高技术通讯 2022 年 第 32 卷 第 10 期:1004-1016

doi:10.3772/j.issn.1002-0470.2022.10.002

基于区块链的 BGP 路由策略检测机制①

冷 峰②* ** *** 赵 琦** 延志伟** 曾 宇③* **

(* 中国科学院计算机网络信息中心 北京 100190)

(** 中国互联网络信息中心 北京 100190)

(*** 中国科学院大学 北京 100049)

摘 要 针对路由传播过程中存在的自治域间策略违背的现象开展研究,提出边界网关协议(BGP)路由策略检测机制(BRPM2),设计包含策略链以及验证模块的系统架构。通过理论分析、原型设计与仿真验证,证明了提出的检测算法和系统架构可充分利用资源公钥基础设施(RPKI)技术资源,使 RPKI 依赖方承载验证功能并与路由器通信,实现功能解耦,便于部署应用。同时 BRPM2 具备验证方法简单、支持增量部署的优点,可在无需修改路由协议的前提下,提升域间路由系统安全。

关键词 资源公钥基础设施(RPKI); BGPsec; 路由决策; 区块链; 边界网关协议(BGP)路由策略检测机制(BRPM2)

0 引 言

互联网是由众多计算机网络相互连接组成的开放性网络,边界网关协议(border gateway protocol, BGP)是互联网网间寻址的事实性标准[1]。但由于 BGP 在设计之初并未充分考虑安全问题,BGP 存在较大的安全缺陷[2],导致安全事件时有发生。业界针对 BGP 安全问题广泛开展研究,着力提升互联网安全水平。

区块链(block chain)是一项新兴技术,具有去中心化、不可篡改、匿名性、可以追溯、集体维护等特性[3],是近年来业界广泛关注的热点技术。利用区块链技术解决互联网基础资源问题的研究陆续开展[4],针对传统互联网关键基础设施安全问题的研究已成为一个新的发展方向,其中利用区块链技术记录自治域(autonomous system, AS)间路由策略并验证路由传输过程中是否存在违规问题是一种可行的尝试。

本研究针对 AS 间策略违背的安全风险开展研究,提出一种利用区块链 2.0,即以太坊技术增强 BGP 协议安全的机制,是发现并检测路由系统潜在安全风险的有效手段,可与互联网码号资源公钥基础设施(resource public key infrastructure, RPKI)、BGPsec 协同配合,共同增强路由系统安全水平。主要研究内容包括以下几个方面。

(1) 设计出一种 BGP 路由策略检测机制(BGP routing policy monitoring mechanism, BRPM2),提出系统架构,阐述技术原理。

(2) 建立包含自治域路由策略等信息的策略链,确保自治域间路由策略无法被轻易篡改,设计区块链关键技术要点,包括基本区块、创世区块以及交易操作等环节的实现方法。

(3) 详细介绍 BRPM2 的代码逻辑以及修正后的 BGP 路由处理流程,并以实际案例的方式说明 BRPM2 的使用方法和运作机制。

(4) 建立原型系统,利用实验验证本机制的有

① 北京市科技新星计划(Z191100001119113)资助项目。

② 男,1982 年生,博士生;研究方向:互联网基础资源安全;E-mail:lengfeng@cnnic.cn。

③ 通信作者,E-mail: zengyu@cnnic.cn。

(收稿日期:2021-05-14)

效性及效能。

(5) 基于 RPKI 依赖方(relying party,RP)功能实现验证功能,使其与 BGP 路由器通信完成策略验证,实现功能解耦。同时对比 RPKI、BGPsec 以及 BRPM2 的异同,描述 BRPM2 的技术特征。

1　问题描述

1.1　BGP 协议概述

BGP 协议是连接自治域间的寻址协议。BGP 可被划分为外部边界网关协议(EBGP)以及内部边界网关协议(IBGP)。与 BGP 路由器建立对等连接的对端叫做 BGP peer。每个 BGP 路由器在收到 peer 传来的路由信息后,将存储在本地的数据库,并根据本地的策略(policy),结合路由信息中的内容进行判断,并根据需要修改路由器的主路由表。

1.2　BGP 面临的安全问题

BGP 安全问题长期存在,对互联网稳定运行构成严重威胁。典型的 BGP 安全问题包括闲置 AS 抢夺、近邻 AS 通告抢夺、长掩码抢夺、路由泄露以及路径缩短等几个方面[5]。以上安全问题并不仅仅停留在理论层面,利用以上安全问题而发起的网络安全事件时有发生[6]。黑客利用此类安全问题发起网络攻击的目的已经逐渐从单纯威胁互联网关键服务稳定运行向非法获取经济价值而转变。如 2018 年发生的亚马逊事件,亚马逊权威域名服务器遭到 BGP 路由劫持攻击[7],据称攻击者借助此次攻击窃取了价值可观的加密货币。Internet Society 的报告显示,2020 年上半年共发生 1430 起 BGP 劫持事件,日均发生 14 起[8]。可以预测的是,未来 BGP 安全问题仍会长期存在,在利益的趋势下,攻击者将利用 BGP 的缺陷制造出更多类型的攻击手段,对互联网安全稳定运行的影响不可忽视。

1.3　抵御 BGP 安全威胁的常见方案

鉴于 BGP 在维护互联网稳定运行中发挥的重要作用,业界针对各类 BGP 安全威胁提出了多种解决方案,部分技术已经在生产环境中实际部署并形成规模。

(1) Secure BGP(S-BGP)

S-BGP[9]提出了一种附加签名的 BGP 扩展消息格式,用以验证路由通告中 IP 地址前缀和传播路径上 AS 号之间的绑定关系,从而避免路由劫持。

(2) Secure origin BGP(SoBGP)

SoBGP[10]同样着重于解决路由起源认证问题,与 S-BGP 采用专用 PKI 系统不同的是,SoBGP 采用 Web-of-Trust 模型,可验证路由来源合法性。

(3) Interdomain route validation(IRV)

IRV[11]是一种较为综合的 BGP 安全解决方案。IRV 的关键组成部分是每个自治域中的域间路由验证器,通过域间路由验证器中的历史路由通告记录以及本地路由策略信息等内容,可以用来验证接收路由的有效性。

(4) RPKI

RPKI[12]是一种用于保障互联网基础码号资源(包含 IP 地址、AS 号等)安全的公钥证书体系。通过对 X.509 公钥证书进行扩展,RPKI 依托资源证书实现了对互联网基础码号资源使用授权的认证,并以路由源声明(route origin authorization,ROA)的形式帮助域间路由系统验证某个 AS 针对特定 IP 地址前缀路由通告的合法性,同时也为其他域间路由安全技术(如 BGPsec)的实施提供了可信的数据源。

(5) BGPsec

BGPsec[13]着重于解决 BGP 路由传输过程中的安全问题,其同样使用数字签名技术,实现 BGP 路径验证。若其可以与 RPKI 技术紧密结合并大规模部署实施,可以极大提高域间路由系统的安全水平。

