专题：内生安全

资源公钥基础设施 RPKI：现状与问题

苏莹莹[1]，李丹[1,2]，叶洪琳[1]

（1. 清华大学，北京 100084；2. 清华大学深圳国际研究生院，广东 深圳 518055）

摘　要：BGP（border gateway protocol，边界网关协议）在设计之初并没有充分考虑安全问题，随着互联网规模的日益壮大，其安全风险也暴露得愈加明显。学术界和工业界提出了诸多方案解决域间路由面临的安全问题，目前真正得以部署的是 IETF（the Internet Engineering Task Force，互联网工程任务组）推动的资源公钥基础设施（resource public key infrastructure，RPKI）。综述了 RPKI 的技术现状和研究进展，重点分析了 RPKI 存在的问题、现有的解决方案以及不足之处，介绍了 RPKI 功能扩展的相关研究，最后指出了未来有潜力的研究方向。

关键词：RPKI；BGP；域间路由；前缀劫持

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000−0801.2021050

Resource public key infrastructure RPKI: status and problems

SU Yingying[1], LI Dan[1,2], YE Honglin[1]

1. Tsinghua University, Beijing 100084, China

2. Tsinghua Shenzhen International Graduate School, Shenzhen 518055, China

Abstract: The BGP (border gateway protocol) did not fully consider security issues at the beginning of its design. With the rapid growth of the Internet, its security risks have become incrementally obvious. Academia and industry have proposed many solutions to the security issues faced by inter-domain routing, and what is really deployed is the RPKI (resource public key infrastructure) promoted by the IETF (the Internet Engineering Task Force). The development status and research advances of RPKI were surveyed, with emphasis on problems of RPKI, existing solutions, and related limitations. Moreover, latest achievements on RPKI function extension were introduced. Finally, future research directions were concluded.

Key words: RPKI, BGP, interdomain routing, prefix hijacking

收稿日期：2021−02−01；**修回日期**：2021−03−15

基金项目：国家重点研发计划项目（No.2018YFB1800100）；广东省重点领域研发计划项目（No.2018B010113001）；国家自然科学基金资助项目（No.61772305, No.61672499）

Foundation Items: The National Key Research and Development Program of China (No. 2018YFB1800100), Guangdong Provincial Research and Development Program (No.2018B010113001), The National Natural Science Foundation of China (No.61772305, No.61672499)

1 引言

BGP 是支持网络之间互联互通的标准协议，作为域间路由至关重要的协议，其对互联网的安全性有着重大影响。但 BGP 在设计之初并没有充分考虑安全性，AS（autonomous system，自治系统）缺乏对路由通告（BGP 宣告）内容真实性的验证，使得 BGP 很容易受网络管理员错误参数配置或恶意攻击行为的影响。

目前 BGP 最严重的一个安全威胁是 BGP 前缀劫持[1]。由于误配置或恶意行为，AS 对外宣告了不属于自己的 IP 地址前缀，从而将发往该 IP 地址前缀的一部分（或全部）流量吸引过来（前缀/子前缀劫持）或充当中继节点窃听流量（中间人劫持）[2]。

BGP 前缀劫持事件每天都在发生，一些大规模的劫持事件更是对网络造成了不可逆转的影响[3-4]。针对 BGP 前缀劫持问题，较为早期的解决方案是 1997 年 BBN 公司提出的 S-BGP[5]，S-BGP 通过在 BGP 宣告中附加 AS 的签名来验证 IP 地址前缀和自治系统号（autonomous system number，ASN）的绑定关系。但由于 S-BGP 存在密钥管理复杂、计算开销大等缺陷，并没有得以部署。RPKI 沿用了 S-BGP 通过签名将 IP 地址前缀和 ASN 绑定的思想，但为了不修改 BGP 以及尽可能降低边界路由器的开销，RPKI 并没有在 BGP 宣告中附加签名，而是将签名以一种带外的方式独立存储于分布式 RPKI 资料库中，由专门的服务器获取并验证签名证书，路由器获取验证后的结果指导路由选择。与 BGP 兼容、带外的设计理念是 RPKI 能够得以部署的重要原因。

IETF 自 2012 年起对 RPKI 进行标准化[6]，并在之后对与 RPKI 相关的概念及标准不断进行更新和完善。RPKI 通过提供 IP 地址前缀和 ASN 之间的可信映射来防止源前缀劫持和源子前缀劫持。其将 BGP 宣告的“默认接受”模式更改为“默认拒绝”模式，只有被 RPKI 判定为真实有效的路由宣告才会被 AS 接受。在 IANA 以及五大 RIR 的不断推动下，目前 RPKI 已初具部署规模。近两年，RPKI 部署率增长相对较快，多个大型 AS 也公开宣布正在部署 RPKI 并将丢弃被 RPKI 判断为无效的 BGP 宣告[7]。

2 RPKI 技术现状

2.1 RPKI 起源及发展

BGP 前缀劫持可以分为前缀劫持和子前缀劫持。前缀劫持如图 1(a)所示，源 AS1 向外发出了带有自身前缀 1.1.0.0/16 的 BGP 宣告，由于 AS5 的误配置或攻击行为，它也向外发出了带有前缀 1.1.0.0/16 的 BGP 宣告。AS 一般会优先选取到达某个前缀 AS_path 最短的 BGP 宣告，因此 AS4 发往 1.1.0.0/16 的流量大概率会发往 AS5，AS3 会综合其他策略选择到达前缀 1.1.0.0/16 的路径。子前缀劫持如图 1(b)所示，AS5 向外发出了相比于 1.1.0.0/16 更加具体的 BGP 宣告（带有前缀 1.1.0.0/24），根据 BGP 的最长前缀匹配原则，AS2、AS3 以及 AS4 到达 1.1.0.0/24 的流量都将会发往 AS5。

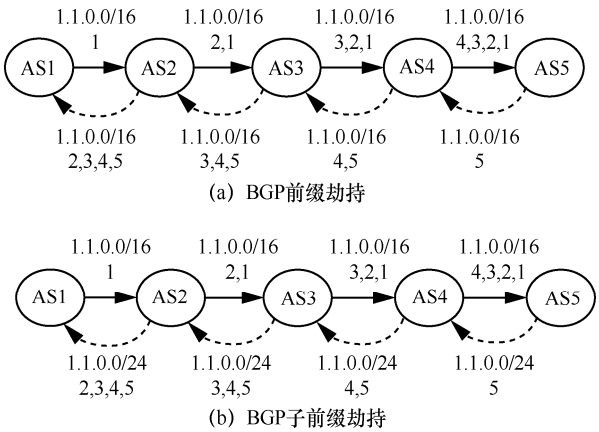

图 1 BGP 前缀劫持及子前缀劫持示意图

为了解决前缀劫持问题，BBN 公司（即 BBN Technology）早在 1997 年就提出安全边界网关协

议（secure BGP，S-BGP）[5]方案。发展至今，前缀劫持问题解决思路主要可分为两大类：异常检测与预防。

异常检测通过对异常 BGP 宣告的识别，让网络管理员快速修复异常情况，从而尽可能降低前缀劫持造成的危害[8-18]，检测的准确性和实时性是这类方案的关键。前缀劫持预防通过丢弃验证失败的 BGP 宣告来达到预防前缀劫持的目的，是一类从根本上解决 BGP 前缀劫持的方案。具有代表性的方案有 S-BGP[5]以及在 S-BGP 基础上发展来的 SPV（secure path vector，安全路径向量）[19]、APA（aggregated path authentication，聚合路径验证）[20]、soBGP（secure origin BGP，安全源边界网关协议）[21]及 psBGP（pretty secure BGP，非常安全的边界网关协议）[22]等。S-BGP 通过两个 PKI（public key infrastructure，公钥基础设施）体系对 BGP 宣告的源伪造及路径伪造进行检测[5]。对于一个 AS 内部的边界路由器来说，每收到一个 BGP 宣告，都要确认这个 BGP 宣告中 AS_path 上的每个 AS 都被授权向外广播了这条 BGP 宣告。S-BGP 存在计算、存储开销较大、密钥管理复杂等缺点，使边界路由器负担过重，难以部署。

