软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2023,34(9):4336−4350 [doi: 10.13328/j.cnki.jos.006660]

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

基于区块链的域间路由策略符合性验证方法*

陈 迪[1,2,3], 邱 菡[1,2], 朱俊虎[1,2], 王清贤[1,2], 樊松委[4]

[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](电子信息系统复杂电磁环境效应国家重点实验室, 河南 洛阳 471003)

[4](郑州大学 软件学院, 河南 郑州 450003)

通信作者: 邱菡, E-mail: qiuhan410@aliyun.com

摘 要: 域间路由系统自治域 (ASes) 间具有不同的商业关系和路由策略. 违反自治域间出站策略协定的路由传播可能引发路由泄露, 进而导致网络中断、流量窃听、链路过载等严重后果. 路由策略符合性验证对于保证域间路由系统安全性和稳定性至关重要. 但自治域对本地路由策略自主配置与隐私保护的双重需求增加了验证路由策略符合性的难度, 使其一直是域间路由安全领域尚未妥善解决的难点问题. 提出一种基于区块链的域间路由策略符合性验证方法. 该方法以区块链和密码学技术作为信任背书, 使自治域能够以安全和隐私的方式发布、交互、验证和执行路由策略期望, 通过生成对应路由更新的路由证明, 保证路由传播过程的真实性, 从而以多方协同的方式完成路由策略符合性验证. 通过实现原型系统并基于真实路由数据开展实验与分析, 结果表明该方法可以在不泄露自治域商业关系和本地路由策略的前提下针对路由传播出站策略符合性进行可追溯的验证, 以合理的开销有效抑制策略违规路由传播, 在局部部署情况下也具有显著的策略违规路由抑制能力.

关键词: 域间路由安全; 区块链; 路由策略符合性; 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, 樊松委. 基于区块链的域间路由策略符合性验证方法. 软件学报, 2023, 34(9): 4336–4350. http://www.jos.org.cn/1000-9825/6660.htm

英文引用格式: Chen D, Qiu H, Zhu JH, Wang QX, Fan SW. Blockchain-based Validation Method for Inter-domain Routing Policy Compliance. Ruan Jian Xue Bao/Journal of Software, 2023, 34(9): 4336–4350 (in Chinese). http://www.jos.org.cn/1000-9825/6660.htm

Blockchain-based Validation Method for Inter-domain Routing Policy Compliance

CHEN Di[1,2,3], QIU Han[1,2], ZHU Jun-Hu[1,2], WANG Qing-Xian[1,2], FAN Song-Wei[4]

[1](Information Engineering University, Zhengzhou 450002, China)

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

[3](State Key Laboratory of Complex Electromagnetic Environment Effects on Electronics and Information System, Luoyang 471003, China)

[4](School of Software, Zhengzhou University, Zhengzhou 450003, China)

Abstract: Various business relationships and routing policies exist among the autonomous systems (ASes) in an inter-domain routing system. Routing propagation violating the export policy agreements among the ASes is likely to cause route leaks, ultimately leading to serious consequences such as network interruption, traffic eavesdropping, and link overload. Verifying routing policy compliance is thus essential for ensuring the security and stability of the inter-domain routing system. However, the dual requirements of ASes for the autonomous configuration and privacy protection of local routing policies increase the difficulty in verifying routing policy compliance and consequently pose a hard problem that remains to be settled properly in the field of inter-domain routing security. This study proposes a

* 基金项目: 国家自然科学基金 (61502528, 61902447)
收稿时间: 2020-11-17; 修改时间: 2021-06-03, 2021-12-27; 采用时间: 2022-02-16; jos 在线出版时间: 2023-02-08
CNKI 网络首发时间: 2023-02-09

blockchain-based verification method for inter-domain routing policy compliance. With blockchain and the cryptographic technology as trust endorsements, this method enables ASes to publish, interact, verify, and execute routing policy expectations in a safe and private manner. The authenticity of the routing propagation process is ensured by generating route attestations corresponding to routing updates. Thus, the verification of routing policy compliance is completed by multi-domain cooperation. A prototype system is implemented, and experiments and analyses are carried out on real routing data. The results show that the proposed method offers traceable verification of export policy compliance of routing propagation without leaking the business relationships and local routing policies among ASes, suppresses policy-violating routing propagation effectively with reasonable overhead, and maintains a remarkable ability to suppress policy-violating routing even in partial deployment scenarios.

Key words: inter-domain routing security; blockchain; routing policy compliance; route attestation

作为互联网基础设施, 域间路由系统的安全性与稳定性对互联网运行至关重要. 边界网关协议 (border gateway protocol, BGP)[1]是现行域间路由系统的事实标准协议, 负责在自治域 (autonomous system, AS) 之间传递路由可达性信息, 实现域间网络的互联互通. 由于 BGP 缺乏路由真实性验证机制[2], 前缀劫持、路由泄露等域间路由安全事件频发, 严重影响互联网的稳定运行. 近 20 年来, BGP 安全一直是研究机构、运营商与设备厂商持续关注的研究热点问题, 涌现了 S-BGP[3]、So-BGP[4]、IRV[5]等许多经典 BGP 安全解决方案. 在此基础上, IETF 安全域间路由工作组提出资源公钥基础设施 (resource public key infrastructure, RPKI)[6]与 BGPsec[7], 并逐步开展实际部署. 然而, 大部分 BGP 安全方案主要关注基于网络资源与拓扑实体认证的路由源与路径传播的认证, 忽略了影响域间路由安全性与稳定性的重要因素: BGP 路由策略符合性问题.

BGP 支持各自治域自定义用于域间选路的本地路由策略. BGP 协议对路由策略的丰富支持是其得以成为互联网核心路由协议的关键[8]. 这些定制的路由策略可用于实现自治域在经济、性能、安全及流量工程等多方面的目标. 由于各自治域分别受独立管理机构控制, 本地路由策略的细节信息通常对外保密. 然而, 路由策略对域间路由系统中诸多重要问题的影响却是不容忽视的, 例如: 网络可靠性、路由收敛性、激励兼容性及地缘政治控制等. Gao 等人充分考虑大多数自治域在经济、性能等方面的需求, 提出了 Gao-Rexford 模型 (GR 模型)[9]等若干经典域间路由策略模型[10−12], 建议自治域遵守. 但实际中自治域并未完全按照这些模型配置本地路由策略[8]. 因配置失误或恶意攻击引发的路由策略违规行为会导致路由泄露事件的发生, 造成由流量重定向引起的网络不可达、流量窃听、链路过载等严重后果. 2017 年 Google 路由泄露事件[13]、2019 年的 Cloudfare 路由泄露事件[14]等多个大规模安全事件均是由于个别自治域在进行 BGP 路由时违反相关路由策略导致的. 研究表明, 即使在 RPKI, ROA 和 BGPsec 全部署情况下, 路由泄露仍可能发生[15]. 解决自治域路由策略符合性问题对于保证域间路由系统安全稳定运行具有重要意义, 却存在很大的困难与挑战, 其难点在于两方面的矛盾: (1) 路由策略符合性验证与本地策略隐私性需求之间的矛盾; (2) 路由策略一致性与自治性之间的矛盾. 因此, 域间路由策略符合性问题是域间路由安全尚未妥善解决的重要问题.

实际域间路由运维中, 网络管理员通常使用互联网路由注册 (Internet route registries, IRR) 数据库 (http://www.irr.net/) 进行策略符合性验证和路由故障排错等操作. IRR 是一个在线结构化数据库, 各自治域的网络管理员自愿地将本地路由策略信息以规格化语言 (routing policy specification language, RPSL)[16]共享至 IRR. 然而 IRR 并未提供身份匿名性与路由策略隐私性, 网络管理员在共享信息时出于隐私考虑会有所保留, 难以保证策略符合检验的准确性. 此外 IRR 还可能被恶意攻击者滥用, 篡改数据库中的策略信息. 另外, 在 BGP 路由过程中, 自治域可使用 BGP Community[17]来标识和传达本地策略需求. Community 属性是 BGP 协议中的一种可选传递属性, 可附加于 BGP 更新报文, 传达本地路由策略期望的语义信息, 例如通往某目的前缀的路由不能宣告给指定链路等. 但 BGP Community 并没有标准化定义, Community 的语义对于不同 AS 群组通常是独立的, 需在 AS 群组中使用电子邮件、机构网站等带外机制达成一致. 并且 Community 属性使用明文附加在 BGP 更新报文中, 在传递中可被伪造、修改或移除, 这使得 BGP Community 属性成为域间路由中常见的误配置原因和潜在的安全威胁.