1.4　AS 策略违背的安全威胁

除上文提及的 BGP 安全问题外,一类相对隐蔽但同样重要的安全威胁引起业界关注,即在 BGP 路由传播过程中违背 AS 间策略的安全威胁。BGP 路由在 AS 间的交互过程中,需遵循 AS 建立的商业关系及原则。由于以上商业关系相对 BGP 协议独立存在,导致此类安全风险难以检测,一旦发生则持续时间较长,可引发 AS 出口拥塞或互联网资源长期被恶意占用等风险,严重威胁 AS 的稳定运行,是一种低成本损害组织商业利益的恶意手段。

2　区块链技术简介与研究现状

2.1　区块链协议概述

区块链是一个去中心化的共享数据库。通过分

布在各地的节点,依照统一的共识规则修改并存储数据备份,确保数据安全。

区块链技术的要点包括以下 4 个方面[14]。(1)共享账本。区块链是共享账本的底层技术,意义在于确保交易过程的真实性。(2)智能合约。“一个智能合约是一套以数字形式定义的承诺”,充分利用了区块链的不可篡改、高可靠的特性。(3)隐私。区块链中的隐私保护问题主要指其提供的匿名性特征。但与此同时,业界针对如比特币中交易内容公开透明而导致的隐私问题引起担忧,已逐步开展研究与应用的探索工作。(4)共识。主要可分为工作量证明机制、权益证明机制、股份授权证明机制和 Pool 验证池等 4 类。

2.2 已开展的相关工作

随着区块链技术的逐步发展,基于区块链的研究与应用日渐丰富。根据 Analytics Insight 统计[15],2020 年,区块链技术在区块链即服务、利用区块链解决社交网络问题、区块链技术在政府机构中的应用、区块链技术与人工智能的结合以及区块链技术在物联网中的应用等方面取得进展。

在此背景下,如何将区块链技术与互联网传统技术相结合已成为一个新的方向。以关键基础设施为例,相关研究与应用逐渐丰富,主要集中在几个方面。如 Stefano 等人[16]尝试使用区块链技术解决 IP 地址管理分配等问题,但这种方式难以跟踪未自愿提供联系方式机构的身份。Namecoin[17]利用区块链技术搭建去中心化域名系统 Namecoin,但鉴于其实现的复杂性等原因,截至 2021 年初其实际使用规模仍然有限。Muhammad 等人[18]提出利用区块链技术尝试解决 BGP 劫持攻击威胁,但暂未涉及面向大规模路由条目下的执行效率及可行性。以及 Wang 等人[19]尝试利用区块链解决 PKI 所面临的集中管理问题等。

以上各个方面均针对互联网关键基础设施面临的问题开展研究。除此之外,如何保证各个自治域在路由转发过程中遵守相关规定是另外一个需要研究的方向。但时至今日,由于相关意识的缺失以及隐私保护等方面的顾虑,行业内仍鲜有关注。Zhao[20]针对此问题设计出一种新的算法以及数据结构,是解决 BGP 隐私与安全性平衡问题的一种新的尝试,其主要关注的是在保护隐私的前提下,BGP 最佳路由的选择是否符合约定的问题。文献[21]设计出一种基于区块链的路由基础设施 BGPChain,旨在解决 RPKI 技术为 BGP 带来的集中管理的问题。张元媛等人[22]提出一种基于导出策略的路由配置错误检测方法,但检测过程由 BGP 路由器承担,明显增加了路由器的负荷。

3 RPKI 与区块链结合的安全机制研究

如前文所述,业界已经开展了利用区块链技术应对 BGP 安全问题的相关研究,取得一定进展。但尚未提出自治域在路由转发过程中是否遵守相关规定的检测方法,导致仍然存在自治域出口拥塞或互联网资源长期被恶意占用等安全风险。本研究提出一种利用区块链技术增强 BGP 安全的机制,可有效检测 BGP 传输过程中是否存在策略违背的现象。区块链技术去中心化、不可篡改的特性可以确保自治域间商业关系和原则的公正权威。基于区块链技术建立自治域间策略的权威数据库,可及时、正确地发现违背策略的恶意行为,及时抵御潜在攻击,迅速恢复异常状况,有效增强域间路由系统安全水平。

为了与 RPKI 等技术保持兼容,并达到充分利用既有资源的目的,本机制采用 RPKI 中依赖方(RP)实现策略验证。在实施过程中,该机制可与 BGP 协议结合,支持迭代部署,减小实施难度,便于推广应用。

3.1 AS 类型与路由策略的关系

3.1.1 AS 类型与特征

依照 AS 的连接类型以及运行策略的差异,当前业界将 AS 划分为 3 个主要类别[23]:(1)多宿主自治域(multihomed);(2)末端自治域(stub);(3)过渡自治域(transit)。每个自治域有各自的特点。其中,多宿主自治域意味着与多个 AS 相互连接,可以抵御单 AS 连接失效的风险。虽然多宿主自治域与多个 AS 相互连接,但并不允许连接的 AS 之间通过多宿主 AS 进行数据传输。末端自治域只与一个自治域相连。过渡自治域与多宿主自治域有相同之

处,都与多个自治域相连接,但允许多个自治域之间进行数据传输。

AS 的类型和特征总结如表 1 所示。

表 1　AS 类型及特征

AS 类型	特征
多宿主	与多个 AS 相互连接,但不允许连接的 AS 之间通过多宿主 AS 进行数据传输
末端	只与一个自治域相连
过渡	与多个自治域相连接,但允许多个自治域之间进行数据传输

3.1.2　AS 之间的商业关系分类

Lixin 的研究结果显示,AS 之间的商业关系主要可以分为提供者-客户(provider to customer,P2C)以及对等体-对等体(peering to peering,P2P)两种类型[24]。其中,P2C 表示提供者向客户提供互联网 transit 服务,允许客户通过提供者到达其他网络并根据使用的流量支付相应费用。P2P 表示对等体之间的客户可以相互可达,所采用的对等连接所产生的业务流量由 2 个 AS 共同承担。

AS 之间的商业关系如图 1 所示。

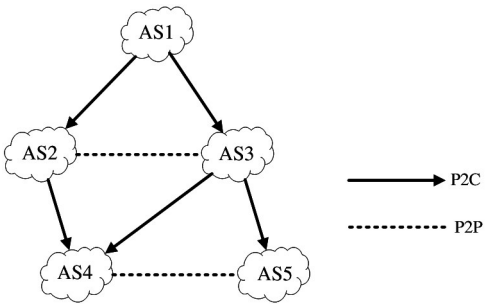

图 1　AS 商业关系示意图

3.1.3　BGP 路由从进到出的交互过程

作为一种域间路由协议,BGP 有相对完善和较为丰富的策略控制选项。一般来说,BGP 路由的策略主要可分为 import 和 export 两类,分别控制入方向路由以及出方向路由,同时在 2 种策略之间实现路由选择和路由表的构建。

