计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(2):316−324 [doi: 10.15888/j.cnki.csa.008321]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于 RPKI-ASPA 改进的 BGP 路径保护机制①

包 卓[1,2], 马 迪[1,2,3], 毛 伟[2,3], 邵 晴[3]

[1](中国科学院 计算机网络信息中心, 北京 100190)
[2](中国科学院大学, 北京 100049)
[3](互联网域名系统北京市工程研究中心, 北京 100190)
通信作者: 包 卓, E-mail: baozhuo@zdns.cn

摘 要: BGP 协议明文传输, 攻击者易对前缀与路径信息进行伪造, 进而引发危害巨大的前缀劫持攻击. 其中, AS 路径信息保护问题主要涉及两个方面: 路径防篡改与非法内容验证. RPKI 作为解决路由劫持的重要安全体系, 目前其体系下的路径验证解决方案主要包括 BGPSec、ASPA 与 Path-End, 其中 BGPSec 主要解决的是路径篡改问题, ASPA 与 Path-End 解决路径合法性验证问题, 而这些方案分别存在计算复杂或者路径保护力度较弱的缺陷. 在 ASPA 方案中引入少量签名, 可对路径篡改的限制粒度进行提升. 据此, 本文提出一种改进的路径保护机制, 并设计了与其余方案的开销、安全性能对比实验. 实验结果表明, 在引入有限开销的情况下, 改进机制的路径保护性能优于其余方案.

关键词: BGP; 路径验证; RPKI; ASPA; BGPSec

引用格式: 包卓,马迪,毛伟,邵晴.基于 RPKI-ASPA 改进的 BGP 路径保护机制.计算机系统应用,2022,31(2):316–324. http://www.c-s-a.org.cn/1003-3254/8321.html

Improved BGP Path Protection Mechanism Based on RPKI-ASPA

BAO Zhuo[1,2], MA Di[1,2,3], MAO Wei[2,3], SHAO Qing[3]

[1](Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190, China)
[2](University of Chinese Academy of Sciences, Beijing 100049, China)
[3](Internet Domain Name System Beijing Engineering Research Center, Beijing 100190, China)

Abstract: In the BGP protocol plaintext transmission, attackers easily forge the prefix and path information, which thereby causes prefix hijacking with great harm. The AS path information protection mainly involves two aspects: path tamper-proofing and verification of illegal content. Resource public key infrastructure (RPKI) is an important security system to solve route hijacking. Currently, the path verification solutions under the RPKI system mainly include BGPSec, ASPA and Path-End, among which BGPSec mainly addresses path tampering, while ASPA and Path-End target path legality verification. However, these schemes have the defects of complicated calculation or weak path protection. A small number of signatures are introduced into the ASPA scheme to improve the granularity limiting path tampering. Therefore, this study proposes an improved path protection mechanism and designs comparison experiments with other schemes regarding the overhead and safety performance. The experimental results show that the performance of the improved scheme is better than that of the other schemes under the condition of introducing limited overhead.

Key words: BGP; path validation; RPKI; ASPA; BGPSec

① 收稿时间: 2021-04-19; 修改时间: 2021-05-19; 采用时间: 2021-06-02; csa 在线出版时间: 2022-01-17

1 背景

1.1 现状

全球互联网中, BGP (border gateway protocol, 边界网关协议) 是目前域间路由器进行可达性信息交换应用最广泛的安全协议, AS_PATH 是 BGP update 报文中一种通用属性, AS 边界路由器在广播前缀地址时, 会在 AS_PATH 最左端加上自己的 AS 号, 随后将该通告传递给邻居. 利用 AS_PATH 信息, 路由器可进行决策信息的补充, “AS-Path Prepend”技术[1] 在路径信息中预装填自己的 AS 号, 用来影响 AS_PATH 属性长度, 实施流量工程. “BGP Poisoning”[2] 则是利用 BGP 防环机制, 通过预装填 AS 号来达到绕过具体 AS 目的的一种方案.

AS_PATH 明文传输且影响路由决策, 攻击者可对 AS_PATH 进行伪造, 删除或者恶意增加, 来影响后续路由器的路径抉择, 以达到 ip 前缀流量劫持的目的. 针对 Update 中 AS_PATH 的验证问题, 学术界提出过多种解决方案, 该文献提出了 sBGP (secure BGP)[3] 的解决方案, sBGP 同样使用 PKI 体系对网络资源进行验证, sBGP 基于资源分配的层级模型, 分别为 ip 前缀分配、AS 编号及其路由器信息建立 PKI 认证体系. 在 BGP 路由器传递数据包过程中, 采用逐跳嵌套的方式, 将“地址”和“路由”的数字签名添加进路径属性中. 结合 IPSec, 保证路由源头和路径的合法授权验证.

soBGP (secure origin BGP)[4] 方案采用分布式认证中心, 为每个 AS 签发用以身份认证的证书 EntityCert, 根据每一个 AS 对 ip 前缀资源的持有状态签发证书, 完成路由源的授权. 同时, 利用证书 ASPolicyCert 将邻间关系签发后进行广播. 通过建立的全局视图, 任意路由器可对 AS_PATH 信息进行验证, 以此对 BGP 通告进行过滤.