针对域间路由策略符合性的研究工作大多基于 GR 模型中的无谷底 (valley-free) 假设, 主要分为本地识别检测与增加传递属性两种方法. 前者主要基于本地 BGP 历史数据分析与 AS 关系逻辑推理对路由泄露类型异常进

行识别与检测[18,19], 后者通过在 BGP 协议中增加标识路由策略期望的传递属性以防止路由策略违规传播[20,21]. 然而, 实际域间路由系统中并非所有自治域都遵从无谷底原则进行路由[8]. Zhao 等人提出一种具有隐私保护特性的域间路由承诺遵从性验证方法 SPIDeR[22], 基于安全多方计算验证自治域路由行为是否遵从与其邻居间建立的自主策略协定. 但 SPIDeR 只能用于 BGP 消息下游 AS 验证相邻上游 AS 的选路策略, 且无法应对参与者恶意滥用的情况 (如: 多个 AS 合谋). Li 等人提出了一种策略期望交换与执行机制 E3[23], 能够在任意 AS 间验证通用的自治域自主路由策略符合性, 但未考虑策略隐私问题. 近年来研究者尝试运用区块链技术解决域间路由安全问题[24], 但基于区块链的域间路由策略符合性验证研究尚处于初步探索阶段. 我们在前期工作中提出一种基于区块链和智能合约的域间路由综合安全方案 ISRchain[25], 但其中的路由策略符合性验证基于无谷底假设. Liu 等人针对 SPIDeR 无法应对合谋攻击的缺陷, 提出一种基于区块链的域间路由遵从性验证模型 BRVM[26], 但其只能验证最短路优先策略, 不适用于实际中由商业关系驱动的复杂域间路由策略. Galmés 等人提出一种基于区块链的路由泄露防范方法[27], 通过将自主策略同步上链提供通用的策略符合性验证, 但该方法不能保证路径真实性, 恶意自治域依然可通过篡改并宣告虚假路径实施路由泄露攻击. 综上, 如何在保证自治域策略隐私性的前提下针对通用的路由策略符合性进行可靠验证是尚未解决的关键问题.

本文提出一种基于区块链的域间路由策略符合性验证方法 (inter-domain routing policy compliance validation, IRPC). IRPC 使自治域能够在区块链上以隐私方式发布本地路由策略期望, 并指定其他自治域完成对路由策略期望的验证和执行, 从而确保 BGP 路径的传播符合 AS 间协定的出站策略, 防止路由泄露的发生. 为了保证路由策略符合性检查的可靠性, IRPC 引入路由证明, 对应每一个更新路由, 将 BGP 路由的传播过程以防篡改方式记录于区块链分布式账本, 保证路径传播的真实性. IRPC 采用全局-本地双层验证方式, 当路由证明与策略期望证明安全地同步到区块链后, 参与自治域可将与本地相关的信息下载并配置于本地 BGP 路由器缓存中, 以对收到的更新路由进行策略符合性验证并执行相应的过滤操作. IRPC 的参与自治域实质上构成基于区块链的多方协同信任覆盖网络, 在不依赖任何中心信任机构的情况下实现路由信息与策略信息的共享, 由参与自治域协同完成路由策略符合性验证, 并能够满足自治域对本地策略灵活配置与隐私保护的需求. 为了验证 IRPC, 基于 Python 开发了原型系统, 并运用真实 BGP 数据进行了仿真实验. 实验结果表明, IRPC 能够有效抑制路由泄露事件期间策略违规路由的传播, 且其时间与空间开销能够满足实际域间路由系统需求. IRPC 与 BGP 并行工作, 支持增量部署, 且具有通用性, 可应用于路由策略遵从性验证、路径真实性认证、流量工程需求调度等场景.

本文第 1 节介绍背景知识. 第 2 节给出问题描述. 第 3 节介绍 IRPC 设计细节与工作机理. 第 4 节是实验与分析. 第 5 节总结全文.

1 背景知识

1.1 AS 商业关系

域间路由系统中相邻自治域间的商业关系一般有 3 种: (1) customer-provider; (2) peer-peer; (3) sibling-sibling. 在 customer-provider 关系中, 作为 provider 的运营商 AS 为其 customer AS 提供需付费的流量传输服务; 在 peer-peer 关系中, 两个具有相似网络规模的 AS 根据彼此的协定可互相交换来自本地 customer 的指定限额流量; 在 sibling-sibling 关系中, 两个属于同一组织的 AS 间协定互相提供定制的传输服务. 自治域实际运营中基于本地与不同邻居 AS 之间的商业关系配置不同的路由策略.

1.2 BGP 路由策略

BGP 是由策略驱动的路径矢量协议, 负责在各自治域间传递网络可达信息, 建立到达不同目的网络或节点的路由. 当一个自治域从某邻居节点收到通往目的前缀 p 的更新消息时, 首先将其放入入站路由表 (Adj-RIB-In), 然后根据本地入站策略从多条通往目的前缀 p 的更新消息包含的路径中选取其中一条放入本地路由表 (Loc-RIB), 最后根据出站策略决定将选择的通往目的前缀 p 的路由宣告给哪些邻居节点. 现在标准的路由策略模型是由 Gao 和 Rexford 建立的, 简称为 GR 模型. GR 模型充分考虑了自治域实现各自商业利益最大化的动机, 根据文献 [8]

的调研, 68% 的运营商自治域出入站策略均按照 GR 模型配置.

BGP 入站策略即自治域本地选择最佳路由的策略. 通常情况下, 首先按照最高本地优先级 (local preference) 作为优先决策因素进行筛选; 然后从本地优先级相等的路由中依据最短路 (shortest paths) 优先原则进一步筛选; 最后如果仍余下多于一条路径, 则可按地理位置、政策审查等其他因素作为决胜局 (tie-break) 的决策依据选出通往目的前缀 p 的最佳路由. 在 GR 模型的入站策略中, 通过相邻 customer 的路由本地优先级 (local preference) 高于通过相邻 peer 或相邻 provider 的路由, 即客户优选原则.

BGP 出站策略即自治域将最佳路由发布给邻居的策略. 当自治域完成选路后, 根据出站策略决定把选择的最佳路由宣告给哪些邻居 AS, 或者不宣告该路由. 出站策略通常由 AS 间的商业关系决定, 因此通常是不对外公开的. GR 模型的出站策略为: 来自 customer 的路由可以宣告给所有相邻 AS; 来自 peer 和 provider 的路由只能宣告给本地相邻的 customer, 这也被形象地称为“无谷底原则”.

1.3 路由泄露

RFC7908[28]给出的路由泄露定义为: 路由泄露是指路由超出预期范围的传播. 即一个 AS 将收到的 BGP 路由宣告给另一个 AS 的行为违反了接收者、发送者或前面路径 (AS-path) 中任意 AS 的期望策略. 这些期望策略通常是根据 AS 两两之间的商业关系 (如: customer-provider, peer-peer) 来定义的. 路由泄露会造成流量向非预期路径重定向, 进一步可能导致流量窃听、链路过载、流量黑洞. 意外误配置或恶意攻击均会导致路由泄露, 但最常见的触发原因是意外误配置. 下面举两个路由泄露的典型例子.

图 1(a) 是 customer 路由泄露的例子. 当目的前缀 p 的拥有者 D 向其邻居传播到达 p 的路径时, C 错误地将从本地的 provider B 处获取的路径传播给本地的另一个 provider A, 导致 A 在选路时根据客户优选原则优先选取从其 customer C 处获取的路径 p: [C, B, D], 从而使 A 通往 D 的网络流量重定向到 C 处, 会导致链路负载或流量窃听等后果. 图 1(b) 是 peer 路由泄露的例子. E 错误地将从本地 provider B 处获取的到达目的前缀 p 的路径传播给本地的 peer D, D 在选路时会从 p: [A, C] 和 p: [E, B, C] 中优先选取从 peer 处获取的后者, 导致 D 通往 C 的网络流量从 D→A→C 变为 D→E→B→C, 违反了无谷底原则.