BGP 路由处理的主要流程如图 2 所示。

从路由传播方向上分类,BGP 策略可以分为import策略以及export策略两类。为了简化问题,便于

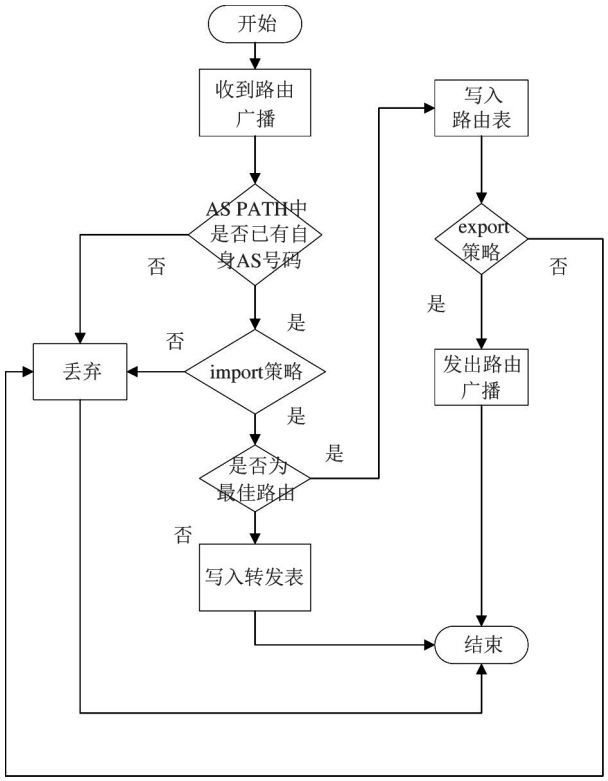

图 2　AS BGP 路由处理流程图

分析研究,以下说明典型 import 和 export 策略的主要流程。

(1)前置于路由导入策略之前的最重要的一条原则是要避免环路,即在收到发来的 BGP 路由时,首先要检查 AS PATH 属性中是否已经存在自己的 AS 号码。若存在,则触发避免环路机制,该路由将被丢弃。

(2)实施 import 策略。典型的 import 策略包括接受或丢弃 BGP 路由,具体的 import 策略与各个 AS 管理机构的配置相关。如典型的丢弃判断准则是接收到由邻居发出的路由,但实际上该邻居并不拥有此段路由。同时 import 策略通常配置 local preference 属性,用来影响路由选择。import 策略应用在形成路由表的步骤之前。

(3)在应用 import 策略后,需进行最佳路由选择过程。经过综合评判,若接收到的路由为最佳路由,则将该段路由写入路由表,同时需写入转发表。

(4)执行 export 策略。根据主流的 BGP 导出策略,基本的原则需要依照以下几点予以执行[24]。

1)导出至提供者。允许的策略:客户可以将本

身的路由以及从其客户学习到的路由导出至提供者;禁止的策略:不应将从其他提供者或者对等体学到的路由导出。

2)导出至对等体。允许的策略:对等体可以将本身的路由以及从其客户学习到的路由导出;禁止的策略:不应将从其提供者或者对等体学到的路由导出。

3)导出至客户。允许的策略:提供者可以将本身的路由以及从其客户学习到的路由导出,且可以将从其他提供者以及对等体学习到的路由导出。

由此可见,BGP 路由策略违背的现象与互联网接入服务提供者、对等体以及互联网接入服务用户直接相关,一旦发生异常将损害三者的利益。

3.2　基于区块链技术的 BGP 路由策略检测机制设计

为了增强 BGP 协议安全,特别是要及时发现在 AS 间路由传播过程中违反策略的现象,以下设计一种利用区块链技术增强 BGP 安全的机制,命名为 BRPM2。

BRPM2 在当前域间路由系统的基础上引入区块链技术,主要使用以太坊并利用验证组件完成针对 BGP 路由策略的验证。BRPM2 的系统架构主要可分为策略链和验证组件两部分,其中策略链用于建立针对各个自治域连接关系以及策略属性的权威记录;验证组件用于和自治域系统中的路由器进行交互,验证是否存在路由策略违背的现象。由于验证组件与策略链相对独立,为了充分利用资源,以及整体考虑增强路由系统安全的各种技术手段,设计利用 RPKI 中的 RP 承载 BRPM2 验证组件的功能。

BRPM2 的系统架构如图 3 所示。

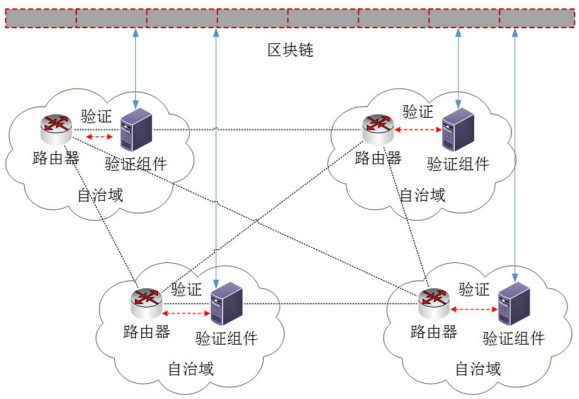

图 3　BRPM2 系统架构图

如图 3 所示,BRPM2 与传统网间路由系统联合实现策略验证功能。每个希望利用 BRPM2 检测违背 BGP 策略现象的自治域将在区块链中录入形成包括与本自治域相连的自治域关系列表、接收到的 BGP 广播地址等相关信息的区块,供验证组件进行检测分析。在接收到路由广播后,路由器与验证组件交互,由验证组件前往策略链获取必要信息后进行逐步验证,最终将验证结果返回路由器。路由器将根据验证结果判断接收或拒绝更新此项路由。

3.2.1　策略链结构

(1)存储设计

在策略链中,主要存储的是针对各个自治域的连接关系以及策略属性的权威记录。策略链的主要设计思路是以简化的形式构成存储系统,使用点对点的设计思想,各节点间建立扁平化连接关系,彼此连接相互完成数据传输。

1) 分布式哈希表

采用分布式哈希表(DHT)协调和维护元数据,基于此实现对所有对等节点的追踪与查找。

2) 身份

为保证存储系统安全,策略链建立身份认证机制,为存储节点命名并分配公私钥对。在首次连接时,对等体交换公钥信息,通过指定字段的标识进行身份认证,确保数据交换安全。

3) 数据交换

在对等节点间通过交换数据块分发数据,利用身份认证机制保证安全,并建立普遍认可的数据交换信用体系。通过奖罚机制,如提升向外发送数据节点信用值,或降低接收数据节点信用值的方式鼓励数据共享,降低策略链存储系统数据损坏的风险。

4) 对象

通过加密哈希(hash)对象的内容实现快速定位,采用有向无环图(DAG)建立索引关系,使内容可寻址,并可有效删除重复数据,节约存储空间。

5) 文件结构

由版本控制、文件系统路径以及路径查找等要点构成。其中版本控制采用的是以存储对象在历史版本中快照的形式加以存储,存储对象改变的历史可回溯。文件系统路径则可使用字符串路径进行遍