IRV (interdomain routing validation)[5] 方案最大的特征是每个 AS 挂载一台验证服务器, 通过提供该 AS 历史通告记录的验证查询, 确保全网路由信息“可查”和“可信”.

1.2 RPKI 体系与路径验证

1.2.1 RPKI 体系架构

RPKI (resource public key infrastructure, 资源公钥基础设施) 是一种基于 PKI 体系的路由资源保护方案, 截至 2021 年 1 月, 全球 RPKI 部署率已达 27.2%[6]. RPKI 工作架构如图 1, 资源持有者通过资源证书的层级签发来进行号码资源的分配, 资料库负责证书的存储, 依赖方负责授权信息的验证与推送, 有效的授权信息将指导 BGP 环境号码资源的认证.

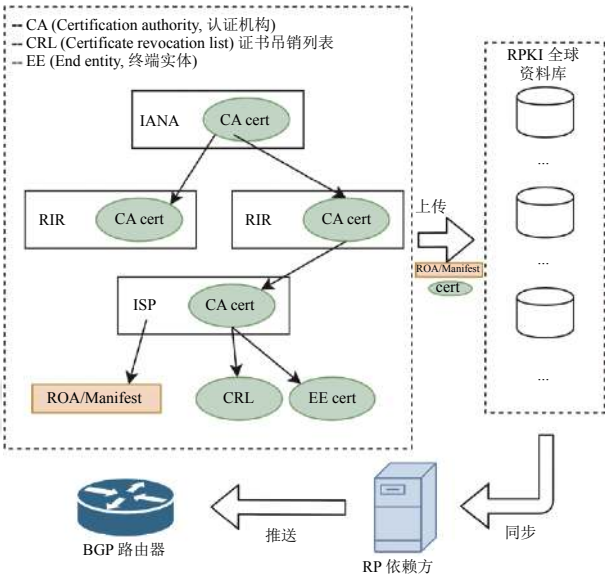

图 1 RPKI 架构

1.2.2 BGPSec

BGPSec (border gateway protocol security)[7] 方案借鉴了上述 sBGP 方案中的签名思路, 利用 RPKI 体系中的路由器证书及其密钥信息, 对链路 AS 信息进行签名. 其中, 路径签名信息循环嵌套, 通过 BGP Update 数据包进行传递. 前 AS 对包含后 AS 号码的路径信息进行签名, 表示对后一 AS 进行通告授权, 严格确保 AS_PATH 属性中的信息不被篡改.

BGPSec 是一种严格的路径保护方案, 其高频率的密码学计算, 给路由器的硬件带来极大的算力考验, 同时也降低了 BGP 的实际收敛速率, 该方案难以在实际环境中进行大规模部署.

同时在身份未知的网络环境中, BGPSec 无法对 AS_PATH“合理性”做出验证, 因此无法阻止路由泄露的发生. 在性能方面, BGPSec 逐跳签名引入了大量的计算开销与内存消耗. 对于两者开销瓶颈, 学术界存在一些优化思路. 例如通过使用签名聚合签名的方法减少签名的传递负载与计算消耗[8], 或者使用新型密码学进行公钥的传递[9], 以减少证书存储的内存消耗等.

1.2.3 Path-End

2016 年, 基于 RPKI 体系, Cohen 提出了 Path-End[10] 方案, Path-End 方案继承路由源认证的同时对路径验证进行了拓展, 使用 RPKI 密钥对源头与邻居的有效连

接声明进行签发. 与“严格”的 BGPSec 方案相比, Path-End 只对 AS_PATH 末尾信息进行验证, 确保离源最近一跳路径的合理性. 通过简单的验证规则, Path-End 能同时抵御路由源劫持与最后一跳路径篡改引发的劫持, 带来不错的安全收益. 但是 Path-End 无法对离源一跳以上及其复杂的路径篡改进行有效识别.