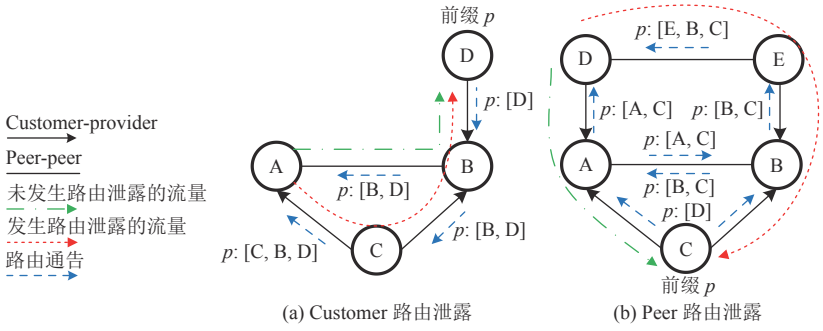

图 1 路由泄露的典型例子

值得注意的是, 域间路由系统实际运营中并非所有自治域都遵循无谷底原则, 在一些复杂的商业关系中自治域具有允许谷底路由存在的需求[29,30]. 例如在图 1(a) 中, 当 A 和 B 同时为 C 的备份提供商, 或 A 与 B 的 peer 连接关系仅为备选路径时, 可达成协定, 允许 C 将从 A 或 B 处获取的路径转发给 B 或 A. 本文的解决方案也支持对良性谷底路由等特殊策略需求的符合性验证.

2 问题描述

自治域路由策略符合性是指自治域在参与 BGP 路由过程中采用的入站/出站策略是否符合与其相邻的路径前驱自治域/后继自治域根据商业关系等因素制定的路由策略协定, 出于对本地路由策略的隐私保护及多样化自主路由策略的需求, 在针对自治域出站策略符合性进行验证时, 需保证合理的隐私性[8], 主要包括: (1) 任意 AS 除

已从 BGP 报文中获取的其他 AS 信息外, 不能额外推测出其他 AS 关系信息; (2) 任意 AS 可根据本地策略隐私需求对指定 AS 合理披露其路由策略信息, 其他非指定 AS 不能获取路由策略具体内容.

为了具体描述本文自治域路由策略符合性验证问题, 我们用图 2 表示域间路由系统中的一个自治域对通往某目的网络的路径选路和传播的情景. 自治域 E 在图 2 中有 4 个邻居节点 A、B、C、F, E 在与邻居自治域建立 BGP 连接时根据彼此商业关系和本地路由偏好达成出站策略协定 (如: E 向 A 承诺不把从 A 处接收到的路由信息传递给 E 的 provider 和 peer). 在 D 宣告本地具有前缀 p 后, A、B、C 分别从某个本地邻居处获取了一条通往目的前缀 p 的路由 p: [r1, D]、p: [r2, D]、p: [r3, D], 并将其选取为最佳路由继续通告给邻居 E (r1、r2、r3 分别为发送给 A、B、C 相应最佳路由的邻居自治域通往目的前缀 p 的路径). 当 E 收到由其 3 个邻居 A、B、C 宣告的通往目的前缀 p 的 3 条不同的路由后, 选取由 A 发送的路由 p: [A, r1, D] 作为最佳路由, 并根据与最佳路由发送者 A 之间的协定决定是否将该路由告诉 F. 然而, 由于自治域对路由策略的隐私考虑, F 并不知道 E 与 A 之间的路由策略协定, 进而无法验证 E 对路由 p: [A, r1, D] 的出站行为是否符合路径中 E 的后继自治域 A 的策略预期. 若 E 恶意 (或失误) 将 p: [E, A, r1, D] 违规出站传递给 F 并被 F 接收, 导致通往 D 的数据流量重定向至非预期路径 F→E→A, 且该非预期路径会不断地传播下去对网络稳定性造成更大的影响. 因此, 需要一种路由策略符合性验证方法, 在不揭露 AS 关系和策略内容的前提下, 使得 F 在收到路由 p: [E, A, r1, D] 后, 可对 E 的路由出站策略符合性进行检查, 根据检查结果决定是否将 p: [E, A, r1, D] 选为最佳路由并传播给其他自治域.

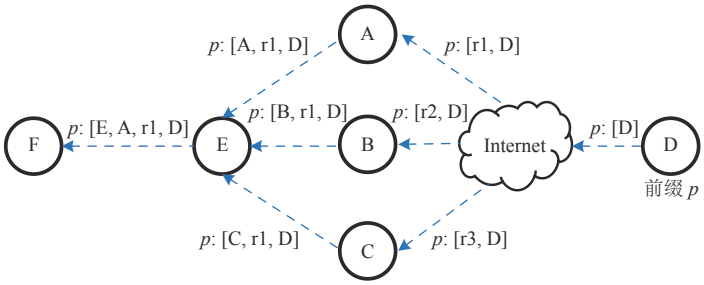

图 2 问题描述情景

综上, 本文要解决的问题是: 在满足自治域隐私保护需求的前提下, 验证自治域出站策略是否符合与其相邻的出站路径后继自治域之间根据商业关系制定的路由策略协定, 并保证验证过程可追溯、防篡改.

3 IRPC

针对上述问题, 提出一种基于区块链的域间路由策略符合性验证方法 IRPC, 利用区块链去中心化、防篡改、可追溯的属性, 使自治域能够以隐私方式发布与交互路由策略期望, 并通过生成对应路由更新操作的路由证明来保证路径真实性. 本节首先概述 IRPC 的整体框架与工作机理, 然后引入路由策略期望与路由证明的概念, 最后给出 IRPC 的策略符合性验证算法.

3.1 IRPC 概述

IRPC 的整体架构与工作流程如图 3 所示. 在 IRPC 中, 自治域需经过许可后方可参与到策略符合性验证中, 每个参与自治域需要运行一个代表本自治域的区块链 IRPC AS 节点, 在不引起混淆的情况下, 下文简称其为 AS 节点. 每个 AS 节点都持有一对公钥-私钥对, 其公钥的哈希值作为该 AS 节点的唯一身份标识. 所有参与 IRPC 的 AS 节点共同构成逻辑上的信任覆盖网络, 用于共享策略期望和路由证明, 并协同验证路由策略符合性. 在 IRPC 中有两种交易类型: 策略期望 (policy expectation, PE) 与路由证明 (route proof, RP). AS 节点根据自身策略需求在链上发布策略期望, 在路由过程中对本地发出或转发的路由消息生成路由证明, 并将其发布上链, 然后路径的接收自治域基于区块链中存储的路由证明与策略期望交易信息进行路由策略符合性验证. 这里我们假设 AS 节点的数字签名不可伪造, 且路由更新的发起 AS (origin AS) 会诚实地发布路由证明与策略期望.