针对 S-BGP 密钥管理复杂的缺点，SPV[19]和 APA[20]通过对密码技术进行改进，降低了 S-BGP 的开销；针对 S-BGP 的计算、存储开销大的缺点，2003 年思科公司提出了 soBGP[21]，soBGP 采用信任网络（Web of trust）的分布式信任模型，牺牲了一定的安全性来提高 S-BGP 的性能；psBGP[22]结合了 S-BGP 和 soBGP 的特点，利用信任网络实现 AS 之间的互相背书，进一步降低了验证开销，但同样没有在实际中得到部署；其他的一些改进方案[23-25]根据 BGP 宣告的特点有针对性地降低 S-BGP 的开销。

由于上述方案对 BGP 有所修改，难以推动部署，之后又提出了不修改 BGP 的安全外包机制。主要有 IRV（interdomain routing validation，域间路由验证）[26]和 ROVER（route origin verification，路由源认证）[27]。IRV 通过向源 AS 询问来实现路由源验证，与源 AS 的通信开销以及网络不可达是 IRV 面临的主要挑战；ROVER 利用 DNS（domain name system，域名系统）反向查询机制对源 AS 进行验证，但 ROVER 依赖 DNSSEC（DNS security，域名系统安全）的部署，而 DNSSEC 本身的部署情况也不理想[28]，因此 ROVER 的部署也受到了较大的阻碍。

2012 年 IETF 安全域间路由（Secure Inter-Domain Routing，SIDR）工作组以 S-BGP 为基础提出资源公钥基础设施（resource public key infrastructure，RPKI），并开始对其进行标准化[25]。RPKI 是一套保障互联网号码资源（IP 地址及自治系统号）安全使用的公钥基础设施。其通过对 X.509 公钥证书进行拓展[29]，完成了公钥及互联网号码资源与资源持有者的绑定和授权。RPKI 通过由上至下逐级颁发资源证书来进行资源授权，最下层资源持有者颁发路由源认证（route origin authorization，ROA）来完成 IP 地址与具体 AS 的绑定。此外，作为一种带外的验证机制，RPKI 证书及签名对象被存放至 RPKI 资料库，供需进行路由源验证（route origin validation，ROV）的实体同步和验证，而后将验证结果下发至路由器，避免了路由器的加密和验证开销。

2.2　RPKI 整体架构

RPKI 体系由 3 部分组成：证书签发体系、证书存储系统以及证书同步验证机制。RPKI 的证书签发体系与互联网号码资源由上至下的分配架构相对应（图 2 左侧）。作为一种带外机制，RPKI 涉及的所有证书都存放至 RPKI 资料库中供依赖方（relying party，RP，即帮助 AS 同步并验证证书的实体）同步（图 2 中间部分），RP 同步并验证 RPKI 证书和签名对象，而后将验证结果（IP 地址前缀和 ASN 的绑定关系）下放至 AS 边界路由器指导路由过滤（图 2

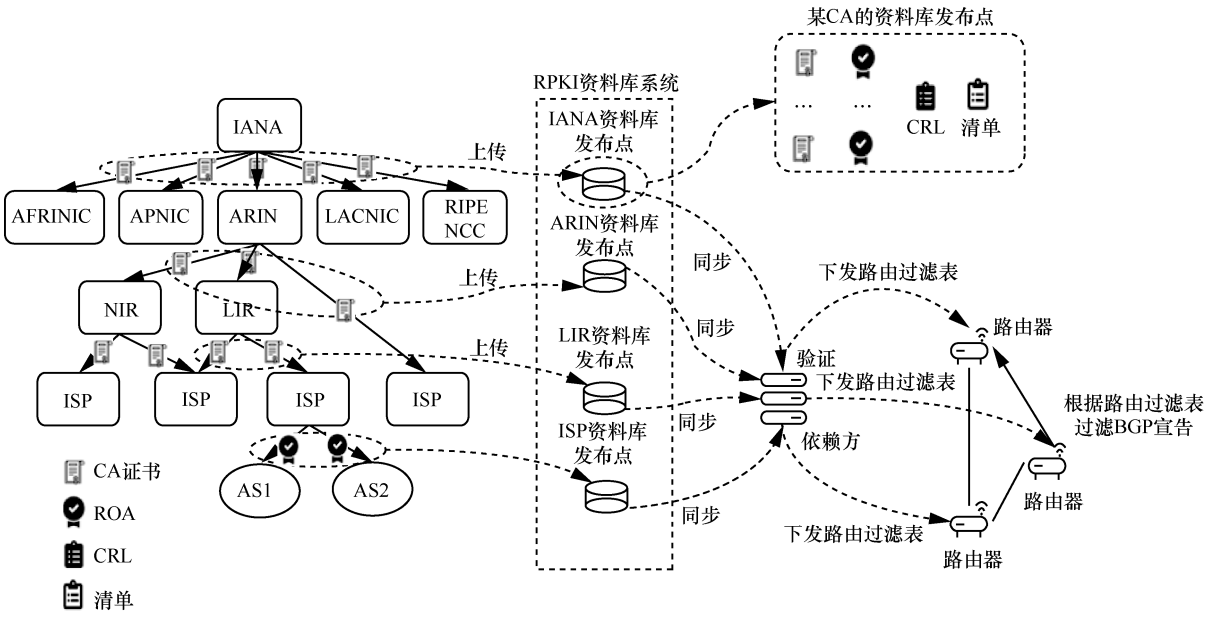

图 2　RPKI 整体架构及运行机制示意图

右侧部分）。

RPKI 利用 X.509 证书及其扩展[29]实现了互联网号码资源使用授权[25]。如图 2 所示，互联网号码分配机构（如五大 RIR）在给互联网号码资源持有者分配资源时，会用自己的私钥签发数字证书（certification authority，CA 证书），证书中包括资源持有者的公钥及相应的互联网号码资源，表明该资源持有者得到了使用此部分号码资源的合法授权[30-31]。证书生成后，上层分配机构会将签发的证书存放于自己的资料库发布点（RPKI 资料库）供 RP 同步。当资源拥有者希望授权某个 AS 宣告自己拥有的 IP 地址前缀时，会先用自己的私钥签发一个终端实体（end-entity，EE）证书，而后用 EE 证书的私钥签发 ROA[32]，完成 IP 地址前缀和此 AS 的绑定。为了减轻撤销证书的负担，EE 证书和 ROA 是一一对应的，RPKI 规定将 EE 证书作为 ROA 的一个字段进行存储[25, 33]，资源拥有者可通过撤销 EE 证书来撤销 ROA。

拥有 CA 证书的实体称为 CA，每个 CA 都会维护一个资料库发布点[34]供 RP 同步自己发布的证书和签名对象，RPKI 资料库系统就是由所有 CA 的资料库发布点共同组成的。RPKI 使用 CA 证书的两个扩展项来链接整个 RPKI 分布式资料库系统：信息发布点（subject information authority，SIA）和权威发布点（authority information authority，AIA）。SIA 记录了该 CA 自身资料库发布点的地址，可通过此字段查找到该 CA 签发的所有证书和签名对象；AIA 记录了该 CA 的父 CA 资料库发布点的地址，可通过此字段查找到该 CA 的上层 CA 发布的所有证书和签名对象。利用 CA 证书中的这两个信息，理论上可以通过 RPKI 证书树中的任意一个 CA 证书链接到整个 RPKI 证书树。

传统 PKI 在撤销证书的时候，需要证书撤销列表（certificate revocation list，CRL）记录还未过期但是已被撤销的证书[30]。RPKI 在撤销证书的时候沿用了此机制，每个 CA 的资料库发布点中都会维护一个 CRL 用来记录该资料库发布点中还未过期但已被撤销的证书的序列号及撤销日期[31]。为了保证 CRL 不被篡改，CRL 也需要对应的 CA 用自己的私钥进行签名。

为了方便 RP 检查同步到的某个资料库发布

点中证书和签名对象的正确性以及完整性，防止在传输的过程中资料库发布点中的内容被恶意删除或篡改，每个资料库发布点还需要维护一个清单[35]。清单记录了该资料库发布点中所有合法（未过期也未被撤销）的证书及签名对象的名称及哈希值。RP 在同步完资料库中的资料后，会根据清单的内容进行证书正确性和完整性验证。同 ROA 一样，清单作为 RPKI 的签名对象，也需要与 EE 证书进行绑定，在撤销清单的时候只需要撤销对应的 EE 证书即可。