1.2.4 ASPA

沿袭于 soBGP 签发邻间关系的思路, 2018 年 IETF SIDROPS 工作组提出了一种 ASPA (autonomous system provider authorization) 的路径验证方案草案[11], 并进行了多次版本迭代. ASPA 同样基于 RPKI 体系, 具体思路如下:

(1) ASPA 整体基于“Valley-Free” (无谷模型)[12], 即认为所有 AS 都遵守基本的路由转发策略, 在 C2P、P2P 和 P2C 三种“合法”商业关系中进行传递. 如图 2 所示, AS1 发出的路由通告途径 AS2、AS3, 到达 AS4, 随后再通过 AS4 发往下游. 图中 ASPA 数据二元组 AS1:{AS2}表示为 AS2 是 AS1 的 provider.

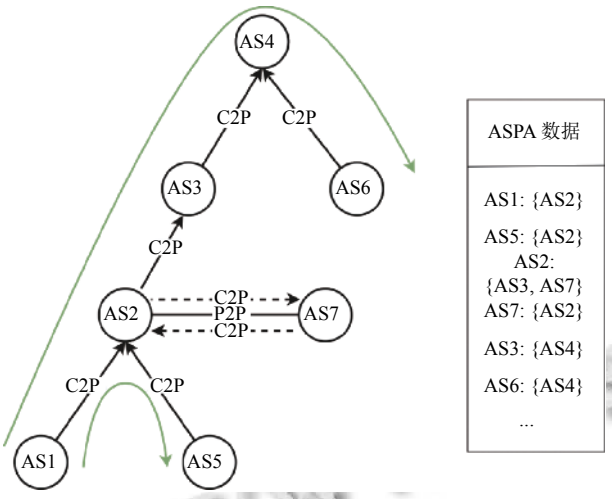

图 2 ASPA 原理图

(2) ASPA 认为在进行路由通告的过程中, 需要重点保护上游部分, 防止错误的信息传递给大型运营商, 造成大规模的路由泄露等安全事件.

(3) AS 发起前缀通告, 开始方向均指向上游, 即路径中的转发关系一定从 C2P 或者 P2P 开始, 当通告到达最大的一个 provider 之后, 转向下游传递, 一旦转向下游之后不会再转向上游.

(4) 解析 Update 报文中的 AS_PATH 属性, 得到 AS_SEQUENCE 信息后, ASPA 方案通过一个单位为 2 的滑动窗口对 AS_PATH 信息进行校验. 在验证过程中, 检索相应 ASPA 对象, 对路径转发状态进行判断, 并根据转发状态对路由信息进行验证过滤.

ASPA 巧妙地利用 RPKI 体系实现了路径的验证, 结合 ROA 路由源验证, ASPA 能够很大程度上限制各类路由泄露的发生. 区别于 BGPSec, ASPA 能够对整个路径属性进行“合法”校验, 不仅对 AS 之间的可达性进行验证, 还对其中转发关系的“合法性”进行验证. 其次, ASPA 的验证过程不产生密码学的计算, 即对路由器的硬件性能无过高要求. 同时在实际部署中, ASPA 能够实现增量部署.

但是对于路径篡改问题, ASPA 并没有提供完整的解决方案. ASPA 相当于将静态的拓扑关系进行发布, 但是在实际 BGP 环境中, 实时通告的最终路径, 均受到复杂的路由策略与决策的影响. ASPA 完全基于 AS 粒度对通告路径进行检测, 存在以下缺陷:

ASPA 对路径的限制基于 AS 粒度, 然而 ip 前缀在广播的过程中存在多条潜在路径, 路由器只对最优路径进行广播. 故在 ip 广播的过程中, AS 粒度级别的路径限制并不能对 AS_PATH 属性进行百分百的保护. 由于 ASPA 提供了全局 AS 拓扑视图, 在缺乏密码学保护的情况下, 任何一个路由器可以根据数据集伪造出能通过验证的路径, 绕过 ASPA 验证完成欺骗. 其次, 随着路径长度的增加, 能够产生多条“合法”路径的可能性越大, 因此被篡改的几率也会随之增加.

图 3 描述了路径篡改的可能性, 图中 ASX, ASY, ASZ, ASP 分别代表号码为 X, Y, Z, P 的自治域边界路由器. ASP 发出一个前缀通告 p, 该条前缀通告通过不同路径到达 ASY, 根据路由策略与路由优选后, 将该通告发送给 ASZ, ASZ 收到包之后, 将包的 AS_PATH 属性进行有意合成篡改, 此举能够绕过 ASPA 的检测.