历,同时可采用隐藏的方式增强存储数据安全。路径查找则可通过缓存的形式减少遍历次数,提高查询性能。

(2)共识设计

共识算法是策略链设计的关键环节,负责在节点处理完各类交易后,保证节点状态的一致性,即将交易打包到区块中。策略链采用实用拜占庭容错算法(practical Byzantine fault tolerance,PBFT)并在此基础上进行改良。

策略链中的共识算法根据投票形成共识过程中权利的大小设定两类角色,分别为验证人和提议人。其中验证人为策略链中的各个节点,提议人则由验证人轮流产生。

概括来说,策略链中的共识算法主要分为 3 个处理步骤:(1)由提议人提出一个区块;(2)发送提交的意图;(3)在签名后提交一个新区块。每一轮只有一个验证人(即提议人)可以提出块,且需要用提议人对应的私钥进行签名,如此可在发生错误时找到为此负责的验证人,形成被动的监督机制。其他验证人需要对每个提议进行投票,且投票需用自己的私钥签名,如此反复。

每轮的提议人对交易中的区块提议并对提议的区块投票,正常情况下达成共识并形成新的区块,结束本轮流程。特殊情况下由于节点离线或网络延迟等原因可能导致提议人提议区块失败,此时的容错机制一方面需要等待提议人一段时间后方可进入下一轮提议,为节点恢复或网络状况好转预留窗口期;另一方面则可选择另外的验证人提议新的区块并开启新一轮投票过程。

(3)网络设计

策略链的网络设计采用区块链中常见的 P2P 形式,可被划分为非结构化 P2P 网络和结构化 P2P 网络。为了增强性能,提升数据查询效率,策略链采用结构化 P2P 网络模型,实现基于分布式哈希表的查询机制。

结构化 P2P 网络在策略链中的应用可解决分布式环境下快速准确地路由、定位数据的问题,具体可将整个网络区分为资源空间和节点空间两类。其中资源空间是所有节点保存数据的集合,而节点空间则为所有节点的集合。数据和节点需要分别编号并以哈希的形式进行存储,形成对应 ID。资源 ID 和节点 ID 间存在映射关系,可将资源和节点紧密相连,避免泛洪广播,提升查询性能。

3.2.2　关键要素

根据区块链文献[23]中的理论,区块链系统中关键的要素包括基本区块的组成(basic blocks)、创世区块(genesis blocks)、交易(transactions)以及工作流程(workflow)等。根据本文主要需解决的关于 AS 间路由传播过程中违反策略的问题,以下针对 BRPM2 中的关键要素展开说明。

(1)基本区块

BRPM2 中的基本区块主要由以下几部分要素构成。

1)交易记录。一个本区块中所有的交易记录的列表。

2)哈希值。本区块内容的哈希值。

3)随机数。用来产生本区块的工作量。

4)前一个区块的哈希值。用来验证区块的连续性,避免区块序列的不连续。

5)索引。本区块在链中的位置。

6)签名。用矿工私钥针对本区块进行的数字签名。

7)时间戳。本区块产生的时间。

8)挖矿的时间戳。本区块被开采的时间。

9)矿工。开采本区块的主体 ID 值,主要由 AS Number 表示。

(2)创世区块

创世区块是区块链中的第一个区块,用来创立整个区块链。创世区块由具有公信力的组织启动,不需要进行开采。在创世区块中需包含基本区块中的典型要素,包括出块者 ID、哈希值、随机数以及时间戳等要素。同时由于 BRPM2 主要用于检测 BGP 路由策略,因此其创世区块应包含 AS 号、相连的 AS、相连 AS 的类型以及 IP 前缀列表等信息,用于验证 BGP 路由广播过程中是否存在违反策略的现象。

(3)交易

BRPM2 中的交易主要是指 AS 间连接状态的变

化,以及 IP 地址广播状态的变更。交易主要表述了输入和输出间的对应关系。交易主要由各个 AS 发起,由整个链共同确认,用来验证 AS 间 BGP 策略的正确性。

交易记录中主要的要素包括以下几个方面。

1)输入。AS 间连接状态的变化,以及 IP 地址广播的变更。

2)输出。一系列输出的参数和数值,用来描述交易的结果以及交易后 AS 的最新状态。

3)类型。包括 AS 间连接状态的变更,以及 IP 地址广播变更等。

4)签名。

5)时间戳。

6)交易的 ID 值。用来唯一标识本次交易。

(4)工作流程

BRPM2 的工作流程主要涉及影响 BGP 策略变更的相关流程。影响 BGP 策略变更的流程主要可归纳为以下两大类。

1)AS 状态变更:包括连接 AS 的增减以及连接 AS 商业关系的变更等情形。其中,连接 AS 的增减是指本 AS 与新的 AS 建立邻接关系或者与部分 AS 终止连接关系等情形;连接 AS 商业关系的变更是指本 AS 与某些 AS 的商业关系的变更,如由原有的 P2C 变更至 P2P 等。

2)IP 地址广播变更:包括 IP 地址起源变更以及 IP 地址广播增加或减少等情形。其中,IP 地址起源的变更是指 IP 地址所属 AS 变更导致其 BGP 广播的起源 AS 的调整;IP 地址广播的增加或减少是指由于策略的调整导致 AS 广播的 IP 地址前缀的增加或者删除。

3.3 机制原理

BRPM2 利用区块链技术建立 AS 间的策略检测机制。其主要利用了区块链的不可篡改特性,将参与到策略检测的 AS 相关元素记录到区块链上,并利用验证组件检测 AS 所发布的路由信息是否存在违背策略的现象。

以文献[25]所提到的错误路由检测方法为原型,以下提出基于 BRPM2 的检测算法。基本假设条件包括以下 3 点。

(1)待检测的 AS 共收到发来的 m 个地址广播前缀 $prefix_i, i = 1 \sim m$;

(2)每一个地址广播前缀 $prefix_i$ 来自 n 个自治域 $AS_j, j = 1 \sim n$;

(3)待检测的 AS 与 k 个 AS 相连。

则检测算法主要的代码逻辑如图 4 所示。

```
isPolicyViolation(prefix_i, AS_j)
 for i=1...m, j=1...n
  do if isLegitimateLink(prefix_i, AS_j)
    then return True
  if isLegitimateAnnouncement(prefix_i, AS_j)
    then return True
  return false

isLegitimateLink(prefix_i, AS_j)
 do if AS_j ∈ [AS_1, AS_2, ..., AS_k]
    then return True
    else return False
```

```
isLegitimateAnnouncement(prefix_i, AS_j)
 case AS_j is Provider
  if prefix_i is originate_from_AS_j
    then return True
 if prefix_i is received_from_Customer
  then return True
 elseif return False
  case AS_j is Peer
   if prefix_i is originate_from_AS_j
    then return True
 if prefix_i is received_from_Customer
  then return True
 elseif return False
  case AS_j is Customer
   if prefix_i is originate_from_AS_j
    then return True
 if prefix_i is received_from_Customer
  then return True
 elseif return False
```