2.3　路由源验证过程

RP 通过 rsync[36]协议或 RRDP（RPKI repository delta protocol，RPKI 资料库更新协议）[37]从所有 RPKI 资料库发布点中同步证书和签名对象，而后沿着证书链由上至下验证 ROA 的有效性，并提取所有有效 ROA 中记录的 IP 地址前缀和 ASN 的映射关系生成路由过滤表，通过 RTR 协议[38]将路由过滤表下发至各个边界路由器，路由器利用该路由过滤表来验证收到的 BGP 宣告的有效性。

ROA 中除了 IP 地址前缀和 ASN 的对应关系外，还有一个最长前缀长度（maxlength）字段。每个 ROA 中的有效条目都可以表示为三元组<ASN，IP prefix，maxlength>[25,32]。如三元组<AS 1688, 100.20.0.0/16, 24>表示 IP 地址前缀 100.20.0.0/16 可由 AS 1688 合法宣告，其能宣告的最长前缀长度是 24，即 100.20.0.0/16~100.20.255.0/24 之间的前缀都可由 AS 1688 合法宣告，在此范围外才会被判断为非法。

路由器在收到 RP 下发的所有有效 ROA 条目集合后，就可以利用该集合对收到的 BGP 宣告进行路由源验证（route origin validation，ROV）[39]，从而过滤掉验证非法的 BGP 宣告。

一条 BGP 宣告的“源路由”定义如下：如果一条 AS_path 的最后一个元素是 AS_sequence 类型，那么源 AS 就是 AS_path 的最后一个元素；如果 AS_path 中的最后一个元素（或元素段）是 AS_set 类型，表明无法确定 ASN 的先后顺序，也就无法确定源 AS，此时不做判断。

ROA 与 BGP 宣告的有效性对应关系见表 1[39]。

表 1　ROA 与 BGP 宣告的有效性对应关系

BGP 宣告中的 IP 地址前缀	BGP 宣告与 ROA 的 ASN 匹配	BGP 宣告与 ROA 的 ASN 不匹配
与 ROA 无交叉	未知	未知
可以覆盖 ROA 中的 IP 地址前缀	未知	未知
与 ROA 中的 IP 地址前缀相匹配	有效	无效
比 ROA 中的 IP 地址前缀更具体	无效	无效

路由器利用 RP 下放的有效 ROA 条目进行 ROV 的具体过程如下。

步骤 1　选取满足 $IP_{BGP} \subseteq IP_{ROA}$（BGP 宣告中 IP 地址前缀覆盖的 IP 地址是 ROA 中 IP 地址前缀覆盖的 IP 地址的子集）的 ROA，构成“候选 ROA”的集合（即满足表 1 中“与 ROA 中的 IP 地址前缀相匹配”或“比 ROA 中的 IP 地址前缀更具体”的所有 ROA）。

步骤 2　如果“候选 ROA”集合为空，那么判断结束，返回“unknown”（未知）。

步骤 3　如果要判断的 BGP 宣告的源 AS 可以确定（AS_path 的最后一个元素是 AS_sequence 类型），且“候选 ROA”集合中存在一个 ROA 的 ASN 字段与源 AS 相同（即满足表 1 中“BGP 宣告与 ROA 的 ASN 匹配”），且该 BGP 宣告的 IP 地址前缀长度不大于 ROA 中的 maxlength 值（即满足表 1 中“与 ROA 中的 IP 地址前缀相匹配”），则判断结束，返回“valid”（有效）。

步骤 4　否则返回“invalid”（无效）。

边界路由器参考 ROV 的结果决定是否接受某条 BGP 宣告，IETF 建议边界路由器优先考虑被判断为 valid 的 BGP 宣告，尽量丢弃被判断为

invalid 的 BGP 宣告[25,39]。

2.4 本地化互联网号码资源管理策略

RPKI 的资源授权是基于全局视角的，它使资源持有者可以对拥有的全局唯一的资源进行可验证的声明。但是，网络管理员也有需求在某些本地化的场景中声明对某些资源的持有情况，比如在本地化场景中声明对 RFC1918[40]规定的某些保留地址的使用权。或者国家出于某些原因需要指导国家内部的网络按照国家权威机构的指示配置域间路由过滤规则。这些本地化的策略，只在本地上下文中生效，不会对超出本地范围内的其他网络的配置产生任何影响。

考虑到以上 ISP 本地化信息控制的需求，Ma 等人[41]在 RFC8416 中提出了简化本地互联网资源管理（simplified local internet resource management，SLURM）。SLURM 提供了一种简单的使 RP 能够对 RPKI 全局资料库的验证结果进行“重写”的机制。如图 3 所示，RP 在验证本地缓存的 RPKI 资料库证书后获取“全局策略”，之后再通过 SLURM 机制添加“本地策略”（“本地策略”与“全局策略”产生冲突时，服从“本地策略”），而后将“综合策略”下放至边界路由器，指导其进行 BGP 宣告过滤。

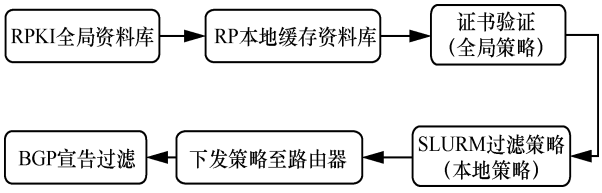

图 3 SLURM 机制示意图

SLURM 采用单个 JSON 文件来导入本地策略。图 4 是 SLURM 文件的格式展示：slurmVersion 字段是 SLURM 的版本号；validationOutputFilters 字段包含需要被过滤掉的与前缀相关条目（prefixFilters）及与 BGPsec 相关条目（bgpsecFilters），所有验证通过的 ROA 条目只要被此字段包含，就必须从 RP 输出给路由器的合法条目中剔除；locallyAdded Assertions 字段表示需要添加的与前缀相关条目（prefixAssertions）及与 BGPsec（bgpsecAssertions）相关的条目，所有验证通过的 ROA 条目只要不包含此字段的内容，RP 输出给路由器的合法条目中必须再额外将此条目的内容添加进来。SLURM 文件的操作是“原子性”的，RP 要么采用 SLURM 文件列出的全部内容，要么完全不采用此 SLURM 文件的策略。当存在多个 SLURM 文件时，RP 需要检查这些文件是否存在冲突，如果存在冲突，RP 需将冲突内容报告给 SLURM 文件的创建者，冲突解决后才能采用这些 SLURM 文件。

```
{
  “slurmVersion”: 1,
  “validationOutputFilters”:{
      “prefixFilters”: [],
      “bgpsecFilters”:[]
  }
  “locallyAddedAssertions”:{
      “prefixAssertions”:[],
      “bgpsecAssertions”:[]
  }
}
```

图 4 SLURM 文件格式

SLURM 给 RP 提供了自由配置自己本地 BGP 宣告过滤策略的机制，且该策略不会影响到除本地之外的其他网络，但是 RP 也需仔细考虑使用 SLURM 所带来的安全隐患，尤其需要关注 SLURM 文件是否存在配置错误或此文件是否由第三方所提供。

2.5 RPKI 部署情况

自 2012 年 RPKI 被标准化以来，IANA 和五大 RIR 就在不断推动 RPKI 的部署，利用 RIPE NCC 维护的 RPKI 历史资料库[42]，对 RPKI 的部署情况进行了分析。