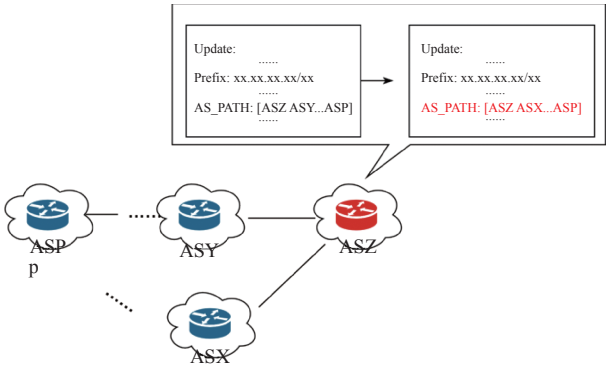

图 3 路径篡改示例

图 4 提供了一个前缀劫持的实际案例, ASX 同样作为说谎者, 将路径属性修改成了较短的路径 1, 由于 ASX 伪造的路径 1 比较短, ASX 便成功劫持了前缀 f1 的流量.

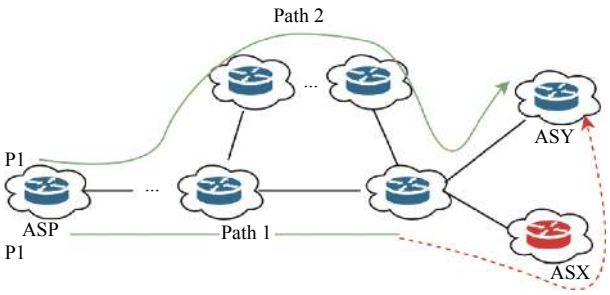

图 4 前缀劫持例子

2 改进的路径保护方案

AS_PATH 的验证方案中, BGPSec 的签名操作实际上引入了用以“比对”的路径“副本”, 在路由进行通告时带上签名, 路由器在收到通告时进行签名的验证等同于“副本”的“比对”, 抵御信息篡改导致的安全攻击. 基于 ASPA 提供的方案, 我们提出了一种间隔签名, 并只做一次签名验证的路径保护方案.

2.1 证书体系

如图 5, 改进方案基于 RPKI, 密钥体系沿用 RFC8635[13] 的方案, 公私密钥对可由管理员生成或者路由器本地生成, 随后向 RPKI 系统中对应组织请求生成携带公钥的路由器证书 (router-cert), 发布于全球 RPKI 仓库. 其中路由器证书属于 RPKI终端 EE 证书, 携带 AS 号码资源, 资源由资源持有者进行层次授权, 并由相应 CA 进行管理.

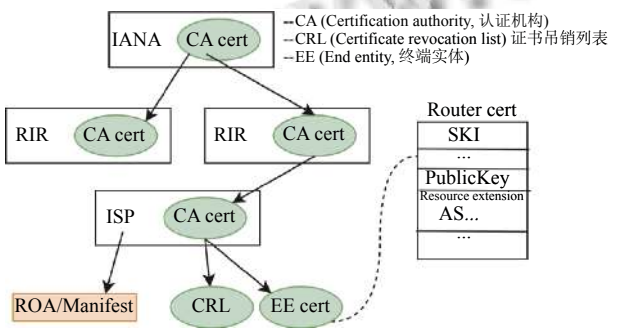

图 5 证书体系

RP 依赖方服务器对 RPKI 资料库进行同步, 并按层级进行一致性检查与资源授权校验后进行本地缓存, 之后定期将合法数据推送给路由器. 路由通告传递过程中, 路由器使用私钥产生签名, 验证者根据 SKI 信息查找对应路由器证书进行签名验证.

2.2 隔跳签名

当路径签名内容包含下一个 AS 时, 后续第一个 AS 受到签名限制, 无法对路径信息进行篡改. 而引入静态的有效数据例如 ASPA 数据后, 能够延长签名的限制半径, 则可考虑适度降低签名的产生频率.

如图 6, 在“Multi-Homing”[1] 的场景中, customer 通过不止一个 provider 连接互联网. 其中, customer 将其路由前缀向其 provider 进行通告, 并按照商业关系制定实际导出策略, 即遵循“Valley-Free”(无谷模型)[12]. 同时为满足一部分性能指标, customer 可给不同 provider 制定不同的转发策略. 以达到降低链路延迟、提高连接可靠性、流量负载均衡等目的.