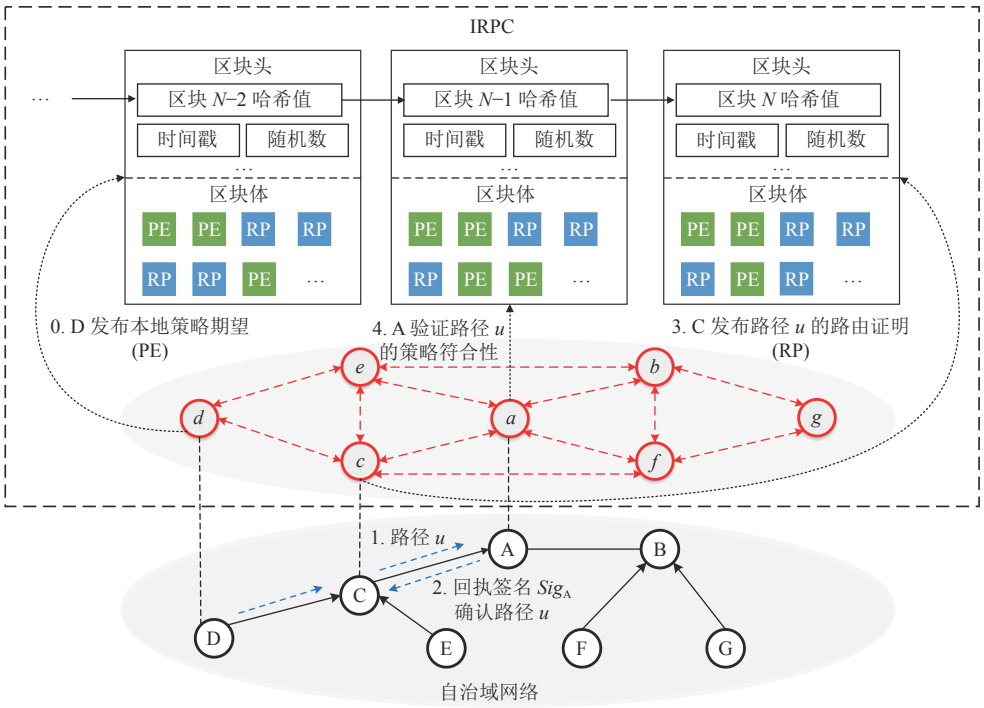

图 3 IRPC 整体框架与工作流程

IRPC 利用区块链同步策略期望与路由证明, 形成分布式账本, 从而使参与自治域能够在去中心化信任的基础上, 实现可追溯、防篡改的路由策略符合性验证, 提供可靠的域间路由安全事件溯源证据. 以图 3 为例, IRPC 工作流程的主要步骤为: (0) D 对应的 AS 节点 d 将其策略期望以区块链交易的形式发布到 IRPC 区块链网络, 经各 AS 节点验证后上链; (1) C 收到并选择了来自 D 的路径 u, 将其出站转发给 A; (2) A 收到 C 发送的路径 u 后, 对路径基本信息进行数字签名并将签名回执发送给 C, 表明 A 已收到路径 u; (3) C 收到 A 的签名回执后, 由 AS 节点 c 创建路径 u 的路由证明 $RP(u)$, 并以交易形式发布至 IRPC 区块链网络, 经验证后上链; (4) A 对应的 AS 节点 a 通过检索 IRPC, 获取相关路由与策略信息, 从而进行路由策略符合性验证, 并向 A 返回对于路径 u 的检查结果. 注意在上述过程中, IRPC 中的策略期望与路由证明的上链存储遵循区块链系统中的交易同步过程, 即节点创建交易后广播至区块链网络, 经由各节点验证后基于共识机制封装区块并发布, 最终加入区块链账本, 达成一致存储.

为了优化路由策略符合性的验证时间, 每个 IRPC AS 节点运行在物理上与 BGP 路由器独立的专用服务器中, 并对应一个运行在 BGP 路由器中的本地验证节点. 策略期望与路由证明发布时, IRPC AS 节点负责基于链上共识机制在区块链网络中完成同步与存储. 本地验证节点负责定期接收 IRPC AS 节点下发的区块并将与本地相关的路由证明与策略期望存储于缓存中以供查询. 区块链的链式存储结构支持每个 IRPC AS 节点对应的本地验证节点根据由路由发送者 IDs、路由接收者 IDr、目的前缀 p 构成的索引生成与该 AS 相关的独立路由证明链. 具体地, 对于任意的 ASr, 可将 $(*, IDr, p)$ 作为索引, 仅将通往某目的前缀 p 和 ASr 作为路由接收者的路由证明按序存储于本地路由验证缓存中.

3.2 策略期望

自治域出于商业关系、备选链路、流量均衡、政治冲突等因素, 具有不同的路由策略期望. 在 IRPC 中, AS 节点可根据本地自主路由策略, 在区块链中发布并存储路由策略期望. 借鉴文献 [27] 中给出的 BGP 路由策略形式化语言, 并考虑自治域对策略的隐私需求, 给出策略期望的定义如下.

定义 1. 策略期望 (policy expectation). $PE(e,p,s)=(ID(e,p,s),Info(A,R,V),Sig_e)$ 是指 AS 节点 e 针对到达目的

前缀 p, 且路径中包含指定验证 AS 节点 s 的路由所期望的路由传播策略规则, 其中:

• $ID(e, p, s)$ 代表策略期望索引, 是策略期望对应的唯一标识, 具体为发布 AS 节点、目的前缀与指定验证节点的哈希值 $hash(e, p, s)$.

• $Info(A, R, V)$ 代表策略期望内容, 包括 Community 属性值 A (根据 RFC 规范[31−33]设置), 策略期望规则 R (通常包括 LOCAL_PREFERENCE, PREPEND, NO_EXPORT, NO_PEER), 策略期望取值 V (定义策略期望程度的整数, 仅应用于某些类型的规则).

• Sig_e 代表策略发布方数字签名, 具体为 $D_{Ska}(ID(e,p,s),Info(A,R,V))$.

在自治域创建策略期望交易时, 若需要由指定 AS 节点保证该策略期望的正确执行, 则使用指定策略期望验证节点的公钥对策略期望进行加密. 具体地, 任一 AS 节点 a 发布针对目的前缀 p 的路由, 且指定期望验证 AS 节点 s 的策略期望交易由交易唯一标识 $txid$、交易类型 PE、时间戳 $timestamp$、策略期望 $PE(a,p,s)$ 组成, 其创建与上链的步骤如下.

(1) 策略期望交易创建. AS 节点 a 根据本地路由策略及其隐私需求创建策略期望交易 ($txid$, PE, $timestamp$, $PE(a, p, s)$), 为了保证该策略期望内容仅由 AS 节点 s 可见, 使用 s 的公钥 Pks 对其进行加密.

(2) 交易广播. AS 节点 a 将创建的策略期望交易广播至 IRPC 区块链网络.

(3) 交易验证与区块封装. IRPC 区块链网络中其他 AS 节点在接收到该策略期望交易后, 对其进行验证, 合法交易纳入待封装区块的交易池, 并被获得区块记账权的 AS 节点打包到一个新建的区块中.

(4) 区块广播. 新区块在 IRPC 区块链网络中被广播并由各 AS 节点进行验证.

(5) 交易上链. 新区块中所封装的交易验证无误后, 为 IRPC 区块链网络中的所有 AS 节点保存, 纳入本地区块链账本中.

以图 1(b) 中的路由泄露场景为例, AS C 出于地理政治等因素, 不希望 AS A 将路径 p: [A, C] 转发给 AS B, 且只希望 AS B 能够获取并执行该策略期望. AS C 的策略期望可表示为 $PE(A, p, B)$=(65281, NO_EXPORT, \), 其中 65281 为该策略期望对应的 Community 属性值; NO_EXPORT 为策略期望规则, 这里为出站限制. 由于 AS C 只希望该策略期望由 AS B 验证并执行, 因此 AS C 在发布策略期望时首先对其执行内容 (65281, NO_EXPORT, \) 使用 B 的公钥加密得到 E_{PkB}(65281, NO_EXPORT, \), 然后使用本地私钥生成策略期望的数字签名 Sig_C; 最后将创建的策略期望交易广播至 IRPC 区块链网络, 经其他 AS 节点验证后, 根据共识机制封装至区块并写入分布式账本, 完成上链. B 在收到 A 发来的更新路径 p: [A, C] 时, 通过匹配策略期望索引并进行确认签名和解密操作, 检查发送路径的 AS A 的转发行为是否符合其路径上游 AS C 的策略期望.

3.3 路由证明

路由策略符合性验证需在保证域间路由传播的路径真实性的基础上进行. 为了保证路由传播的真实性和可追溯性, IRPC 将域间路由的每一次传递过程以路由证明交易的形式分布式存储于区块链, 并对每一个路径标记相应的策略类别. 下面分别给出路径策略类别与路由证明的定义.

定义 2. 路径策略类别 (policy class of route). $PC(u)$ ={0/1}代表路径 u 的策略类别, 其中:

• 0 类别代表无策略期望, 路径 u 可由接收 AS 继续传递给任意 AS.

• 1 类别代表具有策略期望, 需查询宣告路径 u 的 AS 节点发布的策略期望并验证策略符合性.

定义 3. 路由证明 (route proof). $RP(u)$ =($PRP(u)$, $Info(u)$, $ID(u)$, Sig_r, Sig_t) 是对路径 u 所包含路由信息的证明, 唯一对应由 ASt 发送给 ASr 的一条路径 u, 在路径策略符合性验证中代表该路径, 其中:

• $PRP(u)$ 代表路径 u 的上一跳路由证明 (preceding route proof) 的索引, 即路径 u 的发送者 ASt 作为接收者收到并选择的路径对应的路由证明.

• $Info(u)$ 代表路径 u 的基本信息, 包括发送者 ID ASt, 接收者 ID ASr, 时间戳 $timestamp(u)$, 目的前缀 $prefix(u)$, 路径策略类别 $PC(u)$.

• $ID(u)$ 代表路径 u 的索引, 是路径 u 的唯一标识, 具体为路径信息的哈希摘要 $hash(ASt, ASr, timestamp(u)$,

prefix(*u*)).

• Sig_r 代表接收者在收到路径 *u* 之后反馈的数字签名 *DSKr*(*u*), 以确认路径 *u* 被 *ASr* 收到.

• Sig_t 代表发送者的数字签名, 具体为 *DSKt*(*PRP*(*u*), *Info*(*u*), *ID*(*u*), Sig_r), 用于验证路由证明中的内容未被篡改过.

在 IRPC 中, 每个 AS 在向其邻居 AS 宣告路由时, 在 IRPC 区块链网络中创建并发布相应的路由证明交易. 具体地, AS 节点 *a* 发布针对目的前缀 *p* 的路由 *u* 时, 创建的路由证明交易由交易唯一标识 *txid*、交易类型 *RP*、时间戳 *timestamp*、路由证明 *RP*(*u*) 组成, 其在 IRPC 的上链过程与策略期望交易一致. 在路由传播过程中, 所有通往一个目的前缀的路由证明在逻辑上依次相连, 被组织为一条路由证明链 (route proof chain, *RPC*).

