for autonomous systems. In: Proc. of the Applied Networking Research Workshop (ANRW 2018). ACM Press, 2018. 33−39. [doi: 10.1145/3232755.3232785]

[53] Heilman E, Cooper D, Reyzin L, Goldberg S. From the consent of the routed: Improving the transparency of the RPKI. ACM Special Interest Group on Data Communication, 2015,44(4):51−62. [doi: 10.1145/2740070.2626293]

[54] Huston G. The BGP instability report. Techinical Report, 2018. http://bgpupdates.potaroo.net/instability/bgpupd.html

[55] Eyal I, Gencer AE, Sirer EG, Van Renesse R. Bitcoin-NG: A scalable blockchain protocol. In: Proc. of the 13th USENIX Symp. on Networked Systems Design and Implementation (NSDI 2016). 2016. 45−59.

[56] Kalodner H, Carlsten M, Ellenbogen P, Bonneau J, Narayanan A. An empirical study of Namecoin and lessons for decentralized namespace design. In: Proc. of the 14th Workshop on the Economics of Information Security (WEIS 2015). 2015.

[57] Ali M, Nelson J, Shea R, Freedman MJ. Blockstack: A global naming and storage system secured by blockchains. In: Proc. of the 2016 USENIX—Annual Technical Conf. 2016. 181−194.

[58] Vanbever M, Shahbaz SP, Donovan B, Schlinker N, Feamster J, Rexford S, Shenker R, Clark E, Katz-Bassett SDX. A software defined internetexchange. In: Proc. of the SIGCOMM. ACM Press, 2014. 551−562. [doi: 10.1145/2619 239.2631473]

[59] Douceur JR. The sybil attack. In: Proc. of the Int'l Workshop on Peer-to-Peer Systems. Cambridge, 2002.

[60] Mayer H. ECDSA security in bitcoin and ethereum: A research survey. In: Proc. of the CoinFaabrik. 2016. 126.

[61] Karame GO, Androulaki E, Roeschlin M, Gervais A, Čapkun S. Misbehavior in bitcoin: A study of double-spending and accountability. ACM Trans. on Information and System Security (TISSEC), 2015,18(1):2. [doi: 10.1145/2732196]

[62] Miller A, Moser M, Lee K, Narayanan A. An empirical analysis of linkability in the monero blockchain. Networking and Internet Architecture, 2017. 1704.04299.

[63] Atzei N, Bartoletti M, Cimoli T. A survey of attacks on Ethereum smart contracts (sok). In: Proc. of the Int'l Conf. on Principles of Security and Trust. 2017. 164−186. [doi: 10.1007/978-3-662-54455-6_8]

[64] Chen T, Li X, Luo X, Zhang X. Under-optimized smart contracts devour your money. In: Proc. of the 24th IEEE Int'l Conf. on Software Analysis, Evolution and Reengineering (SANER). 2017. 442−446. [doi: 10.1109/SANER.2017.7884650]

[65] Ethereum Foundation. Proof of stake FAQ. Techinical Report, 2018. https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ

[66] Buterin V. Slasher ghost, and other developments in proof of stake. Techinical Report, 2014. https://blog.ethereum.org/2014/10/03/slasher-ghost-developments-proof-stake/

[67] Ghiro L, Maccari L, Cigno RL. Proof of networking: Can blockchains boost the next generation of distributed networks? In: Proc. of the 14th Annual Conf. on Wireless On-demand Network Systems and Services (WONS). Isola, 2018. 29−32. [doi: 10.23919/WONS.2018.8311658]

附中文参考文献:

[4] 黎松,诸葛建伟,李星.BGP 安全研究.软件学报,2013,24(1):121−138. http://www.jos.org.cn/1000-9825/4346.htm [doi: 10.3724/SP.J.1001.2013.04346]

[31] 邱菡,李玉峰,兰巨龙,等.域间路由系统的级联失效攻击及检测研究.中国科学:信息科学,2017,47:1715−1729. [doi: 10.1360/N112016-00259]

陈迪(1992－),女,河南郑州人,博士生,助理研究员,主要研究领域为域间路由系统安全,区块链技术与应用.

朱俊虎(1974－),男,博士,教授,CCF 高级会员,主要研究领域为网络对抗,网络安全测试与评估.

邱菡(1981－),女,博士,副教授,主要研究领域为域间路由安全,网络安全模拟与评估.

王清贤(1960－),男,教授,博士生导师,CCF 高级会员,主要研究领域为网络安全.