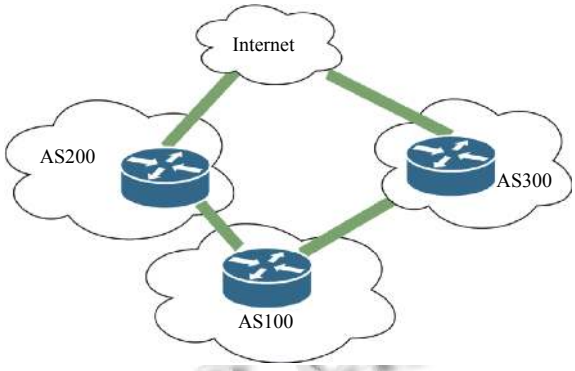

图 6 Multi-Homing 模型

在添加签名机制之后, 因数据包存在路径签名信息, 故在未实际窃取数据包的情况下, 攻击者无法凭空进行数据包的伪造. 可知具体前缀的路径决策为 ASPA 数据的子集. 因此将 ASPA 用于路径验证存在以下情况如图 7, AS100 路径签名后将 ip 数据包转发给 AS200, 同时, AS200 对应的 ASPA 二元组数据集有 AS400 与 AS300, 其中 AS300 与 AS400 为不同运营商, 同时为 AS200 提供服务. 因为使用不同的转发策略, AS200 的一部分前缀只向 AS400 转发. 但是攻击者 AS300 通过网络嗅探等方式, 获取到该前缀的数据包, 可进行数据包的重放转发, 污染后序 AS 的路由表.

在此攻击场景中, AS400 与 AS300 作为 ISP 竞争者, 同时为 customer 提供连接互联网服务, 其重放攻击目的通常仅出于流量计费利益, 此类基于竞争的攻击对全局互联网危害具有局部性, 并且易被 customer 察

觉. 同时, 根据 caida relationship[14] 数据分析可得, 只有一个 provider 的 customer 数量占比接近 40%. 在不考虑此种攻击的情况下, 可以直接使用 ASPA 数据作为路由决策的验证数据.

ASPA 数据中, 授权关系不存在传递性, 即 ASPA 的授权关系是一对一的, 无法通过多个 ASPA 数据拼接进行传递, 则可知一次签名加上一次 ASPA 授权验证, 签名频率最多可减为隔跳一次. 可知在基于 ASPA 数据的隔跳签名的机制中, 有以下特性:

1) 保证路径内容合法. ASPA 二元组数据携带了两类基本信息, 其一为二元组之间的连接关系. 其二两者存在商业关系. 利用第一类信息, 可对任意两个 AS 之间连接性进行验证. 利用第二类信息, 能够路径内容合理性, 即转发与决策过程的合法性进行校验.

2) 防止路径篡改. ASPA 机制下, 长度大于一的路径存在篡改的隐患. 通告传递过程中, 其中每个 AS 均知晓通告 AS_PATH 和邻间者 AS 信息. 在隔跳签名操作下, 签名内容能够覆盖所有的 AS 号码. 其中, 签名内容直接包含后续第 1 个 AS. 而对于后续第 2 个 AS 来说, 已无法对签名包含的历史路径进行修改, 而其与第一个 AS 连接合理性可由 ASPA 二元组给出证明. 则可知签名的最大有效半径为 2, 签名者间距最长可为 2. 同时, 为防止签名者缓存路径后进行签名重放伪造, 签名信息加入可 ip 前缀信息.

如图 8, 对于签名者 AS3 来说, 存在邻居 AS8 和 AS4, 当通告发送至不同邻居时, AS3 针对不同出口 AS 进行签名. path1 中, 当通告途径 AS4 转发时, 后续 AS 通过签名可证 AS_PATH 中 AS4 真实性, 同时在 ASPA 提供的数据中, 能检索到 (AS4, AS5)、(AS4, AS6) 和 (AS4, AS7) 二元组, 可知, AS5、AS6、AS7 均与 AS4 存在有效连接. 则 AS3 所提供的路径签名能够对半径为 2 以内的 AS 做出路径篡改的限制.

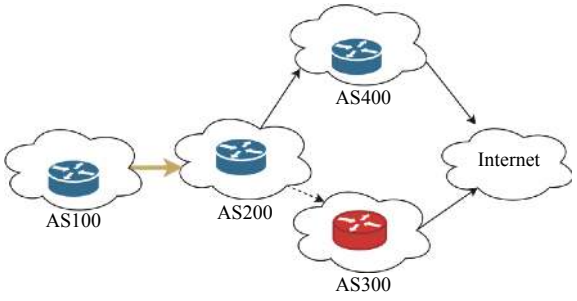

图 7 嗅探重放攻击示例

对于两跳之外的 AS, 如 AS5、AS6、AS7 的后续邻居, AS3 的签名信息无法对后续路径内容作出限制. 同样的, 对于另外一条路径 path2{…AS3 AS8 AS4…} 来说, AS5、AS6 和 AS7 均在半径两跳之外, 此时, 需要 AS4 进行后续签名补充, 对半径为 2 以内的 AS 进行限制.