如图 4 中的场景所示, 当 A 作为目的前缀的拥有者向其邻居 AS 发布路径 *w*, B 接收到路径 *w* 并将其选择为最佳路由, 对其进行签名后作为回执返回给 *w*, A 生成路径 *w* 的路由证明 *RP*(*w*) 并发布到 IRPC; 当 B 根据路径 *w* 创建新的路径 *d* 并继续传递给本地邻居 C 时, 也用同样方式生成 *RP*(*d*), *RP*(*d*) 的上一跳路由证明 *PRP*(*d*) 即为 *RP*(*w*) 的索引, C 可通过 *RP*(*d*) 中的 *PRP*(*d*) 找到 *RP*(*w*), 进而根据 *RP*(*w*) 中的路径策略类别 *PC*(*w*) 及相应的策略期望证明判断 B 的路由行为是否违反了 A 的策略期望. 同样地, 当 C 选择了路径 *d*, 创建新路径 *u* 传递给邻居 E, 并生成 *RP*(*u*) 时, E 也可以根据 *RP*(*u*) 的上一跳路由证明 *RP*(*d*) 对 C 进行路由策略符合性验证. 在 IRPC 中, *RP*(*w*), *RP*(*d*), *RP*(*u*) 等所有通往目的前缀 *p* 的路径对应的路由证明构成逻辑上的路由证明链 *RPC*. *RPC* 可用于验证更新路径发送 AS 的策略合规性, 确保路径的每一跳传递过程均没有违反路径上游的路由策略, 防止策略违规路径的不断传播, 并为合谋攻击等复杂安全事件提供溯源证据.

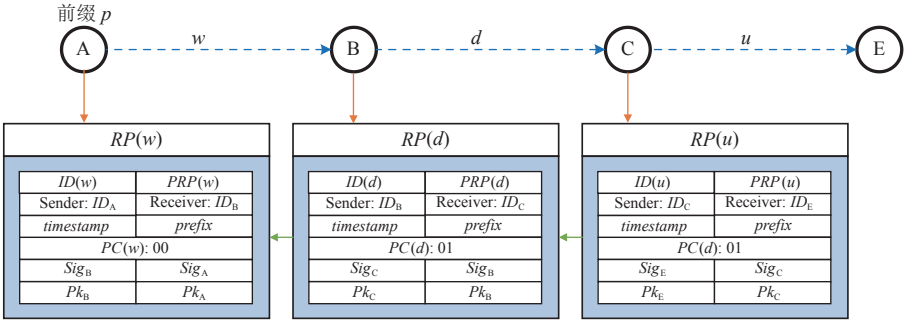

图 4 IRPC 路由证明链

3.4 策略符合性验证

IRPC 基于链上存储的策略期望与路由证明信息完成策略符合性验证. 当自治域收到 BGP 更新消息后, BGP 更新消息的接收者通过在 IRPC 区块链中查询相应的路由证明及策略期望判断发送该 BGP 更新消息的 AS 是否遵循了路由策略承诺.

IRPC 的路由策略符合性验证 (policy compliance validation, PCV) 算法如算法 1 所示. 当 *ASr* 接收到来自 *ASt* 发送的路径 *u* 时, 首先检查路由的基本信息的真实性 (1–5 行): (1) 根据路径 *u* 对应的路由证明 *RP*(*u*) 及其上一跳路由证明索引 *RP*(*u*).*PRP*(*u*), 检查其是否存在 (1–3 行); (2) 检查路径 *u* 上一跳路径 *v* 的路由证明中的前缀一致性 (4–5 行), 确保路径 *u* 在传播过程中目的前缀和 AS 路径未被篡改. 然后分别使用接收 *ASr* 和发送 *ASt* 的公钥验证路由证明中的数字签名 (6–7 行), 确保发送路由证明的 AS 节点与检验 AS 节点的身份真实性; 最后对 *ASt* 的路由转发行为进行策略符合性验证 (8–15 行): 当 *RP*(*v*). *PC* 为 1 时, 代表路径 *v* 的发送 AS *RP*(*v*).*IDt* 对于该路径的传播具有策略期望, 并在 IRPC 中发布了该策略期望. 在该情况下, 分别将代表路径 *u* 接收自治域的 *RP*(*u*).*IDr* 、路径 *u* 的目的前缀 *u*.*prefix* 和上一跳路径发送自治域对应的 AS 节点身份标识 *RP*(*u*).*IDt* 共同生成哈希摘要作为待匹配项 *Matchitem*, 与 IRPC 中存储的策略期望交易索引键值进行匹配 (8–10 行). 若存在索引项为 *Matchitem* 的策略期望 *PE*, 则继续验证策略期望发布 AS 的签名是否正确, 以及 *PE* 的策略期望内容 (*A*, *R*, *V*) 是否可由接收 AS 节点 *RP*(*u*).*IDr* 的私钥解密或为公开未加密内容, 进而根据该策略期望内容判断 *ASt* 对路径 *u* 的宣告行为是否策

略合规 (11–15 行).

由于 IRPC 采用本地-全局的验证机制, 本地验证缓存位于物理路由器中, 在执行 PCV 算法时, 可直接检索本地缓存中的路由证明链 RPC 及对应的策略期望 PE. 假设不同目的前缀数量为 v, 参与 AS 节点数量为 w, AS 平均邻居个数为 d, 每条路由变化次数为 c, 发布策略期望的 AS 节点数量为 b, 则 IRPC 在全局进行检索的时间开销为 $O(wvc)+O(b)$, 本地缓存检索时间开销为 $O(dvc)+O(d^2)$. 当前域间路由系统中自治域数量与拓扑数据较为稳定, 目前有 70 400 个 AS, 其中非底层的传输 AS 有 10 200 个; 路由 AS-path 平均长度为 5.7; AS 的平均邻居个数为 5[34]. 因此, IRPC 进行路由策略检验的时间开销可稳定在合理范围内.

算法 1. 路由策略符合性验证 PCV $(u.prefix, u.ASpath, t, r)$.

输入: 路径 u 的目的前缀 $u.prefix$; AS 序列 $u.ASpath$; 发送 ASt; 接收 ASr;
输出: 发送 ASt 对路径 u 的宣告行为是否策略合规 (True/False).

1. **if** 在 IRPC 中不存在 $RP(u).PRP(u)$:
2. **return** False;
3. $RP(v) \leftarrow RP(u).PRP(u)$;
4. **if** $RP(v).prefix \neq u.prefix$:
5. **return** False;
6. **if** $RP(u).Sig_r$ 或 $RP(u).Sig_t$ 签名验证失败:
7. **return** False;
8. **if** $RP(v).PC == 1$:
9. $Matchitem \leftarrow hash(RP(v).IDt, u.prefix, RP(u).IDr)$;
10. **if** 在 IRPC 中存在索引项为 $Matchitem$ 策略期望 PE:
11. **if** $PE.Sig_{RP(v).IDt}$ 签名验证成功:
12. **if** PE 的策略期望内容 (A, R, V) 可用 $Sk_{RP(u).IDr}$ 解密或为公开策略期望:
13. **if** 发送 ASt 对路径 u 的宣告行为违反 PE 的策略期望内容 (A, R, V):
14. **return** False;
15. **return** True;

4 实验与分析

本节通过实现 IRPC 的原型系统并基于真实路由泄露事件开展实验, 分别对 IRPC 的有效性、可扩展性与隐私性进行分析.

4.1 仿真实验设计

我们初步实现了具备 IRPC 功能的原型系统, 当前为使用 Python 开发的私有链, 采用 PoW 共识机制, 底层数据存储基于 MangoDB 实现, 运行在一台 16 GB 内存, Intel®Core™ i7-7500U CPU @ 2.70 GHz/2.90 GHz 的服务器. 原型系统中的 AS 节点基于 CAIDA 提供的域间路由拓扑数据 (http://data.caida.org/datasets/topology/) 和 AS 关系数据集 (http://data.caida.org/datasets/as-relationships/) 生成, 共有 28 817 个模拟 AS 节点, 分别代表域间路由系统中相应的自治域. 原型系统中选用 RSA-1024 用于签名, SHA-512 用于哈希. 仿真实验以发生于 2019 年 6 月 24 日 10:30 UTC 的 Cloudfare 路由泄露事件[14]为背景, 基于 Routeviews 提供的更新报文数据, 模拟 AS 节点路由策略符合性验证的过程. 参考文献 [23] 中的分类方法, 将自治域按照 ASrank (https://asrank.caida.org/) 提供的排序分类, 将前 100 个 AS 作为 tier-1 AS, 接下来 900 个 AS 作为 tier-2 AS, 1 000 个 AS 作为 tier-3 AS. 通过在不同层级部署不同比例的路由策略符合性验证节点, 分别针对策略违规次数、时间开销、空间开销等指标开展实验, 进而分析

IRPC 的有效性、可扩展性与隐私性.