2.5.1 部署 RPKI 的 AS 数量及比例变化

五大 RIR 部署 RPKI 的 AS 增长趋势如图 5 所示，图 5 展示了自 2015 年至 2020 年，每年的

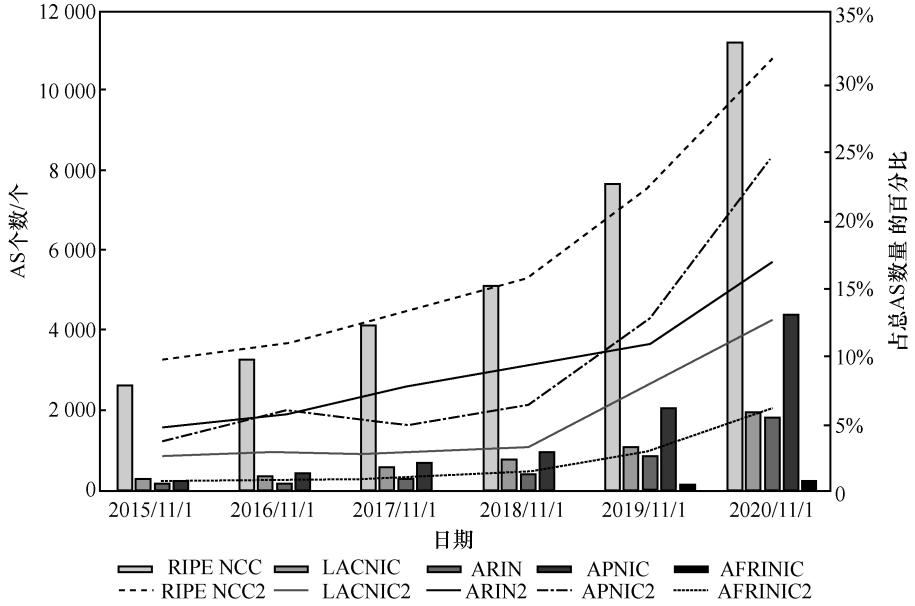

图 5　五大 RIR 部署 RPKI 的 AS 增长趋势

11 月 1 日，部署了 RPKI 的 AS 数量及比例的变化。图 5 中的柱状图表示在五大 RIR 中，部署了 RPKI 的 AS 数量上的变化；折线图表示部署了 RPKI 的 AS 占在本 RIR 注册的所有 AS 在百分比上的变化。从图 5 可以看出，从 2015 年开始，五大 RIR 的 AS 部署 RPKI 的数量和比例都呈上升趋势。2015—2017 年增长趋势较为平缓，在 2018 年及以后，增长逐渐加快，其中 RIPE NCC 的变化趋势最为明显，且部署的数量和比例在 5 个 RIR 中都是最高的，到了 2020 年 11 月 1 日，部署 RPKI 的 AS 比例更是超过了 30%。

2.5.2　被 ROA 覆盖的 BGP 前缀比例变化

ROA 覆盖的 BGP 宣告中的 IP 地址前缀的比例也是衡量 RPKI 部署情况的一个重要指标。使用了 Routeviews[43]观测点所维护的 RIB 表数据，截至 2020 年 11 月 1 日，Routeviews 共有 26 个观测点，但是由于在 2015—2020 年时间段内，观测点的数量有所变化，为了更加真实地反映被 ROA 覆盖的 BGP 宣告中的 IP 地址前缀的变化趋势，本文选取了 Routeviews 中一个较大的观测点所维护的 RIB 表进行分析。图 6 是从 2015—2020 年，被 ROA 覆盖的 BGP 宣告（IPv4 前缀及 IPv6 前缀）的变化趋势。从图 6 可以看出，2015—2017 年，BGP 宣告中的前缀被 ROA 覆盖的比例不到 0.1，但 2018 年以后，BGP 宣告中的前缀被 ROA 覆盖的比例逐渐上升。这与图 5 中 2018 年后部署 RPKI 的 AS 数量增长变快相符。但从图 6 也可以发现，截至 2020 年 11 月 1 日，在所有 BGP 宣告的 IP 地址前缀中，被 ROA 覆盖的比例仍不到 0.25，因此距离 RPKI 的全面部署仍有较大距离。

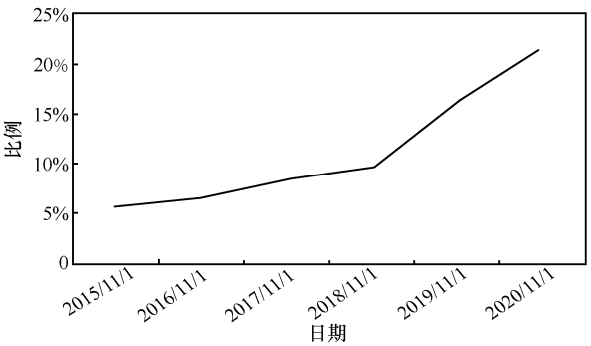

图 6　BGP 宣告的前缀被 ROA 覆盖的比例

3　RPKI 存在的问题及研究进展

3.1　RPKI 可扩展性问题

作为一种带外机制，RPKI 不利用 BGP 传输

证书内容，而是建立“资料库”来存储证书，供RP下载使用。目前网络中大约有65 000个活跃的AS，如果所有的AS都使用RPKI进行路由源验证，且假设一个RP服务一个AS，那么每一个RPKI资料库发布点的服务器都需要满足65 000个RP同时同步资料的需求。

RPKI设计之初采用的同步协议是rsync[36]。rsync使用了增量同步机制，有效地避免了大量数据的传输，但rsync要求资料库发布点服务器为每一个有同步资料需求的RP计算其距上次同步需要增量同步的内容，如果65 000个RP同时同步，RPKI资料库服务器需要消耗大量的内存和CPU资源，这对服务器提出了较高的要求。对于一些ISP来说，部署一个7×24 h在线，并且能同时支持65 000个RP频繁地进行同步的RPKI资料库发布点，其开销可能是无法承受的[44]。

为了解决这个问题，IETF提出了一个新的同步协议——RRDP[37]，其实现了增量同步，且极大地降低了资料库发布点服务器的开销。RRDP让资料库发布点服务器维护一个更新文件，资料库发布点中的所有的更新操作（如更新了清单和CRL、发布了新的证书或ROA等）及更新的时间戳都被记录在此文件中，RP只需要同步更新文件，根据更新文件中的更新内容及时间戳去增量同步指定的对象即可。RRDP同时结合了Web缓存机制，能够极大地缓解rsync带来的可扩展性问题。但是目前RPKI并没有实现完全部署，RRDP是否能够完全满足同步的性能要求还有待考证。

RPKI部署的早期，为了简化CA的资料库管理负担，推动部署，五大RIR为下属的NIR/ISP提供了“托管模式”服务。NIR/ISP只需要在RIR提供的网页上进行注册，就可以将自己的资料库发布点完全托管给RIR。NIR/ISP不再维护自己的资料库发布点，降低了自己的管理开销，也更有动力去部署RPKI。但“托管模式”要求NIR/ISP将自己的密钥和资料库管理权都上交给RIR，这导致RIR可以随意修改NIR/ISP资料库发布点中的内容，为RIR的主动恶意行为或被迫恶意行为提供了便利。目前，大多数部署了RPKI的机构都选择了“托管模式”，只有极少数的ISP选择亲自管理自身的资料库发布点。

3.2 RPKI资料库对象相关恶意操作

RP通过获取并验证RPKI资料库所有的资源证书及签名对象（统称为资料库对象）来生成路由源验证条目，因此任何针对RPKI资料库对象的误操作或恶意操作都会影响验证结果，从而影响BGP宣告过滤规则的准确性。关于对象的恶意操作主要分为以下几类[45]。

- 删除：任何有权限操控资料库发布点的实体恶意删除资料库发布点中的对象（CA证书、ROA、CRL、清单），使RP无法同步这部分证书。
- 抑制：任何有权限操控资料库发布点的实体恶意抑制CA对其资料库所进行的更新，使RP无法同步到CA进行的更新。
- 损坏：任何有权限操控资料库发布点的实体损坏资料库发布点中的对象（CA证书、ROA、CRL、清单），使证书内容无法解析验证。
- 篡改：掌握资料库发布点对应的CA证书私钥的实体任意篡改资料库发布点中的对象（CA证书、ROA、CRL、清单）。
- 撤销：掌握资料库发布点对应的CA证书私钥的实体恶意将CA证书、ROA和清单列入CRL列表，使其验证失败。
- 注入：掌握资料库发布点对应的CA证书私钥的实体任意使用其私钥发布没有经过此CA同意的证书或签名对象。

上述6种恶意操作的前两种，只要有资料库发布点的操作权限即可进行，后3种需要掌握资料库发布点对应的CA证书的私钥。需要注意的是，上层CA可以通过删除、篡改、撤销自己给下层CA颁发的CA证书来影响下层CA资料库中

对象的有效性。目前，RPKI 的资料库主要采用的是托管模式（hosted model），CA 将自己的资料库和私钥交给五大 RIR 统一管理，仅少数的 ISP 采用自主管理资料库及私钥的模式（delegated model）。本文将自身资料库发布点中的证书或自身的 CA 证书受到破坏的 CA 称为受害 CA，对受害 CA 产生影响的两个主要来源有受害 CA 的上层 CA 以及外界攻击者。表 2 列出了在两种资料库发布点管理模式下，两个威胁源分别可以对受害 CA 的 CA 证书及其资料库发布点的对象进行的恶意操作。