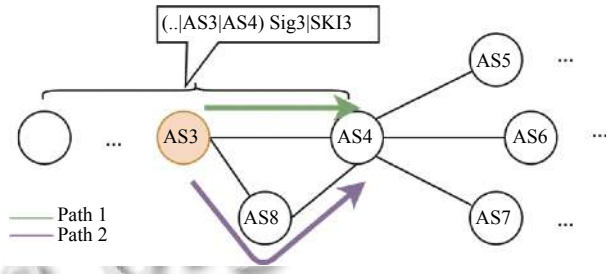

图 8 隔跳签名保护

2.3 具体方案

根据上述原则, 如图 9, BGP 协议 Update 路径属性中增加可选过渡的属性“PATH_SIGNATURE”, 该属性保存 ip 前缀及其 AS_PATH 属性对应的签名和签名者 SKI 信息, 设置该属性缓存队列长度为 2, 即最多保存两个签名信息. 假设 ASPA 数据的签发与改进机制部署同步, 即可通过查询该 AS 对应 ASPA 数据个数是否为零来判断部署情况, 则在 ASPA 数据签发率较高的情况下, 改进方案如下.

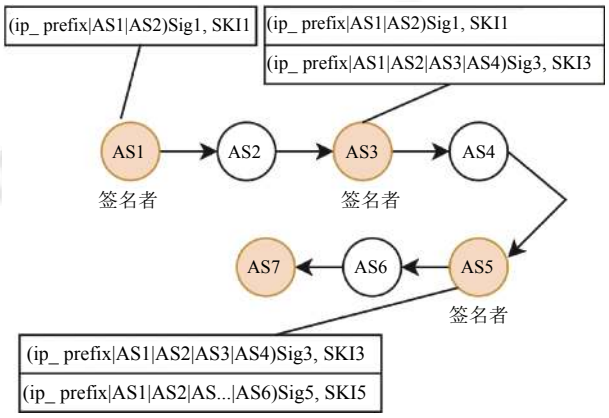

图 9 隔跳签名方案

1) 签名. 如算法 1 描述, 在 BGP 通告转发过程中, 进行路径信息的隔跳签名. 同时签名缓存队列只保留两个最新的签名信息. 通过第 2.2 节所述隔跳签名原理, 该签名方案能够将定期将 AS_PATH 信息以签名副本的形式进行保存, 并且签名者同时受到上一个签发者签名信息制约, 可保证每一个签名的内容合理性. 在全局部署的情况下, 签名者次序为连续奇数.

算法 1. AS_PATH 签名算法

1) 路由源 AS 发起 ip 前缀通告时产生签名, 跳转步骤 5.
2) 解析路径属性 AS_PATH, 遍历 AS 号, 获取 AS 号码的次序索引.
3) 如果次序为奇数, 则将即将转发的 AS 编号拼接 AS_PATH 作为数字签名的摘要内容, 利用私钥进行签名, 跳转步骤 5).
4) 如果次序不为奇数, 判定为非签名者, 则直接返回.
5) 取签名队列块部分, 将产生的签名进队操作.
6) 如果队列长度大于 2, 则出队至长度为 2 为止.

2) 验证. 如算法 2 描述, 每一个 AS 接收到 BGP 通告时, 将 AS_PATH 信息和 PATH_SIGNATURE 信息进行解析, 首先对 AS_PATH 进行 ASPA 的常规检查, 判断整条 AS_PATH 的转发关系是否合法. 后对 AS_PATH 信息遍历, 匹配到最新两个签名者的 AS 号及其签名, 使用签名携带的 SKI 信息匹配到对应的路由器证书, 对有效验证半径内的签名信息 PATH_SIGNATURE 和 AS_PATH 明文进行密码学验证, 返回验证结果.

算法 2. AS_PATH 签名验证算法

1) 解析得到 AS_PATH, 并记录索引, 根据 ASPA 数据集, 统计路径中已部署 AS 序列;
2) 遍历进行常规 ASPA 校验, 校验状态为 invalid 直接跳转步骤 8;
3) 判断已部署 AS 序列中, 上一个 AS 是否为签名者, 是则跳转步骤 4, 否跳转步骤 5;
4) 获取队列首部签名, 截取取倒数第 2 个签名者索引后一位的 AS_PATH 信息, 跳转步骤 6;
5) 获取队列尾部签名, 获取全局 AS_PATH 信息, 跳转步骤 6;
6) 根据 SKI 匹配路由器证书;
7) 将 ip 前缀与 AS_PATH 信息拼接, 进行签名验证;
8) 返回校验结果.