图 4 基于 BRPM2 的检测算法示意图

以上代码主要由 isPolicyViolation 主进程以及 isLegitimateLink 和 isLegitimateAnnouncement 2 个分进程构成。其中 isLegitimateLink 用来验证接收到的 BGP 地址广播是否与本自治域存在合法连接,isLegitimateAnnouncement 用来验证接收到的 BGP 地址广播是否存在违背策略的现象。

如图 5 所示,在运用 BRPM2 机制后,BGP 路由处理的主要流程产生相应变更。

3.4 技术特点

3.4.1 支持渐进式部署

如上文记录中所述,BRPM2 依赖于区块链技术和验证组件,与当前自治域系统的连接形式相对独立,可支持渐进式部署形式。即在当前网间路由系统运作的基础上同步部署 BRPM2 系统,当具备 BRPM2 相关功能时则启用,未具备 BRPM2 功能则不启动验证功能。

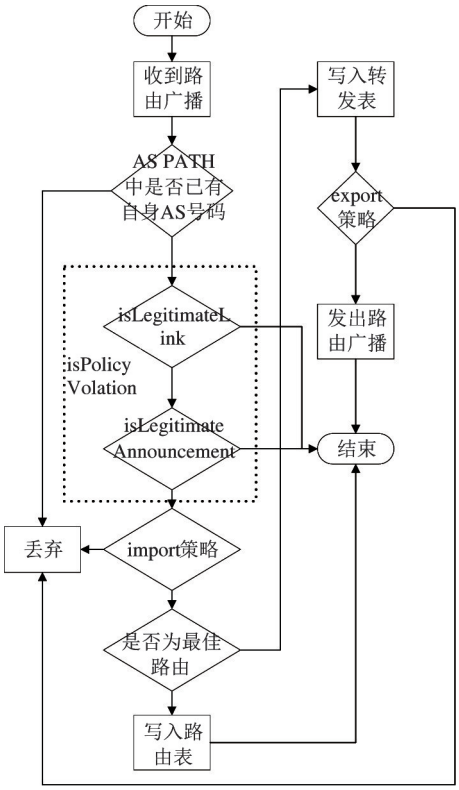

图 5　改进后的 BGP 路由处理流程图

为了加快 BRPM2 的部署应用,BRPM2 可提供完全验证以及部分验证 2 种级别的检测方案。在采用完全验证手段时,验证模块可沿 AS PATH 路径进行逐级验证,直至 BGP IP 地址段始发 AS,实现针对此段 IP 的完整策略验证功能。针对部分验证检测手段,验证模块可检测与待测 IP 地址段所在 AS 直接或次直接相连的 AS 之间的关系,检查发出测试 IP 地址段所在 AS 是否存在策略违背现象。由于 BRPM2 至多需要检测两级 AS 的策略设置等相关信息,因此可局部小规模部署实现。

3.4.2　安全性分析

BRPM2 使用区块链技术,针对 AS 间策略违背的问题加以验证,有利于提升 BGP 传输过程中的安全水平。但区块链技术的应用同时也引入了新的安全问题,比如双花问题,随着 BRPM2 策略链网络规模的逐步扩大以及 RPKI 等技术的同步发展,发起此类攻击的难度将成倍提升,可有效解决 51% 攻击问题。或者如女巫攻击问题,可以在 BRPM2 建链初期设定 N 个可信节点,N 个信任节点可以对其他节点进行担保,担保其他节点同样可以信任,以此类推,则可利用此类非直接认证的方式对抗女巫攻击等等。总之,由区块链技术引入的新的安全问题,其应对手段将随着区块链技术的发展而逐步强化,BRPM2 也将根据应对手段的转变而逐步升级完善。

3.4.3　功能及效能特征

BRPM2 采用 PBFT,其属于拜占庭类共识算法。若分布式系统中节点发生了任意类型的错误,只要系统中错误节点数量少于一定比例,拜占庭类共识算法都能保证系统的可靠性。PBFT 降低了拜占庭协议的运行复杂度,具有高一致性、高可用性、抗欺诈能力强等特点。

可以看出,BRPM2 的执行效率与共识算法具有直接关联,PBFT 的特性决定了 BRPM2 达成共识的速度。

基于 PBFT 的效能特性,BRPM2 具有较高的运行效率。根据文献[26]中记载,以算法出块速度和每秒系统可处理的交易数量(transaction per second, TPS)为主要指标,PBFT 的出块速度可达到秒级,远高于工作量证明(pow of work, PoW)的处理速度。但其缺点是当系统中节点数量大幅增加时的整体性能呈现明显降低的趋势,在全网路由器广泛使用的条件下的性能问题将成为需要考量的重点。在实际应用过程中,BRPM2 可根据路由系统以及区块链技术的发展调整所采用的共识算法,进一步优化算法性能,提升方案效率。

3.4.4　与 RPKI、BGPsec 的对比

BRPM2 主要应对的是违背 AS 间策略的问题,在验证过程中至多追溯至与发起检测的 AS 进行二级连接的 AS,涉及环节较少。BRPM2 无需更改 BGP 协议,主要借助于区块链技术以及验证环节进行检测。同时,与 RPKI 类似的是,BRPM2 支持增量部署形式,有助于迅速推广其应用部署。

RPKI 主要应对的是路由起源认证的问题,在验证过程中需追溯至路由分配机构,涉及环节数量居中。RPKI 无需更改 BGP 协议,借助 PKI 体系以及 RP 等环节进行验证。RPKI 支持增量部署形式。

BGPsec 主要应对的是路由传播过程中的问题,在验证过程中需逐跳验证路由传播的正确性,涉及环节较多。BGPsec 需更改 BGP 协议,将 BGP AS _ PATH

属性替换为 BGPsec _ Path 属性。BGPsec 需要 BGP 传播过程中全路径支持 BGPsec 协议,其应用率与部署率直接相关。

BRPM2 与其他增强域间安全协议的区别如表 2所示。

表 2　BRPM2 与其他协议的对比

协议名称	BRPM2	RPKI	BGPsec
应对问题	AS 间策略违背验证问题	路由起源认证	BGP 传播过程中的篡改问题
涉及环节	直接与次直接相连 AS	至信任锚的所有 AS	BGP 传播过程中所有 AS
协议修改	无	无	AS _ PATH 属性替换为 BGPsec _ Path
增量部署	是	是	否

3.5　原型系统设计

基于 BRPM2 技术原理,建立 BRPM2 原型系统。BRPM2 原型系统主要由策略链以及验证组件两部分组成,其中策略链用于记录关于自治域以及 BGP 广播地址等信息,供验证组件进行检测分析,验证组件通过查询记录上述信息后,对 BGP 路由器发起的验证请求进行检测,最终给出验证结果。基于以上原理,设计 BRPM2 原型系统架构如图 6 所示。