表 2　在不同管理模式下可进行的恶意操作

对比项	自主管理模式	托管模式
受害 CA 的上层 CA	通过删除、篡改、撤销发布的 CA 证书来影响受害 CA	所有资料库及资料库对应的私钥都由五大 RIR 掌管，可进行针对证书的任意恶意操作
外界攻击者	攻破了受害 CA 的资料库：删除、损坏证书和签名对象	攻破了受害 CA 的资料库：删除、损坏证书和签名对象
	攻破了受害 CA 的资料库及私钥：可进行针对证书的任意恶意操作	攻破了受害 CA 的资料库及私钥：可进行针对证书的任意恶意操作

由于资料库发布点中的对象有多种类型（CA 证书、ROA、CRL、清单），对每种对象采取上述 5 种不同的操作产生的不良影响也是不一样的。这里仅介绍几种危害较为严重的恶意操作，更多关于证书的恶意操作可参考 RFC 8211[45]。

上层 CA 恶意撤销、删除下层 CA 的 CA 证书：由于下层 CA 的 CA 证书存放在上层 CA 的资料库发布点中，上层 CA 可直接删除下层受害 CA 的 CA 证书（无须修改 CRL 列表）或撤销下层受害 CA 的 CA 证书（需将下层 CA 的 CA 证书放至 CRL 列表）。两者产生的效果是相似的，RP 无法再同步到下层受害 CA 的 CA 证书，无法定位受害 CA 的资料库发布点，进而导致受害 CA 资料库中的所有对象都不能被同步到。不同的是，删除 CA 证书的情况下，RP 还会继续使用之前缓存的受害 CA 的 CA 证书及其资料库发布点中的对象，直到 CA 证书和资料库中的对象过期；而撤销 CA 证书会导致所有受害 CA 签发的对象都验证失败。

上层 CA 恶意篡改下层 CA 的 CA 证书：与撤销、删除下层受害 CA 的 CA 证书不同，篡改证书一般是更改原 CA 证书的资源授权情况，比如减少对下层 CA 授权的 IP 地址资源或 ASN 资源（一般不会增加对下层 CA 的授权资源），导致下层 CA 签发的与减少的那部分资源相关的 ROA 验证失败，进而影响相关 AS 的 BGP 宣告的有效性。

目前，防止上层 CA 单方撤销下层 CA 的 CA 证书的方案有两种，第一种是改进 RPKI 机制，使其能够平衡上下层 CA 的权利；第二种是设计全新的去中心化互联网基础设施方案。Heilman 等[46]于 2014 年提出的 RPKI 证书透明机制属于第一种。其核心思想是上层 CA 想要撤销下层 CA 的 CA 证书，必须经过所有可能受影响的下层机构的“同意签名”，但是在目前 90%以上的 CA 资料库都由 RIR 托管的模式下，此方案起不到限制作用。第二种方案的典型代表就是基于区块链的去中心化互联网基础设施方案。

2016 年 Hari 等[47]首次在文献中提出了基于区块链的去中心化互联网基础设置方案的基本框架，其核心思想是把 IP 地址的分配与 IP 地址和 ASN 的绑定关系抽象成交易发布到区块链系统中，利用区块链账本的分布式和防篡改特性防止恶意操作，但是文献并没有提出一个完整的解决方案。随后 Alfonso 等[48]提出的 SBTM、Paillisse 等[49]提出的 IPchain、Xing 等[50]提出的 BGPcoin、Angieri 等[51]提出的 InBlock 和 DII[52]、Saad 等[53]提出的 RouteChain 以及 He 等[54]提出的 ROAchain 和 Chen 等[55]提出的 ISRchain 都是基于此思想的去中心化方案。InBlock 强调互联网号码资源在初始时不属于任何一个机构，资源的分配依靠智能合约完成，从根本上避免了互联网号码资源在属于某个实体时（比如 RIR），此实体封锁资源分配的情况；BGPcoin 解决了基于区块链的去中心

化互联网号码资源方案与 BGP 兼容性问题，其对资源分配对应交易的流程设计完整，且基于以太坊搭建了本地仿真网络；ROAchain 指出了之前方案采用基于 PoW 或 PoS 共识机制的不合理性，并设计了一套理论上更加安全有效的共识机制，大大提高了交易速率；ISRchain 将 AS 之间的邻接关系数据和商业关系数据上传至区块链，使系统能同时解决域间路由的路径篡改和路由泄露问题。基于区块链的方案有诸多优势，比如：能有效防止 CA 恶意撤销证书、相比于 RPKI 能保证 RP 获取资源分配数据的一致性、简化证书管理的复杂度等。但是，由于区块链技术尚未完全发展成熟，基于区块链的方案也存在一定的问题，比如交易吞吐量低、智能合约的安全性问题等。但由于区块链去中心化、防篡改、可追溯的特性使得采用区块链技术解决互联网号码资源分配的去中心化问题成为未来的一大趋势。

3.3 最长前缀长度

ROA 中 maxlength 字段使得 ROA 能以单个 IP 地址前缀的形式授权一个 AS 宣告一组合法的子前缀，其优势主要有以下两点：（1）减少 ROA 中 IP 地址前缀条目，书写方便，且减少了 RP 下放给路由器的 IP 地址前缀条目数量；（2）可使网络管理员更加灵活便捷地重新配置其网络，无须更改 ROA 即可灵活地宣告 maxlength 范围内的任意子前缀。但同时，maxlength 也给域间路由引入了新的安全风险。

定义一个 ROA 中授权给某一 AS 的所有 IP 地址前缀（包括 maxlength 内的子前缀）都在此 AS 的 BGP 宣告中出现，则称此 ROA 为“minimal ROA（最小化 ROA）”，否则称其为“loose ROA（松散 ROA）”[56]。比如 maxlength 值设置为/24，但是只有/20 的子前缀出现在了此 AS 的 BGP 宣告中，则此 ROA 为“loose ROA”。参考文献[56]显示 2017 年 RPKI 资料库中 30%的 ROA 都属于“loose ROA”。其主要原因是网络管理员在设置 maxlength 值时一般非常宽松，超过 85%的“loose ROA”的 maxlength 值为 24（IPv4）或 48（IPv6）。但是网络管理员一般不会将 maxlength 包含的所有子前缀都宣告出去，这部分被 ROA 覆盖但是并没有宣告出去的 IP 地址前缀很容易受到伪造源子前缀劫持（forged origin subprefix hijack）。

伪造源子前缀劫持示意图如图 7 所示，AS A 是 IP 地址前缀 1.2.0.0/16 的合法拥有者，其允许宣告的最长前缀长度是 24，但是其仅向 AS B 宣告了/16 位的前缀，显然此 ROA 为“loose ROA”。恶意攻击者 AS 666 通过伪造与 AS A 的邻接关系，向 AS B 宣告了通过路径 666-A 能到达前缀 1.2.0.0/24。由于 AS 666 并没有伪造 IP 地址前缀和源 AS 的对应关系，此宣告并不会被 AS B 判断为非法（invalid）。通过借助 AS A 发布的“loose ROA”以及篡改路径，AS 666 能够吸引到 AS A 没有宣告出去的所有 IP 子前缀的流量。这种攻击手段即被称为伪造源子前缀劫持。

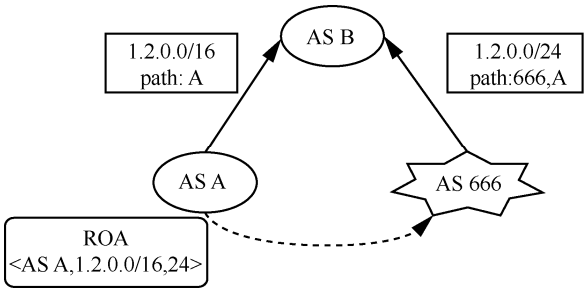

图 7 伪造源子前缀劫持示意图

IETF 草案[57]建议网络管理员尽量将 maxlength 值设置成 IP 地址前缀的原始长度，或尽量把 maxlength 包含的子前缀都宣告出去，从而避免“loose ROA”带来的危害。参考文献[58]指出，弃用 maxlength 并不会导致 ROA 数量的增加（一个 ROA 可包含多个 IP 地址前缀），且在 RPKI 全面部署的情况下，也不会对路由器需要验证的 IP 地址前缀条目数量造成太大影响。已被标准化但尚未被部署的 BGP 安全（BGP security，BGPsec）[59]是基于 RPKI 的防止路径篡