2.4 性能分析

2.4.1 收敛时间

建立简单的 BGP 收敛拓扑图 $G(V, E)$, 其中节点和边集合分别表示为 $V=\{v_1, v_2, v_3, \cdots, v_n\}$, $E=\{e_1, e_2, e_3, \cdots, e_n\}$, 其中, 定义路径集合 $R_{i\to j}(G)=\{\{v_i, v_{i+1}, \cdots, v_{j-1}, v_j\}, \cdots\}$表示所有从节点 v_i 到节点 v_j 合法路径, 路径 $r_{i\to j}\in R_{i,j}(G)$ 表示集合中最长路径.

节点 v_i 发起路由通告, 当其余节点均接收到该通告, 并作出相应一致性处理后, 认为 v_i 发起的路由通告全局收敛. 可知收敛时长为式 (1), P_{vi} 表示 v_i 节点对数据包处理的总体时间开销, 包括路由表项定位与处理更新及其出口数据处理时间开销, T_l 为通信链路时间开销. 则可知 ASPA 与 Path-End 开销为式 (2), BGPSec 方案总体时间开销为式 (3), 改进方案时间开销为式 (4), 其中 $T_{\text{sign\_path}}$ 与 $T_{\text{validate\_path}}$ 分别为进行一次数字签名与签名验证的时长, 可知 $T_{\text{sign\_path}}$ 与 $T_{\text{validate\_path}}$ 系数增长趋势如图 10 和图 11.

$$T_{con}=(|r|-1)T_l+\sum_{v_i\in r}P_{v_i} \tag{1}$$

$$T_{con}=(|r|-1)\left(T_l+T_p\right) \tag{2}$$

$$T_{con}=(|r|-1)\left(T_l+T_p\right)+(|r|-1)T_{\text{sign\_path}}+(|r|-1)\left\lfloor\frac{|r|}{2}\right\rfloor T_{\text{validate\_path}},|r|\geqslant 1 \tag{3}$$

$$T_{con}=(|r|-1)\left(T_l+T_p\right)+\left\lfloor\frac{|r|}{2}\right\rfloor T_{\text{sign\_path}}+(|r|-1)T_{\text{validate\_path}},|r|\geqslant 1 \tag{4}$$

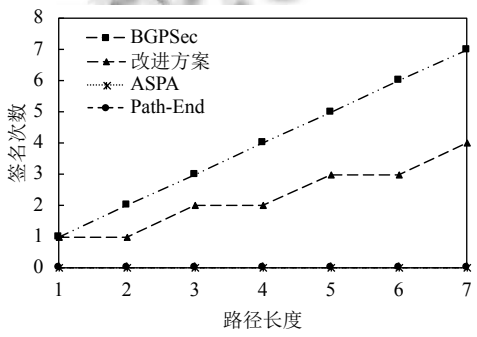

图 10 签名次数

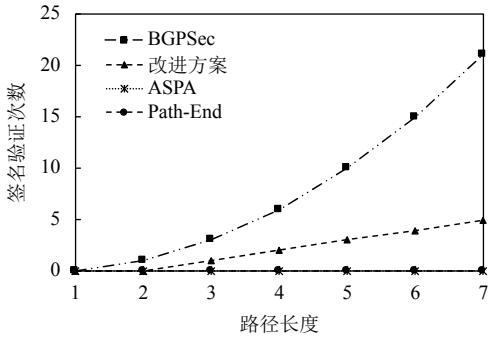

图 11 签名验证次数

假设最长传播路径长度为 n, 对于 BGPSec 来说, 可知密码计算消耗主要体现在签名验证部分. 其总体签名次数为 n, 签名验证次数为 $n(n–1)/2$, 相比之下, 改进方案只有奇数次序路由器产生签名, 故签名总次数为 $n/2$. 验签的次数为 n. 可知收敛时间性能方面, 改进方案优于 BGPSec.

而对于只考虑路径“合理”校验的 ASPA 与 End-Path 来说, 不涉及到密码计算, 故整个过程签名与验签次数均为 0.

可知全球 AS_PATH 长度平均为 4.3[15], 改进方案中, 大部分路由通告从传播到收敛, 实际只需要进行一到两次的签名, 签名验签次数也平均为 3 次, 相比较

BGPSec 的消耗而言, 改进方案在原 ASPA 方案基础上引入的时间消耗有限.

2.4.2 空间消耗

内存消耗. 考虑路由器 RIB 表随签名增加的内存消耗. 可知 RIB 中路径属性的内存消耗与表项数存在线性关系, 单个表项内存消耗也与签名数量存在线性关系, 可知, 改进方案中, 路由器需要处理的签名数量少于 BGPSec, 在路径属性带来的内存消耗方面, 改进方案也小于 BGPSec.