4.2 有效性分析

为了评估 IRPC 的有效性, 我们首先分析了在全部署情形下 IRPC 路由符合性验证的正确性, 然后根据 2019 Cloudfare 路由泄露事件期间的 BGP 更新报文数据, 测量在 IRPC 没有部署的情况下接收或传播策略违规路由的 AS 个数 (polluted AS), 并以此作为有效性评价基线; 最后, 我们测量在不同 AS 部署比例情况下, 接收或传播策略违规路由的 AS 个数占评价基线的百分比, 作为评价 IRPC 增量部署有效性的指标.

在 IRPC 全部署情况下, 可以保证路由的传播过程不违反路由路径中每一跳 AS 的出站策略. IRPC 路由策略符合性验证正确性由路由证明与策略期望证明共同保证. 从路由证明的方面, 当每个自治域发出或转发路由消息时, 对应 AS 节点需要发布包括路由本地签名与接收者签名的路由证明. 若其中某 AS 节点发布了虚假的路由证明, 路由接收者可通过追溯路由证明链中的其他路由证明检测出路由证明的不一致. 根据第 4.1 节中 AS 节点的数字签名不可伪造且路由更新的发起 AS (origin AS) 会诚实地发布路由证明与策略期望的假设, 即使在多个 AS 节点合谋的情况下, 也可保证路径真实性和不可篡改性, 这是路由策略符合性验证的必要条件. 从策略期望证明的方面, IRPC 的期望发布需经发布者签名, 以保证策略期望发布实体身份的真实性和策略期望内容的完整性. IRPC 对策略期望的链上存储, 使得发布节点不可否认其发布策略期望, 便于故障溯源, 能够防止 AS 节点滥用策略期望发布机制. IRPC 的关键在于区块链中记录的路由证明与策略期望证明的正确性和完整性. 对于滥用 IRPC 的恶意 AS 节点合谋攻击, 其成功的概率取决于区块链中的一致性算法, 以 PoW 共识机制为例, 当恶意 AS 节点不超过总节点个数的 50% 时, 可避免此类攻击.

在 IRPC 局部部署情况下, 我们以 2019 年 Cloudfare 路由泄露事件为仿真实验背景, 通过复现路由节点间的 BGP 更新报文交互, 分析 IRPC 以不同比例部署在不同层级 AS 时, 未被抑制的策略违规路由占原有违规路由数量的百分比, 从而评估 IRPC 在部分部署情况下的有效性. 我们首先测量 Routeviews Oregon 采集点 UTC 时间 2019 年 6 月 24 日 10:00–11:00 期间的 BGP 更新报文数据, 统计出共有 207 个 AS 违规传递 provider-provider 谷底路由 56 549 条, 50 个 AS 违规传递 peer-peer 谷底路由 9 128 条. 然后将 IRPC 的 AS 节点分别以不同比例部署于 tier-1 AS、tier-2 AS 和 tier-3 AS, 研究在部署后策略违规路由的传播情况. 对于每个层级的不同部署比例均运行了 10 次实验, 对每次得到的违规谷底路由数量计算均值. 如图 5 所示, 当 IRPC 以 40% 的比例分别部署于 tier-1、tier-2 和 tier-3 的 AS 时, provider-provider 违规谷底路由的个数分别是未部署情况下的 51.5%, 83.2%, 99.3%; 随着部署比例的不断增加, 部署在 tier-1 AS 的情况下 provider-provider 违规谷底路由减少的速度最快, 部署在 tier-2 AS 次之, 部署在 tier-3 AS 最慢. 当 80% 的 tier-1 AS 部署 IRPC 时, provider-provider 违规谷底路由个数减少到原有的 10% 以内. 同样, 如图 6 所示, 对于数量偏少的 peer-peer 谷底路由而言, 当 IRPC 以 40% 的比例部署于 tier-1、tier-2 和 tier-3 的 AS 时, peer-peer 违规谷底路的个数分别是未部署情况下的 59.8%, 68.8%, 88.6%. 随着在不同层级 AS 中部署 IRPC 的比例增加, 部署于 tier-1 AS 时能够抑制更多 peer-peer 违规谷底路由的传播. 当 80% 的 tier-1 AS 部署 IRPC 时, peer-peer 违规谷底路由个数减少到原有的 25%. 综上, 当 IRPC 以超过 50% 的比例部署时, 能够防止 50% 以上策略违规路由的传播; IRPC 部署在 tier-1 AS 时对策略违规路由抑制的效果最为显著, 当 IRPC 以 80% 的比例在 tier-1 AS 中部署时, 对所有类型的策略违规路由传播的抑制比例可达到 87.9% 以上, 即 tier-1 中的 AS 节点通常是对路由泄露事件具有决定传播范围的关键节点.

由于当前不基于无谷底假设的通用策略符合性验证工作中, SPIDeR[22]与 BRVM[26]仅针对入站选路策略进行验证, 且目前均只给出验证最短路优先策略的具体方法, 解决的问题与 IRPC 不同; E3 与文献 [27] 可以针对通用路由策略符合性进行验证, 但文献 [27] 提供的功能范围不包括路径真实性证明, 且未给出相关实验. 为了进一步比较 IRPC 与同类工作在不同部署情景下对路由泄露的抑制能力, 我们以 E3[23]作为比较对象. 我们采用与 E3 的仿真实验同样的数据集和部署情景, 基于 2012 年加拿大路由泄露事件数据[35]测量了 IRPC 以不同比例部署时错误传播策略违规路由的自治域数量减少的比例, 并与 E3 的实验结果进行对比, 如图 7 所示. 由图 7 可看出, 对于 tier-3 AS, IRPC 与 E3 对于自治域错误转发策略违规路由的抑制能力相差不大; 对于 tier-2 AS, 随着 IRPC 和 E3 部署比

例的增加, IRPC 相较于 E3 能够防止更多的自治域传播策略违规路由; 对于 tier-1 AS, 当 IRPC 和 E3 的部署比例小于 40% 时, 随着部署比例的增加, IRPC 对应的策略违规自治域数量的减少速度比 E3 更快, 但当 E3 在 tier-1 AS 中的部署比例达到 50% 时就能够防止所有自治域错误转发策略违规路由, 而 IRPC 在 tier-1 AS 中的部署比例需达到 70% 才能抑制所有自治域的策略违规行为. 上述现象表明 IRPC 在 tier-2 AS 和 tier-3 AS 中部署的有效性优于 E3, 在 tier-1 AS 中较小比例部署时有效性优于 E3, 但需达到较高部署比例才能防止所有自治域传播策略违规路由. 导致上述问题的原因可能是本文的仿真实验无法获知部分处于 tier-1 的大型运营商 AS 的本地路由策略, 仅能基于已有公开 AS 商业关系和策略开展. 然而在实际应用中 IRPC 提供的策略隐私保护功能可以促使自治域发布并验证更丰富的路由策略.