改的方案。BGPsec 的大规模部署能够解决伪造源子前缀劫持问题，但由于其开销极大，推广部署进行得十分缓慢，第 4 节将对 BGPsec 方案进行介绍。

3.4　资源重复分配

RPKI 通过上层机构给下层机构签发 CA 证书来实现资源授权，但是由于上层机构的错误配置或恶意操作等原因，同一个资源可能会被上层机构分配给多个下层机构，造成资源所有权冲突。

目前真实运行的 RPKI 架构存在多个信任锚，包括 IANA 和五大 RIR[25]，它们都拥有一个包含所有 IP 地址资源的自签名根证书，可为下层机构签发带有任意 IP 地址资源的 CA 证书（正常情况下，一个 RIR 只能再分配自己拥有的那部分 IP 地址）。这就会导致潜在的一个 IP 地址前缀（一块 IP 地址）被多个 RIR 同时分配给下层机构，资源的重复分配造成路由冲突。但多个信任锚也存在一定的优势，当一个 RIR 受限于某个国家或者其他外界因素的压力，被迫封锁一块 IP 地址资源时，其他 RIR 依然可以完成这块 IP 地址的再分配。

除了拥有所有 IP 地址资源根证书的五大 RIR 可以造成资源重复分配之外，由于 RPKI 并没有机制从技术上保证同一块 IP 地址不能被分配多次，RPKI 架构中的任意资源持有者理论上都可以重复分配其资源。但除了合法的 MOAS，任何 IP 地址资源都不应该被同时分配给两个机构。因此，资源持有者也应通过验证证书的过程及时发现自己持有的资源是否被上层机构重复分配。

3.5　上下层 CA 依赖

由于 RPKI 的层级化资源授权架构，下层机构签发 ROA 需要上层机构提前签发 CA 证书（向上依赖），上层机构签发的 ROA 也可能会影响下层机构的 BGP 宣告（向下影响）。机构之间签发证书的依赖和签名对象相互影响会对路由源验证造成一定的危害[56]。

向上依赖：RPKI 体系中向上依赖示意图如图 8(a)所示，ISP A 从 RIR 处分得地址 10.1.0.0/16，但是 RIR 并没有给其签发 CA 证书，因此 ISP A 不能通过签发 ROA 对象来保护自己拥有的地址块，同时 ISP A 也不能进一步给下层机构 AS 1 和 AS 2 签发 CA 证书。由于下层机构对上层机构的依赖，导致下层机构部署 RPKI 受到限制（需等上层机构先部署），不利于 RPKI 部署率的增加。

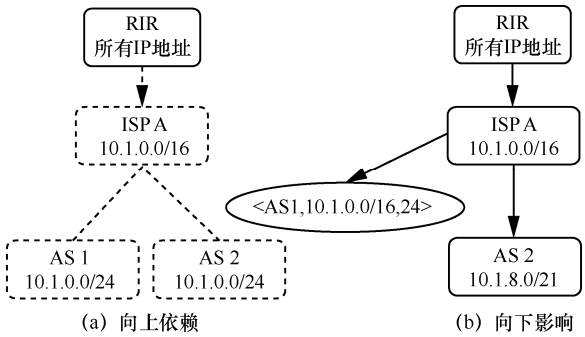

图 8　RPKI 体系上下层依赖示意图

向下影响：RPKI 体系中向下影响示意图如图 8(b)所示，ISP A 从 RIR 处分得地址 10.1.0.0/16，并获取相应的 CA 证书，ISP A 通过签署 ROA 将此地址块与 AS1 绑定。随后 ISP A 将子前缀 10.1.8.0/21 分配给 AS2，但是 AS2 并没有签发 ROA 保护自己拥有的地址块。由于路由源验证的规则（前缀覆盖、maxlength 符合、ASN 不匹配），AS2 的 BGP 宣告会受 ISP A 签发 ROA 的影响被误判为前缀劫持，进而导致 BGP 宣告被其他 AS 拒收。

因此建议下层机构从上层机构分得 IP 地址资源时，尽量要求上层机构为其签发 CA 证书，避免“向上依赖”；上层机构在为拥有的大块 IP 地址签发 ROA 时，尽量帮助或者督促下层机构（分得了子前缀）签发 ROA 保护地址块。参考文献[56]提出了“wildcard ROA”方案缓解“向下影响”，核心思想是在 ROA 中增加一个剔除某些 IP 地址块的字段，使得上层机构在为拥有的 IP 地址块签署 ROA 时，能够将已经分配出去的子前缀剔除掉，从而避免影响下层机构的

BGP 宣告。

4 RPKI 功能扩展

4.1 BGPsec 签名机制

BGPsec[59]是建立在 RPKI 基础上的防止域间路由路径篡改的方案。BGPsec 要求前一个 AS 在向下一跳 AS 传播 BGP 宣告时，附带上自身的签名保证路径的真实性。与 RPKI 不同的是，其并非带外路径验证机制，BGPsec 对 BGP 进行了修改，在 BGP 报文中增加了 BGPsec_path 字段来携带逐跳的路径签名信息。BGPsec 逐跳加密示意图如图 9 所示，ASa 向 ASb 发起原始路由宣告，ASa 在 BGP 宣告的 BGPsec_path 字段加入前缀和路径信息（ap1），并用自己的密钥对 ap1 进行签名；ASb 收到来自 ASa 的宣告后，提取 BGPsec_path 中的签名(sign1)、自身的 ASN 及下一跳的 ASN 组合成 ap2，并对其签名生成 sign2，而后将<ap2, sign2>追加到 BGPsec_path 字段。ASc 在收到 ASb 的 BGP 宣告后，依次使用 ASb 和 ASa 的公钥对 BGPsec_path 字段中的签名进行验证，若验证通过，则此 BGP 宣告不存在路径篡改问题。

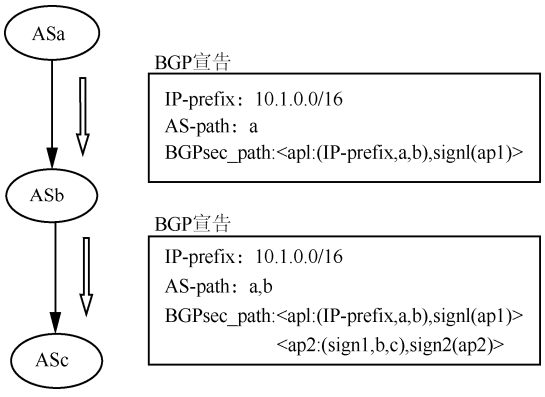

图 9 BGPsec 逐跳加密示意图

BGPsec 通过逐跳签名的机制有效地防止了路径篡改，但是其要求一条路径上的所有 AS 都具备签名和验证的功能，在网络中的 AS 部分部署 BGPsec 的情况下，效果有限（一条路径上的一跳不可验证，则这条路径就无法验证）。同时，BGPsec 面临着协议降级攻击，有些恶意 AS 故意采用旧版本的 BGP（不支持 BGPsec），使得其恶意行为并不能被检测[60]。BGPsec 由于需要边界路由器对每一个 BGP 宣告都验证、签名，无疑给路由器带来了不小的开销。

4.2 ASPA 供应商授权机制

正在 IETF 标准化的草案 AS 供应商授权（autonomous system provider authorization，ASPA）[61]旨在解决如何使 RPKI 支持路由泄露检测的问题。草案建议在 RPKI 资料库中新增一种签名对象 ASPA 表示 AS 之间的客户到提供商（customer to provider，C2P）关系（BGP 宣告层面的 C2P 关系，非具体的商业关系）。ASPA 是由扮演客户角色的 AS 进行签名的签名对象，对于选定的一组 IP 地址簇（address family identifier，AFI），该对象将一组供应商 ASN 与此客户 ASN 绑定。ASPA 签名对象可由三元组<ASa, AFI, [ASb, ...]>表示，ASa 代表客户 AS，[ASb, ...]代表在指定的地址簇（AFI）下与 ASa 具有 C2P 关系的供应商 AS。