如图 6 所示,策略链主要设计为 3 层机构。(1)网络层用于构成策略链的底层,用于实现区块链节点地址的广播与发现、用于寻址的路由协议集合以及与验证组件之间的接口等。(2)数据库层基于区块链网络记录与自治域相连的自治域关系列表、接收到的 BGP 广播地址等相关信息,供验证组件进行检测分析。(3)应用层则用于建立交互界面,实现权限管理、数据管理以及状态统计等功能。

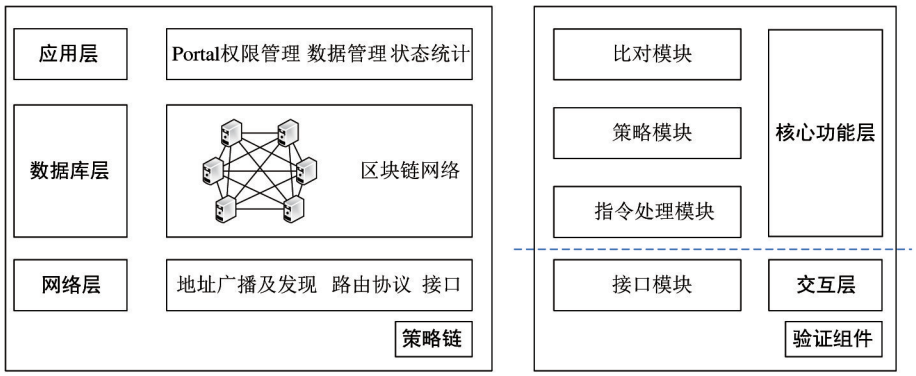

图 6　BRPM2 原型系统架构图

验证组件则主要分为交互层和核心功能层两部分。交互层主要由接口模块构成,分别用于与路由器以及策略链之间进行数据传输,接收路由器发来的验证请求,并向策略链发起验证所需信息的请求。核心功能层主要由三部分组成,指令处理模块主要负责处理由接口模块发来的各项验证请求;比对模块根据接收的必要信息完成 BGP 广播合理性判断,得出参考意见;策略模块则负责根据预设策略结合比对模块的参考意见,形成验证结果。

3.6　仿真实验

3.6.1　有效性验证

(1)仿真环境

以下以仿真实验的形式验证 BRPM2 的有效性。为充分模拟 BRPM2 的应用环境,以 AS 为基本单位,设定模拟设备主要包括以下 3 种。

1)设定 BGP 路由器,负责管理 AS 内路由信息。

2)设定验证组件 RP,负责检测是否存在策略违背现象。

3)设定区块链节点,负责建立含有邻接 AS 商业关系等信息的基本区块。

(2)仿真场景

为开展充分评估,设定 3 种策略违背场景,包

括:

1)违背“导出至提供者”原则;

2)违背“导出至对等体”原则;

3)违背“导出至客户”原则。

(3)AS 商业关系设定

为模拟 BRPM2 典型工作场景,以图 1 为例设定模拟环境:假设 AS1 为大型 ISP,其为 AS2、AS3 提供互联网接入服务,即 AS1 与 AS2 形成 P2C 关系,AS1 与 AS3 形成 P2C 关系。AS2 与 AS3 为 P2P 关系。AS2、AS3 为 AS4 提供互联网接入服务,即 AS2 与 AS4 形成 P2C 关系、AS3 与 AS4 形成 P2C 关系。AS3 同时为 AS5 提供互联网接入服务,即 AS3 与 AS5 形成 P2C 关系。AS4 与 AS5 为 P2P 关系。

根据以上商业关系,设定各个自治系统涉及的路由广播信息如表 3 所示。

表 3　AS 路由广播信息表

自治域	路由前缀	路由类型
AS1	1.1.1.0/24	起源
AS2	2.2.2.0/24	起源
AS3	3.3.3.0/24	起源
AS4	4.4.4.0/24	起源
AS5	5.5.5.0/24	起源

(4)仿真过程

根据以上假设搭建测试环境。针对 BRPM2 策略链的设定,需要在每个 AS 中建立基本区块,记录每个 AS 的连接关系及 IP 地址广播等信息。以 AS4 为例,假设其 AS 号码为 10004,其基本区块应包含的核心信息如图 7 所示。与 AS4 相连的自治域可以通过验证组件检验在 BGP 广播过程中是否存在违背策略的现象。

```
AS_Number:
        10004
Relationship:
        P2C:
                AS2 → AS4
                AS3 → AS4
        P2P:
                AS4 → AS5
.....
```

图 7　自治域典型区块信息

各 AS 内 BGP 路由器依照表 3 进行路由广播,经路由收敛后路由转发表如表 4 所示。

表 4　各自治域路由转发表

AS 类型	特征
AS1	1.1.1.0/24 AS1 2.2.2.0/24 AS2 3.3.3.0/24 AS3 4.4.4.0/24 AS2 AS4 5.5.5.0/24 AS3 AS5
AS2	3.3.3.0/24 AS3 4.4.4.0/24 AS4 5.5.5.0/24 AS3 AS5 1.1.1.0/24 AS1 2.2.2.0/24 AS2
AS3	3.3.3.0/24 AS3 4.4.4.0/24 AS4 5.5.5.0/24 AS5 1.1.1.0/24 AS2 AS1 2.2.2.0/24 AS2
AS4	3.3.3.0/24 AS3 4.4.4.0/24 AS4 5.5.5.0/24 AS5 1.1.1.0/24 AS2 AS1 2.2.2.0/24 AS3 AS2
AS5	3.3.3.0/24 AS3 4.4.4.0/24 AS4 5.5.5.0/24 AS5

表 4 的路由转发表代表了测试环境中各台路由器在充分交换路由信息后形成的路由转发表。后续数据传输将依照路由转发表进行路径选择,完成信息交互。

基于以上环境,分别模拟发生 3 种策略违背场景,检验 BRPM2 算法的有效性。以违背“导出至对等体”原则场景为例,模拟 AS4 发生违背协议的现象,即将关于 2.2.2.0/24 的路由经 BGP 广播传递至 AS5。AS5 中验证组件在收到路由信息后执行 BRPM2 算法,主要步骤如下。

步骤 1　明确验证对象以及相关参数,进入 isPolicyVolation 主进程。

步骤 2　进入 isLegitimateLink 子进程。检查 AS4 与 AS5、AS2 与 AS4 是否分别建立 BGP 连接。

步骤 3　进入 isLegitimateAnnouncement,检查从

AS4 收到的关于 2.2.2.0/24 的路由是否存在违背策略的现象。

1)根据区块链信息中记载,AS4 与 AS5 之间为 P2P 关系、AS2 与 AS4 之间与 P2C 关系。

2)由于三者间的关系属性,根据导出策略原则,对于 AS4(作为 Customer)不应将从 AS2(作为 Provider)学习到的路由转发至 AS5(作为 Peer),与实际路由传播情况相违背。