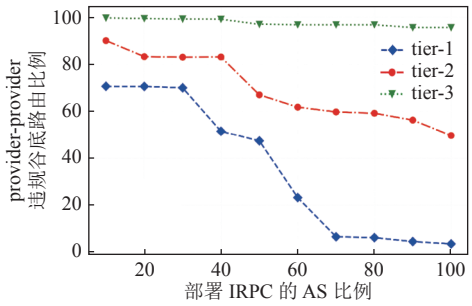

图 5 IRPC 对 provider-provider 违规路由的影响

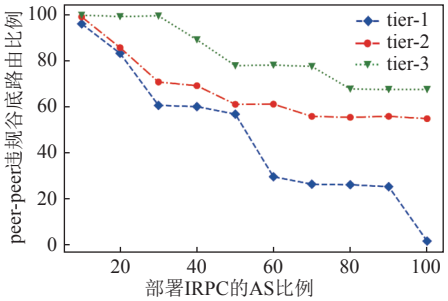

图 6 IRPC 对 peer-peer 违规路由的影响

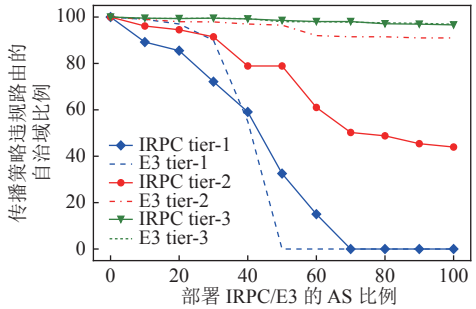

图 7 IRPC 与 E3 的有效性比较

4.3 可扩展分析

为了分析 IRPC 时间规模的可扩展性, 我们基于 IRPC 原型系统分别对上链确认时间及策略符合性验证时间进行测量与分析. IRPC 原型系统中每个区块最多能包含 390 个路由证明或 380 个策略期望证明. 设置区块时间为 3 s. 因此 IRPC 确认一个路由证明交易和策略期望交易的时间分别为 7.7 ms 和 7.9 ms, 平均每秒交易量为 130 个. IRPC 采用本地-全局的验证机制, 本地验证节点只将于本地关联的路由证明和策略期望证明缓存于物理路由器中, 因此我们分别对 IRPC 策略符合性验证的本地时间和全局时间进行实验. 本地验证时间取决于本地缓存大小, 因此我们分别测试了 50 个 tier-1 AS 节点和 50 个 tier-2 AS 节点的本地验证时间 (对于每一个 AS 节点均进行 100 次测试并求均值). 如图 8 所示, 80% 的 tier-1 AS 节点的本地策略符合性验证时间在 300 ms 内; 80% 的 tier-2 AS 节点策略符合性验证时间在 125 ms 内. 这是因为相较于 tier-2 AS, tier-1 AS 拥有更多网络前缀和邻居 AS, 从而具有更多与本地关联的路由证明与策略期望证明. 当本地验证节点未在本地找到相应路由证明或策略期望时, 向全局 AS 节点发送验证请求, 每个 IRPC 全局 AS 节点维护同样的 IRPC 区块链分布式账本. 我们对 IRPC 全局策略符合性验证时间进行测试, 其中包括路由证明验证时间和策略期望验证时间. 如图 9 所示, 随着 IRPC 处理路由数量的增加, 全局策略符合性验证时间呈线性增长, 当路由数量为 15 000 时, IRPC 的全局验证时间需要 400 ms.

全局策略符合性验证时间主要由验证路由证明的时间组成, 策略期望验证的时间较少. 这是因为并不是路由路径中的每一个 AS 都具有策略期望, 在 IRPC 处理同等路由数量时, 策略期望存储一般小于路由证明存储. 当前域间路由系统中平均每秒产生 8.45 个 BGP 前缀更新报文, BGP 默认最小路由通告间隔时间为 30 s[34]. IRPC 原型系统同步路由证明或路由策略的每秒交易量平均为 130 个, 且路由符合性检查的时间规模在毫秒级别, 能够满足域间路由系统实际需求.

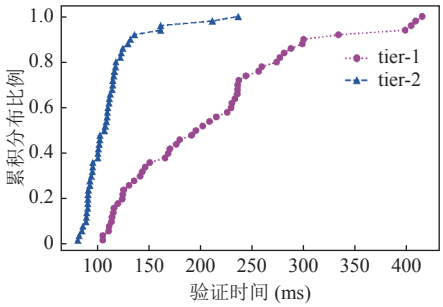

图 8 IRPC 本地验证时间

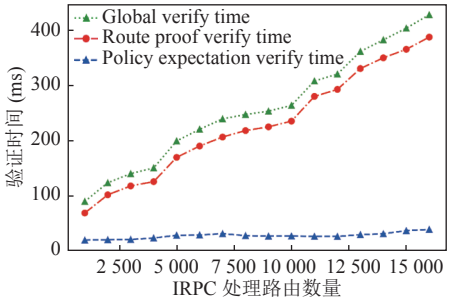

图 9 IRPC 全局验证时间

为了分析 IRPC 空间规模的可扩展性, 我们基于 IRPC 原型系统分别对路由证明及策略期望的空间开销进行测量并观察其增长趋势. 如图 10 所示, 存储路由证明与策略期望所需空间开销均随其数量增加呈线性增长, 当路由证明链上有 15 000 个路由证明时, 其空间开销约为 7.3 MB; 当策略期望链中具有 15 000 个策略期望时, 其空间开销约为 8 MB. 在路由证明与策略期望所占空间开销中, 加密签名所占存储比例分别为 33.82% 与 61.04%. 当前域间路由系统中每日更新报文数量约为 400 000[34], 因此 IRPC 全局路由证明链将以每日约 200 MB 的速度增长, 一年的路由证明约需 71.2 GB 的存储空间, 可以适应当前通用商用硬盘. 当前域间路由系统共有 70 400 个 AS, 通常具备策略期望的是其中 10 200 个传输 AS[36]. 为了估计具备策略期望的自治域数量, 我们统计了 Routeviews Oregon 采集点 2019 年 6 月 24 日全天 BGP 更新报文中携带的 Community 属性, 出现在当天 BGP 更新报文中的 AS 共有 61 136 个, 其中 2 526 个 AS 在路由更新中携带了 Community 属性, 每个 AS 平均声明 8.46 个不同的 Community 属性值. 考虑到 IRPC 提供的策略自主性和隐私性会激励更多的策略期望发布, 假设每个传输 AS 平均发布 10 个策略期望, IRPC 全局策略期望链所需空间开销约为 54.4 MB. 由于域间路由系统自治域数量相对稳定, IRPC 策略期望存储不会以较快的速度增长, 策略期望所需空间开销远小于存储路由证明的空间开销. 因此, IRPC 应用于实际域间路由系统的空间规模扩展性是可行的.

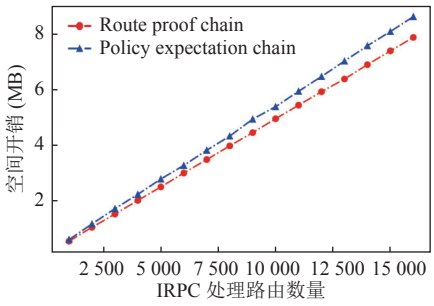

图 10 IRPC 存储开销

4.4 隐私性分析

本节从 AS 节点身份隐私及链上交易内容隐私两个方面对 IRPC 能够提供的隐私性进行分析.

从 AS 节点身份隐私的方面, IRPC 能够为参与自治域提供一定的身份匿名性. IRPC 适合基于许可链 (即私有链或联盟链) 实现, 只有经过授权的内部成员可以维护并查询 IRPC 区块链数据, 其他非授权节点没有接触 IRPC 区块

链中存储数据的通道. IRPC 区块链网络中, 每个 AS 节点的唯一身份标识均在本地生成, 无需第三方参与, 并且生成的唯一身份标识与 AS 号码信息无关. 因此, 相对于 IRR 数据库等方法, IRPC 具有更好的隐私性. 然而, 当 AS 节点在 IRPC 中发布的策略期望交易或路由证明交易上链后, 攻击者仍有可能关联用户地址与交易内容, 推测 AS 节点的真实身份并进一步获知其路由策略等敏感信息. 为此, IRPC 采用加密机制对交易中包含的敏感信息进行保护.

从链上交易内容隐私的方面, 加入 IRPC 区块链网络的攻击者很难获取 AS 商业关系与路由策略等敏感信息. 我们分别从路由证明与策略期望两类交易类型所披露的信息, 分析 IRPC 对路由策略和路由证明中的敏感信息保护能力. 在路由证明交易披露的信息方面, 对于任一路由证明, 对应唯一的一条路径及其相应 BGP 更新报文, 其披露的信息均为 BGP 更新报文中的已有信息. 因此, 攻击者很难从 IRPC 路由证明中获知 BGP 报文以外的信息. 在策略期望交易披露的信息方面, IRPC 采用加密机制保护具有隐私需求的策略期望交易内容, 即发布策略期望交易的 AS 节点使用指定策略期望验证节点的公钥对策略期望内容进行加密, 从而使得只有指定的 AS 节点能够解密并获取策略期望内容, 其他 AS 节点很难获取该策略期望的具体内容, 其难度取决于使用的公钥密码体制的安全性.

综上, IRPC 可以对上链的路由策略和路由证明包含的敏感信息进行保护, 可以满足第 2 节所描述的隐私需求. 对于攻击者进一步通过观察、关联、分析、推测所导致的身份和路由策略泄露风险, 可以将本文 IRPC 方案与地址混淆、信息隐藏和通道隔离等机制相结合[37], 以提供更强的隐私保护功能.