RP 可以利用同步到的 ASPA 签名对象验证一条 AS-path 是否存在路由泄露。一条 AS-path 是否存在路由泄露可以通过验证这条 AS-path 上所有相邻的 AS 是否存在路由泄露完成。输入为<ASa，ASb，afi>，其中，ASa 和 ASb 表示这条 AS-path 上的任意两个邻接 AS，afi 是此 BGP 宣告中的 IP 地址前缀。首先 RP 搜索 ASa 签署的所有 AFI 包含 afi 的 ASPA 签名对象，获取这部分 ASPA 签名对象中所有供应商 ASN，生成“备选供应商 ASN”集合。如果此集合为空，则返回“unknown”，表示无法判断；如果 ASb 被包含在此集合中，则返回“valid”，表示验证通过；如果 ASb 没有被包含在此集合中，则返回“invalid”，表示验证失败。通过逐跳判断相邻 AS 是否存在路由泄露可完成整条 AS-path 的判断，具体判断过程可参考草案 ASPA[61]。需要注意，如果一条 AS-path 有一

组相邻的 AS 不能判断，则整条 AS-path 就不能判断，输出结果“unknown”；如果一条 AS-path 有一组相邻的不合法，则输出“invalid”；否则验证通过，输出“valid”。草案建议 AS 抛弃被判断为非法的 BGP 宣告，对于无法判断的 BGP 宣告，则降低其优先级。

ASPA 继承了 RPKI 技术的思想，不改动 BGP，避免给交换机增加额外的开销，是一种带外的验证机制。其支持增量部署，不存在 BGPsec 的“降级攻击”问题。但其不能验证更复杂的传输关系，比如 AS 之间的互相传输关系（mutual transit）。同时，AS 之间的传输关系一般由 AS 之间的商业关系确定，存在间接暴露 AS 之间的商业关系的风险，而商业关系一般被 AS 视为机密，影响 AS 部署的积极性。

5　结束语

作为保障域间路由安全的重要互联网基础设施，RPKI 技术及相关问题越来越受工业界和学术界重视。自 2019 年，RPKI 的部署率得到了极大的改善。但是，RPKI 同样也存在着自身的缺陷，比如可扩展性问题、maxlength 带来的安全风险、潜在的资源重复分配以及上下层 CA 权利不均衡等问题。已有工作提出了诸多解决或缓解方案，但是目前这些方案自身也存在不足，有效性也有待验证，距离被 IETF 采纳尚有距离。且 RPKI 只能预防最简单的前缀劫持或子前缀劫持，并不能预防带有路径篡改和路由泄露的更“高级”的劫持或恶意攻击。因此，改进 RPKI 以及对 RPKI 进行功能扩展是目前研究的焦点。下面对 RPKI 未来的研究重点和发展趋势进行探讨。

（1）去中心化 RPKI

如何平衡 RPKI 架构中上层 CA 与下层 CA 的权利、如何避免资料库中的对象被恶意破坏是研究人员关注的焦点。由于区块链的去中心化、防篡改、可追溯的特性，使其有望解决 RPKI 存在的中心化、可篡改的问题。目前学术界也提出了多种基于区块链的去中心化互联网基础设施方案（参考第 3.2 节），但区块链本身的技术限制以及目前 RPKI 已初具部署规模的事实使得完全基于区块链的方案离真正落地还有距离。将区块链技术或其他防篡改账本技术作为保障 RPKI 去中心化以及防篡改的带外机制，在 RPKI 的基础上设计与 RPKI 兼容的轻量级方案来限制 CA 或者 RIR 恶意颁发、破坏证书的机制有望解决目前完全基于区块链去中心化方案面临的困境。

（2）RPKI 功能扩展

RPKI 目前仅支持简单的前缀劫持和子前缀劫持预防，并不能预防路径篡改和路由泄露。扩展 RPKI 的功能，使其支持预防 BGP 面临的其他安全问题也是研究关注的焦点。目前，基于 RPKI 的 BGPsec 方案面临开销较大、协议降级攻击等问题；ASPA 存在暴露 AS 之间商业关系的风险。如何降低基于 RPKI 的功能扩展方案的开销、如何使其支持增量部署、如何保护 AS 隐私性是亟待解决的问题。目前，如 SMPC（secure multi-party computation，安全多方计算）等基于隐私保护的计算模式有望使得 AS 在不泄露具体隐私信息的场景下，联合完成某一计算任务（判断一条 AS-PATH 是否存在路由泄露等），为 AS 之间协作检测异常提供了可能性。

目前，RPKI 的部署规模虽有较大的增长，但是距离全面部署仍存在距离，让网络管理员深入了解 RPKI 技术、解决 RPKI 存在的问题以及扩展 RPKI 的功能是提高 RPKI 部署率的关键。

参考文献：

[1] BULTER K, FARLEY T R, MCDANIEL P, et al. A survey of BGP security issues and solutions[J]. Proceedings of the IEEE, 2010, 98(1): 100-122.

[2] BALLANI H, FRANCIS P, ZHANG X Y. A study of prefix hijacking and interception in the Internet[J]. ACM SIGCOMM Computer Communication Review, 2007, 37(4): 265-276.

[3] TOONK A. BGP hijack incident by Syrian Telecommunications Establishment[Z]. BGPMon, 2015.