3)根据区块链不可篡改的特性,验证模块有理由相信本次学习到的路由信息存在异常,将根据客户预先设置好的处置策略(忽略、警告、阻断)告知 BGP 路由器执行相应操作。

实际仿真过程依照上述步骤执行。首先模拟出 AS1 ~ AS5 5 个自治域,各个自治域内包括 BGP 路由器、区块链节点以及验证组件等元素。在仿真实验前期,各自治域内 BGP 路由器形成邻接关系,完成 BGP 路由收敛。此后,通过控制 AS4 内 BGP 路由器,模拟 AS4 发生违背协议的现象,将关于2.2.2.0/24 的路由经 BGP 广播传递至 AS5。AS5 中 BGP 路由器验证组件在收到路由信息后,依照设定策略执行 BRPM2 算法,检测出异常现象,并将检测结果返回 BGP 路由器,避免了 AS4 违规现象的进一步传播,达到了提升路由安全的目的。经仿真环境验证,AS5 中验证组件在收到验证请求后于24.41 ms检测出异常,实际证明了 BRPM2 算法的有效性。

3.6.2 性能分析

BRPM2 基于区块链技术,其运行效能主要由形成区块的时间以及验证的时间共同决定。影响形成区块的时间主要由共识算法,即 PBFT 算法的效能决定;验证的时间则主要由数据传输时间以及 RP 运算效率等因素决定。以下展开具体分析。

(1)形成区块效能评价

形成区块的关键是要完成共识。根据 PBFT 高一致性、高可用性、抗欺诈能力强等特点,BRPM2 算法选用 PBFT 为共识算法。PBFT 共识算法的效率主要由区块链节点数量影响。考虑到 BRPM2 的策略链面向对象为 AS 间的策略,在生产环境中 AS 间策略的变更频率远低于 BGP 路由宣告的变更频率,因此达成共识的时间是影响 BRPM2 效能的非主要因素。

以 Sukhwaih 等人[27]提出的关于 PBFT 共识性能评估手段为例,通过建立最多 100 个节点以及多种 AS 间策略形成 BRPM2 策略链,检验其共识效能。通过仿真可知,经 100 次模拟实验,以上条件下 BRPM2 形成共识的时间均值为 5.034 ms。BRPM2 形成共识的时间与节点数量相关,节点数量越少则效能越好。基于以上情况,选取 10 个节点、50 个节点、100 个节点 3 种情况进行对比测试,其形成共识的时间均值分别为 4.38 ms、5.86 ms 以及 7.04 ms,印证了节点数量多少影响共识时间长短的关系。从以上测试结果可以看出,BRPM2 形成共识的时间为毫秒级别,在当前真实网络环境下应用不会影响路由系统的运行效率。

(2)策略验证效能评价

BRPM2 的策略验证效能主要由数据传输时间以及 RP 运算效率等因素决定。由于验证功能完全由 RP 决定,BGP 路由器仅需要从 RP 获得验证结果,因此 BRPM2 不会额外增加 BGP 路由器负载。为完成策略验证,RP 需主要执行以下步骤:(1)收到 BGP 路由器发来的待验证 BGP 路由信息;(2)获取策略链中验证所需的策略信息;(3)根据规则完成本地策略验证;(4)将验证结果返回 BGP 路由器。其中影响步骤(1)、(2)、(4)的主要因素为网络传输效率,影响步骤(3)的主要因素为 RP 计算性能。

为评估策略验证效能,建立仿真实验环境。仿真环境主要以 4 台 x86 主机构成,以虚拟机的形式构成实验环境,形成主要环节包括 BRPM2 策略链、BGP 路由器以验证器(RP)。

在 BRPM2 策略链达成共识后,模拟 BGP 路由器接收到 BGP 路由更新,则通知 RP 完成策略验证。在此场景下记录 RP 完成各个步骤所消耗的时间。为了充分评估策略验证效能,设置(1)违背“导出至提供者”原则;(2)违背“导出至对等体”原则;(3)违背“导出至客户”原则三类场景进行对比验证。经 3 轮实验验证,三类场景下 RP 执行步骤(1)、(4)的网络传输时延均在 3.54 ms 左右,步骤(2)的网络传输时延均在 6.78 ms 左右,相对存在较大差异的环节在步骤(3)。在场景(1)中,步骤(3)的策略验

证时延均值为 21.23 ms,在场景(2)中,步骤(3)的策略验证时延均值为 24.34 ms,在场景(3)中,步骤(3)的策略验证时延均值为 23.21ms。策略验证实验结果如表 5 所示。

表 5　策略验证实验结果统计表

	场景 1	场景 2	场景 3
步骤 1	3.54 ms	3.42 ms	3.66 ms
步骤 2	6.78 ms	6.59 ms	6.97 ms
步骤 3	24.34 ms	23.32 ms	25.36 ms
步骤 4	3.54 ms	3.64 ms	3.44 ms

可以看出,策略验证步骤为本环节效能的主要影响因素,与 RP 计算性能紧密相关。若出现性能瓶颈,可以通过提升 RP 单机计算能力或形成 RP 处理集群等手段进行优化。其余对效能造成影响的因素主要由网络时延决定,若出现瓶颈,可以通过优化 BGP 路由器与 RP 之间的网络或利用内容分发网络等手段加速数据传输速度等手段进行优化。

从以上仿真实验可以看出,BRPM2 可有效发现三类策略违背现象,随之增加的系统负载较低,执行效率可适用于生产环境,其应用可大幅减少由于恶意 AS 不遵守策略而造成的互联网资源长期被恶意占用等风险,对于提升 BGP 安全水平具有积极意义。

除 BRPM2 以外,业界常基于互联网路由注册表(Internet routing registry,IRR)判断路由策略违背现象。根据 Andree[28]研究结果显示,使用 IRR 判断路由策略违背现象的准确率约为 46%,可见使用 IRR 判断路由策略违背的现象的准确率不尽人意。BRPM2 是针对此问题提出的新的解决方案,路由策略违背检测的准确率取决于策略链建立及维护期间数据的准确率。鉴于区块链技术特性有效增强了不同自治域间路由策略记录的权威性,可以推测,BRPM2 在实际应用后的有效性及实用性会优于传统手段。

5　结　论

本研究结合区块链技术特征,利用以太坊技术针对路由协议中存在的自治系统间策略违背的现象提出一种新的检测算法。

BRPM2 的主要改进点包括:

(1)利用区块链技术建立包含自治域路由策略等信息的策略链,确保自治域间路由策略无法被轻易篡改,采用 PBFT 完成共识,具有高可用性及抗欺诈能力强等技术特性。

(2)基于 RPKI 依赖方(RP)功能实现验证功能,与 BGP 路由器通信完成策略验证,实现功能解耦。

(3)与 RPKI、BGPsec 等技术所解决的问题相辅相成,无需修改 BGP 协议,验证方法简单,便于增量部署。

从以上技术特征可以看出,BRPM2 具备较广阔的应用前景,但仍存在一些需要加以解决的问题。一方面在节点数量大幅增加时机制处理性能呈现明显降低趋势,需在全网路由器广泛应用前重点考虑应对方案;另一方面尚未开展在生产网络环境下的应用状况评估,未掌握 BRPM2 大规模推广应用后对互联网运行产生的实际压力。后续的研究工作可以从以上方面着手改进。