5 结束语

本文提出了 IRPC, 一种基于区块链的域间路由策略符合性验证方法. IRPC 通过隐私发布与分布式存储路由策略期望和路由证明链, 能够在保证自治域本地路由策略自主配置和隐私保护的条件下, 以自治域多方协同的方式完成路由策略符合性验证. 实验结果表明, IRPC 能够有效抑制路由泄露事件期间策略违规路由的传播, 且其时间与空间开销能够满足实际域间路由系统需求. 下一步工作将从 IRPC 功能扩展与部署验证两个方面展开: 基于 IRPC 提供的路由与策略信息扩展验证内容范围 (如: 路由选路承诺遵从性; 路由策略冲突检测等); 基于软件路由器与已有商用联盟链测试平台在不同网络拓扑与部署情景中进一步开展性能测试与可扩展性分析.

References:

[1] Rekhter Y, Li T, Hares S. A border gateway protocol 4 (BGP-4). RFC 4271, 2006.

[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] Kent S, Lynn C, Seo K. Secure border gateway protocol (S-BGP). IEEE Journal on Selected Areas in Communications, 2000, 18(4): 582–592. [doi: 10.1109/49.839934]

[4] White R. Securing BGP through secure origin BGP (soBGP). Business Communications Review, 2003, 33(5): 47–53.

[5] Goodell G, Aiello W, Griffin T, Ioannidis J, McDanial PD, Rubin AD. Working around BGP: An incremental approach to improving security and accuracy in interdomain routing. In: Proc. of the 2003 Network and Distributed System Security Symp. San Diego, 2003.

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

[7] Lepinski M, Sriram K. BGPSEC protocol specification. RFC 8205, 2017. [doi: 10.17487/RFC8205]

[8] Gill P, Schapira M, Goldberg S. A survey of interdomain routing policies. ACM SIGCOMM Computer Communication Review, 2014, 44(1): 28–34. [doi: 10.1145/2567561.2567566]

[9] Gao LX, Rexford J. Stable Internet routing without global coordination. IEEE/ACM Trans. on Networking, 2001, 9(6): 681–692. [doi: 10.1109/90.974523]

[10] Griffin TG, Shepherd FB, Wilfong G. The stable paths problem and interdomain routing. IEEE/ACM Trans. on Networking, 2002, 10(2): 232–243. [doi: 10.1109/90.993304]

[11] Huston G. Interconnection, peering and settlements: Part I. Internet Protocol Journal (Cisco), 1999, 2(1). 1–29.

[12] Huston G. Interconnection, peering and settlements: Part II. Internet Protocol Journal (Cisco), 1999, 2(2): 1–29.

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

[14] Catchpoint. BGP leak highlights the fragility of the Internet with real consequences. 2019. https://blog.catchpoint.com/2019/06/26/bgp-

leak-internet-fragility/

[15] Goldberg S, Schapira M, Hummon P, Rexford J. How secure are secure interdomain routing protocols. ACM SIGCOMM Computer Communication Review, 2010, 40(4): 87–98. [doi: 10.1145/1851275.1851195]

[16] Alaettinoglu C, Villamizar C, Gerich E, Kessens D, Meyer D, Bates T, Karrenberg D, Terpstra M. Routing policy specification language (RPSL). RFC 2622, 1999.

[17] Donnet B, Bonaventure O. On BGP communities. ACM SIGCOMM Computer Communication Review, 2008, 38(2): 55–59. [doi: 10.1145/1355734.1355743]

[18] Siddiqui MS, Montero D, Serral-Gracià R, Yannuzzi M. Self-reliant detection of route leaks in inter-domain routing. Computer Networks, 2015, 82: 135–155. [doi: 10.1016/j.comnet.2015.02.029]

[19] Li S, Duan HX, Wang ZL, Li X. Route leaks identification by detecting routing loops. In: Proc. of the 11th Int'l Conf. on Security and Privacy in Communication Systems. Dallas: Springer, 2015. 313–329. [doi: 10.1007/978-3-319-28865-9_17]

[20] Sundaresan S, Lychev R, Vytautas V. Preventing attacks on BGP policies: One bit is enough. Technical Report, Georgia: Institute of Technology, 2011.

[21] Sriram K, Montgomery D. Enhancement to BGPSEC for protection against route leaks. 2014. https://datatracker.ietf.org/doc/html/draft-sriram-route-leak-protection

[22] Zhao MC, Zhou WC, Gurney AJT, Haeberlen A, Sherr M, Loo BT. Private and verifiable interdomain routing decisions. In: Proc. of the ACM SIGCOMM 2012 Conf. on Applications, Technologies, Architectures, and Protocols for Computer Communication. Helsinki: ACM, 2012. 383–394. [doi: 10.1145/2342356.2342434]

[23] Li J, Stein J, Zhang MW, Maennel O. An expectation-based approach to policy-based security of the border gateway protocol. In: Proc. of the 2016 IEEE Conf. on Computer Communications Workshops (INFOCOM WKSHPS). San Francisco: IEEE, 2016. 340–345. [doi: 10.1109/INFCOMW.2016.7562098]

[24] 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 with English abstract). http://www.jos.org.cn/1000-9825/5867.htm [doi: 10.13328/j.cnki.jos.005867]

[25] Chen D, Ba Y, Qiu H, Zhu JH, Wang QX. ISRchain: Achieving efficient interdomain secure routing with blockchain. Computers & Electrical Engineering, 2020, 83: 106584. [doi: 10.1016/J.COMPELECENG.2020.106584]

[26] Liu YP, Zhang S, Zhu HJ, Wan PJ, Gao LX, Zhang YX, Tian ZH. A novel routing verification approach based on blockchain for inter-domain routing in smart metropolitan area networks. Journal of Parallel and Distributed Computing, 2020, 142: 77–89. [doi: 10.1016/j.jpdc.2020.04.005]

[27] Galmés MF, Aumatell RC, Cabellos-Aparicio A, Ren SS, Wei XP, Liu BY. Preventing route leaks using a decentralized approach: An experimental evaluation. In: Proc. of the 28th IEEE Int'l Conf. on Network Protocols (ICNP). Madrid: IEEE, 2020. 1–6. [doi: 10.1109/ICNP49622.2020.9259367]

[28] Sriram K, McPherson D, Montgomery D, Osterweil E, Dickson B. Problem definition and classification of BGP route leaks. RFC 7908, 2016.

[29] Flach T, Katz-Bassett E, Govindan R. Quantifying violations of destination-based forwarding on the Internet. In: Proc. of the 2012 Internet Measurement Conf. Boston: ACM, 2012. 265–272. [doi: 10.1145/2398776.2398804]

[30] Giotsas V, Zhou S. Valley-free violation in Internet routing—Analysis based on BGP community data. In: Proc. of the 2012 IEEE Int'l Conf. on Communications. Ottawa: IEEE, 2012. 1193–1197. [doi: 10.1109/ICC.2012.6363987]

[31] Chandra R, Traina P, Li T. BGP communities attribute. RFC 1997, 1996.

[32] Sangli S, Tappan D, Rekhter Y. BGP extended communities attribute. RFC 4360, 2006.

[33] Heitz J, Snijders J, Patel K, Bagdonas I, Hilliard N. BGP large communities attribute. RFC 8092, 2017.

[34] Huston G. BGP in 2020—BGP update churn. 2021. https://blog.apnic.net/2021/01/06/bgp-in-2020-bgp-update-churn/

[35] BGPmon. A BGP leak made in Canada. 2012. https://bgpmon.net/a-bgp-leak-made-in-canada/

[36] Huston G. BGP in 2020—The BGP table. 2021. https://blog.apnic.net/2021/01/05/bgp-in-2020-the-bgp-table/

[37] Zhang A, Bai XY. Survey of research and practices on blockchain privacy protection. Ruan Jian Xue Bao/Journal of Software, 2020, 31(5): 1406−1434 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5967.htm [doi: 10.13328/j.cnki.jos.005967]

附中文参考文献:

[24] 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 [doi: 10.13328/j.cnki.jos.005867]
[37] 张奥, 白晓颖. 区块链隐私保护研究与实践综述. 软件学报, 2020, 31(5): 1406−1434. http://www.jos.org.cn/1000-9825/5967.htm [doi: 10.13328/j.cnki.jos.005967]

陈迪(1992－), 女, 博士, 讲师, 主要研究领域为域间路由系统安全, 区块链技术与应用.

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

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

樊松委(1997－), 男, 硕士生, 主要研究领域为区块链技术, 域间路由安全.

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.