[4] TOONK A. Turkey Hijacking IP addresses for popular Global DNS providers[Z]. BGPMon, 2014.
[5] KENT S, LYNN C, SEO K. Secure border gateway protocol (S-BGP)[J]. IEEE Journal on Selected areas in Communications, 2000, 18(4): 582-592.
[6] LEPINSKI M, KENT S. An infrastructure to support secure internet routing: IETF RFC6480[S]. 2012.
[7] BORKENHAGEN J. AT&T/AS 7018 now drops invalid prefixes from peers[Z]. NANOG. 2019.
[8] KHARE V, JU Q, ZHANG B C. Concurrent prefix hijacks: occurrence and impacts[C]//Proceedings of the 2012 Internet Measurement Conference. [S.l.:s.n.], 2012: 29-36.
[9] ZHAO X L, PEI D, WANG L, et al. An analysis of BGP multiple origin AS (MOAS) conflicts[C]//Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement. New York: ACM Press, 2001: 31-35.
[10] LAD M, MASSEY D, PEI D, et al. PHAS: a prefix hijack alert system[C]//Proceedings of USENIX Security Symposium. [S.l.:s.n.], 2006: 3.
[11] SHI X, XIANG Y, WANG Z, et al. Detecting prefix hijackings in the internet with argus[C]//Proceedings of the 2012 Internet Measurement Conference. [S.l.:s.n.], 2012: 15-28.
[12] HU X, MAO Z M. Accurate real-time identification of IP prefix hijacking[C]//Proceedings of 2007 IEEE Symposium on Security and Privacy (SP'07). Piscataway: IEEE Press, 2007: 3-17.
[13] ZHENG C, JI L, PEI D, et al. A light-weight distributed scheme for detecting IP prefix hijacks in real-time[J]. ACM SIGCOMM Computer Communication Review, 2007, 37(4): 277-288.
[14] LI J, EHRENKRANZ T, ELLIOTT P. Buddyguard: A buddy system for fast and reliable detection of IP prefix anomalies[C]//Proceedings of 2012 20th IEEE International Conference on Network Protocols (ICNP). Piscataway: IEEE Press, 2012: 1-10.
[15] SIGANOS G, FALOUTSOS M. Neighborhood watch for internet routing: can we improve the robustness of internet routing today?[C]//Proceedings of IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications. Piscataway: IEEE Press, 2007: 1271-1279.
[16] KHAN A, KIM H, KWON T, et al. A comparative study on IP prefixes and their origin ASes in BGP and the IRR[J]. ACM SIGCOMM Computer Communication Review, 2013, 43(3): 16-24.
[17] QIU S Y, MONROSE F, TERZIS A, et al. Efficient techniques for detecting false origin advertisements in inter-domain routing[C]//Proceedings of 2006 2nd IEEE Workshop on Secure Network Protocols. Piscataway: IEEE Press, 2006: 12-19.
[18] HIRAN R, CARLSSON N, SHAMEHRI N. Crowd-based detection of routing anomalies on the Internet[C]//Proceedings of 2015 IEEE Conference on Communications and Network Security (CNS). Piscataway: IEEE Press, 2015: 388-396.
[19] HU Y C, PERRIG A, SIRBU M. SPV: Secure path vector routing for securing BGP[C]//Proceedings of the 2004 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications. [S.l.:s.n.], 2004: 179-192.
[20] ZHAO M, SMITH S W, NICOL D M. Aggregated path authentication for efficient BGP security[C]//Proceedings of the 12th ACM Conference on Computer and Communications Security. New York: ACM Press, 2005: 128-138.
[21] WHITE R. Securing BGP through secure origin BGP (soBGP)[J]. Business Communications Review, 2003, 33(5): 47-47.
[22] OORSCHOT P C, WAN T, KRANAKIS E. On interdomain routing security and pretty secure BGP (psBGP)[J]. ACM Transactions on Information and System Security (TISSEC), 2007, 10(3): 11.
[23] BULTER K, MCDANIEL P, AIELLO W. Optimizing BGP security by exploiting path stability[C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. New York: ACM Press, 2006: 298-310.
[24] XIANG Y, SHI X G, WU J P, et al. Sign what you really care about–Secure BGP AS-paths efficiently[J]. Computer Networks, 2013, 57(10): 2250-2265.
[25] AIELLO W, IOANNIDIS J, MCDANIEL P. Origin authentication in interdomain routing[C]//Proceedings of the 10th ACM Conference on Computer and Communications Security. New York: ACM Press, 2003: 165-178.
[26] GOODELL G, AIELLO W, GRIFFIN T, et al. Working around BGP: An incremental approach to improving security and accuracy in interdomain routing[C]//Proceedings of the Network and Distributed System Security. [S.l.:s.n.], 2003: 156.
[27] GERSCH J, MASSEY D. Rover: Route origin verification using DNS[C]//Proceedings of 2013 22nd International Conference on Computer Communication and Networks (ICCCN). Piscataway: IEEE Press, 2013: 1-9.
[28] CHUNG T, VAN RIJSWIJK-DELI R, CHANDRASEKARAN B, el al. A longitudinal, end-to-end view of the {DNSSEC} ecosystem[C]//Proceedings of 26th {USENIX} Security Symposium ({USENIX} Security 17). [S.l.:s.n.], 2017: 1307-1322.
[29] LYNN C, KENT S, SEO K. X. 509 extensions for IP Addresses and AS identifiers: IETF RFC3779[S]. 2004.
[30] COOPER D, SANTESSON S, FARRELL S, et al. Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile: IETF RFC5280[S]. 2008.
[31] HUSTON G, MICHAELSON G, LOOMANS R. A profile for X.509 PKIX resource certificates: IETF RFC6487[S]. 2012.
[32] LEPINSKI M, KENT S, KONG D. A profile for route origin authorizations (ROAs): IETF RFC6482[S]. 2012.
[33] LEPINSKI M, CHI A, KENT S. Signed object template for the resource public key infrastructure (RPKI): IETF RFC6488[S]. 2012.
[34] HUSTON G, LOOMANS R, MICHAELSON G. A profile for resource certificate repository structure: IETF RFC6481[S]. 2012.
[35] AUSTEIN R, HUSTON G, KENT S, et al. Manifests for the resource public key infrastructure (RPKI): IETF RFC6486[S]. 2012.
[36] TRIDGELL A, MACKERRAS P. The rsync algorithm[Z]. 1996.
[37] BRUIJNZEELS T, MURAVSKIY O, WEBER B, et al. The

RPKI repository delta protocol (RRDP): IETF RFC8182[S]. 2017.
[38] BUSH R, AUSTEIN R. The resource public key infrastructure (RPKI) to router protocol: IETF RFC6810[S]. 2013.
[39] HUSTON G, MICHAELSON G. Validation of route origination using the resource certificate public key infrastructure (PKI) and route origin authorizations (ROAs): IETF RFC6483[S]. 2012.
[40] REKHTER Y, KARRENBERG D, MOSKOWITZ B. Address allocation for private internets: IETF RFC1918[S]. 1996.
[41] MA D, MANDELBERG D, BRUIJNZEELS T. Simplified local Internet number resource management with the RPKI: IETF RFC8416[S]. 2018.
[42] RIPE NCC. Index of /rpki[Z]. 2020.
[43] ROUTEVIEWS. University of oregon route views archive project[Z]. 2020.
[44] DURAND A. Resource public key infrastructure (RPKI) technical analysis[R]. ICANN. 2020.
[45] KENT S, MA D. Adverse actions by a certification authority (CA) or repository manager in the resource public key infrastructure (RPKI): IETF RFC8211[S]. 2017.
[46] HEILMAN E, COOPER D, REYZIN L, et al. From the consent of the routed: improving the transparency of the RPKI[C]//Proceedings of the 2014 ACM conference on SIGCOMM. New York: ACM Press, 2014: 51-62.
[47] HARI A, LAKSHMAN T V. The Internet blockchain: A distributed, tamper-resistant transaction framework for the Internet[C]//Proceedings of the 15th ACM Workshop on Hot Topics in Networks. New York: ACM Press, 2016: 204-210.
[48] ALFONSO DLRG, PAPADIMITRATOS P. Blockchain-based public key infrastructure for inter-domain secure routing[C]//Proceedings of International Workshop on OPEN Problems in Network Security (iNetSec). [S.l.:s.n.], 2017: 20-38.
[49] PAILLISSE J, FERRIOL M, GARCIA E, et al. IPchain: Securing IP prefix allocation and delegation with blockchain[C]// Proceedings of 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Piscataway: IEEE Press, 2018: 1236-1243.
[50] XING Q, WANG B, WANG X. BGPcoin: Blockchain-based Internet number resource authority and BGP security solution[J]. Symmetry, 2018, 10(9): 408.
[51] ANGIERI S, GARCÍA-MARTÍNEZ A, LIU B, et al. A distributed autonomous organization for Internet address management[J]. IEEE Transactions on Engineering Management, 2019, 67(4): 1459-1475.
[52] 刘冰洋, 杨飞, 任首首, 等. 去中心化互联网基础设施[J]. 电信科学, 2019, 35(8): 74-87.
LIU B Y, YANG F, REN S S, et al. Decentralized internet infrastructure[J]. Telecommunications Science, 2019, 35(8): 74-87.
[53] SAAD M, ANWAR A, AHMAD A, et al. RouteChain: towards blockchain-based secure and efficient BGP routing[C]// Proceedings of 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). Piscataway: IEEE Press, 2019: 210-218.
[54] HE G, SU W, GAO S, et al. ROAchain: Securing route origin authorization with blockchain for inter-domain routing[J]. IEEE Transactions on Network and Service Management, 2020.
[55] CHEN D, BA Y, QIU H, et al. ISRchain: Achieving efficient interdomain secure routing with blockchain[J]. Computers & Electrical Engineering, 2020(83): 106584.
[56] GILAD Y, COHEN A, HERZBERG A, et al. Are we there yet? On RPKI's deployment and security[C]//Proceedings of NDSS. [S.l.:s.n.], 2017.
[57] GILAD Y, GOLDBERG S, SRIRAM K, et al. The use of maxlength in the RPKI: draft-ietf-sidrops-rpkimaxlen-05 (work in progress)[Z]. 2020.
[58] GILAD Y, SAGGA O, GOLDBERG S. Maxlength considered harmful to the RPKI[C]//Proceedings of the 13th International Conference on Emerging Networking Experiments and Technologies. [S.l.:s.n.], 2017: 101-107.
[59] LEPINSKI M, SRIRAM K. BGPsec protocol specification: IETF RFC8205[S]. 2017.
[60] LYCHEV R, GOLDBERG S, SCHAPIRA M. BGP security in partial deployment: Is the juice worth the squeeze?[C]// Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM. New York: ACM Press, 2013: 171-182.
[61] PATEL K, SNIJDERS J, HOUSLEY R. A profile for autonomous system provider authorization: draft-azimov- sidrops-aspa-profile-04[Z]. 2020.

[作者简介]

苏莹莹（1997− ），女，清华大学计算机科学与技术系博士生，主要研究方向为互联网体系结构及其安全。

李丹（1981− ），男，清华大学计算机科学与技术系教授，主要研究方向为互联网架构与协议设计、数据中心网络、软件定义网络。

叶洪琳（1998− ），女，清华大学网络科学与网络空间研究院硕士生，主要研究方向为互联网体系结构及其安全。