参考文献

[1] The Internet Engineering Task Force (IETF). A border gateway protocol 4 (BGP-4)[EB/OL]. https://tools.ietf.org/html/rfc4271:IETF,[2021-04-01]

[2] 黎松, 诸葛建伟, 李星. BGP 安全研究[J]. 软件学报, 2013, 24(1):121-138

[3] 曾诗钦, 霍如, 黄韬等. 区块链技术研究综述:原理、进展与应用[J]. 通信学报, 2020, 41(1): 134-151

[4] XING Q Q, WANG B S, WANG X F. BGPcoin: blockchain-based internet number resource authority and BGP security solution[J]. *Symmetry*, 2018,10(9):408

[5] 王娜, 杜学绘, 王文娟. 边界网关协议安全研究综述[J]. 计算机学报, 2017, 40(7): 1626-1648

[6] Catchpoint Systems, Inc. One year of BGP (In)security [EB/OL]. https://blog.catchpoint.com/2020/04/09/one-year-bgp-security/:Catchpoint,[2020-11-04]

[7] OLIVIER M. Border gateway protocol hijacking-examples and solutions [EB/OL]. https://www.anapaya.net/blog/border-gateway-protocol-hijacking-examples-and-solutions:Anapaya,[2020-11-10]

[8] Internet Society. Securing BGP[EB/OL]. https://www.internetsociety.org/deploy360/securing-bgp/:Internetsociety,[2020-11-12]

[9] KENT S, LYNN C, SEO K. Secure border gateway protocol (S-BGP)[J]. *IEEE Journal on Selected Areas in*

Communication, 2000,18(4):582-592
[10] WHITE R. Architecture and deployment considerations for secure origin BGP (soBGP)[EB/OL]. https://tools. ietf. org/html/draft-white-sobgp-architecture-02: IETF,[2021-04-01]
[11] GEOFFREY G, WILLIAM A, TIMOTHY G. et al. Working around BGP: an incremental approch to improving security and accuracy of interdomain routing[C]// NDSS, San Diego, USA, 2003:156-158
[12] 冷峰, 赵琦, 延志伟,等. 资源公钥基础设施数据同步的改进方法研究[J]. 网络与信息安全学报, 2021, 7(3): 123-133
[13] MATTHEW L, KOTIKALAPUDI S. BGPsec Protocol specification[EB/OL]. https://tools. ietf. org/html/rfc8205:IETF,[2021-04-02]
[14] 韩璇, 袁勇, 王飞跃. 区块链安全问题:研究现状与展望[J]. 自动化学报, 2019, 45(1): 206-225
[15] PUJA D. Five trends that are dominating blockchain technology in 2020[EB/OL]. https://www. analyticsinsight. net/five-trends-that-are-dominating-blockchain-technology-in-2020/:Analytics Insight,(2021-01-04),[2021-04-01]
[16] STEFANO A, ALBERTO G, BINGYANG L, et al. An experiment in distributed Internet address management using blockchains[J]. *IEEE Transactions on Engineering Management*, 2020, 67: 1459-1475
[17] Namecoin[EB/OL]. https://www. namecoin. org/: Namecoin, (2021-03-11),[2021-04-02]
[18] MUHAMMAD S, AFSAH A, ASHAR A, et al. Route chain: towards blockchain-based secure and efficient BGP routing[C]// IEEE International Conference on Blockchain and Cryptocurrency, Seoul, Korea, 2019: 210-218
[19] WANG Z, LIN J Q, CAI Q W, et al. Blockchain-based certificate transparency and revocation transparency[J]. *Financial Cryptography and Data Security*, 2018, 19: 681-697
[20] ZHAO M C, ZHOU W C, ALEXANDER J, et al. Private and verifiable interdomain routing decisions[J]. *IEEE/ACM Transactions on Networking*,2016,42(4):1011-1024
[21] YAN Z W, LEE J H. BGPChain: constructing a secure, smart, and agile routing infrastructure based on blockchain[J]. *ICT Express*, 2021, 7(3):376-379
[22] 张元媛, 张大方, 曾彬, 等. 基于导出策略的路由配置错误检测方法[J]. 计算技术与自动化, 2008, 1: 107-110
[23] Ilias S, Vasileios K. Validating IP prefixes and AS-Paths with blockchains[EB/OL]. https://arxiv. org/abs/1906. 03172v1:arXiv,(2019-06-07),[2021-04-03]
[24] GAO L X. On inferring autonomous system relationships in the Internet[J]. *ACM/IEEE Transactions on Networking*, 2001,9:733-745
[25] JIAN Q, GAO L, RANJAN S, et al. Detecting bogus BGP route information: going beyond prefix hijacking[C]//2007 3rd International Conference on Security and Privacy in Communications Networks and the Workshops, Nice, France, 2007: 381-390
[26] 陆歌皓, 谢莉红, 李析禹. 区块链共识算法对比研究[J]. 计算机科学, 2020, 47(S1):332-339
[27] SUKHWANI H, MARTINEZ J M, CHANG X, et al. Performance modeling of PBFT consensus process for permissioned blockchain network (Hyperledger Fabric)[C]. //2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), Hong Kong, China, 2017: 253-255
[28] ANDREE T. How accurate are the Internet Route Registries (IRR)[EB/OL]. https://bgpmon. net/how-accurate-are-the-internet-route-registries-irr/: Cisco, (2009-03-28),[2021-05-16]

BGP routing policy monitoring mechanism based on block chain technology

LENG Feng[*,**,***], ZHAO Qi[**], YAN Zhiwei[**], ZENG Yu[*,**]
([*] Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190)
([**] China Internet Network Information Center, Beijing 100190)
([***] University of Chinese Academy of Sciences, Beijing 100049)

Abstract

Aiming at the phenomenon of policy violations between autonomous system in the process of routing propagation, the border gateway protocol (BGP) routing policy monitoring mechanism (BRPM2) is proposed, and a system architecture including a policy chain and a verification module is carried out. Through theoretical analysis, prototype system design and simulation verification, it is shown that the monitoring mechanism could make full use of resource public key infrastructure (RPKI) resources, the RP takes the responsibility of verification function and communicated with the routers, which could realize the function decoupling and facilitate the deployment of applications. BRPM2 is simple and can be deployed incrementally, thus it can improve the security of the inter-domain routing system without modifying the BGP protocol.

Key words: resource public key infrastructure (RPKI), BGPsec, routing decision, blockchain, border gateway protocol (BGP) routing policy monitoring mechanism (BRPM2)