通信负载消耗. BGPSec 方案通过直接修改 AS_PATH 信息来负载签名信息, 改进方案则通过增加路径属性来负载签名信息. 在签名算法一致的情况下, BGPSec 需要增加路径长度等量的签名信息, 而改进方案只保留长度为 2 的签名缓存队列, 故改进方案通信负载消耗也小于 BGPSec.

ASPA 与 End-Path 均未对 BGP 进行修改, 无需增加额外的通信负载与路由表负载, 故在与上述两种方案对比之下, 改进方案引入了相对有限的空间消耗.

2.5 安全性分析

假设绝大多数 AS 都完成了 ASPA 部署, 即 ASPA 数据签发率足够高, 则改进方案对路径安全保护性能分析如下:

1) 路由泄露: 该方案基于 ASPA 改进, 在 ASPA 验证结束后才进行路径签名验证, 使用 ASPA 原生数据获得 AS 之间的商业关系, 可以识别 1、2、3、4 型路由泄露[4], 结合 ROV, 可以识别 5、6 型路由泄露. 改进方案集成了路由泄露检测的功能. 有效地保护部署者, 防止部署者受到路由泄露的危害.

2) 路径删除: 路径签名中, 已经对历史签名进行签名, 攻击者对 AS_PATH 属性进行恶意删除将会导致签名验证不通过. 因此路径删除直接导致通告被丢弃.

3) 路径增加: 与路径删除攻击一致, 构造签名信息时, 签名代表一定程度上可以视为历史版本的凭证. 一旦对 AS_PATH 属性进行恶意增加, 需要同时增加签名信息, 或者修改签名信息, 否则路径签名验证不通过. 因此恶意增加路径信息也被成功限制.

4) 路径合成: 在路径伪造的同时, 也需对路径信息的数字签名进行伪造, 否则无法通过验证. 私钥只有签名者自己持有, 其余 AS 路由器无法修改 AS_PATH 的签名信息. 由于 ASPA 数据验证的存在, 且连续两个签名信息的明文存在交集, 故任一 AS 均受到上一个签名者 AS 的限制, 无法进行路径的合成伪造.

原生 ASPA 方案使用转发关系进行路径验证, 能够有效阻止路由泄露的发生, 改进方案继承了 ASPA 方案的优点的基础上, 引入了周期性的签名, 增强了其安全性能.

相应的, BGPSec 方案使用签名嵌套, 因此密码计算消耗较大, 并且由于转发关系的未知, BGPSec 方案无法阻止路由泄露与虫洞攻击的发生.

Path-End 校验规则简单, 只能对简单的源头一跳路径进行有效验证, 无法对复杂的路径篡改进行有效识别.

四者的具体优缺点对比见表 1.

表 1 4 种路径验证方案的比较

验证机制	主要优点	主要缺点
BGPSec	路径属性进行嵌套签名, 进行严格保护	签名复杂, 计算消耗大; 降级攻击; 虫洞攻击; 无法阻止路由泄露
ASPA	基于商业关系进行验证, 轻量, 增量部署效果好	路径属性保护粒度较小; 只能对篡改进行“限制”, 仍然可以通过路径合成绕过验证
Path-End	验证规则简单, 能过滤最常见的一跳路径篡改	无法对复杂的路径篡改进行识别与过滤
改进方案	获取商业关系基础上引入签名, 保护路径属性, 计算开销小	依赖全局ASPA数据, 保护性能受ASPA部署率制约. 无法阻止合法竞争者嗅探重放攻击

3 实验分析

3.1 实验设计

BGP 路由器处理路由通告的流程如图 12, 路由器从邻居接收到通告数据包, 路由信息经过策略决策和路径优选后, 将被存入本地 RIB 表中, 随后路由器将最优路径转发给邻居 AS, 完成路由信息的传达.

近年来容器虚拟化技术逐渐兴起, 利用容器虚拟化技术, 可在有限的资源里进行资源扩展, 使物理机器实现对多台设备的虚拟. 利用虚拟网络, 可对节点交互进行模拟, 进行网络仿真实验.

为模拟路由器的实时响应, 该实验使用 golang 语言轻量级的 goroutine 编写服务, 整体架构如图 13, 仿照 BGP 邻间协商, 该实验模拟 AS 路由器建立连接, 并且将节点拓展到其余容器实例, 进行 BGP Update 仿真模拟. 节点部署完毕, handle 模块将采集的通告信息进行同步发送, 同时设置路由通告计数器, 根据计数器数

值判定收敛状态. 其中, 每一个路由器根据通告路径信息可知自己的位置索引, 根据对路径属性不同处理方案完成路由通告的解析与验证, 具体实验环境参数如表 2.

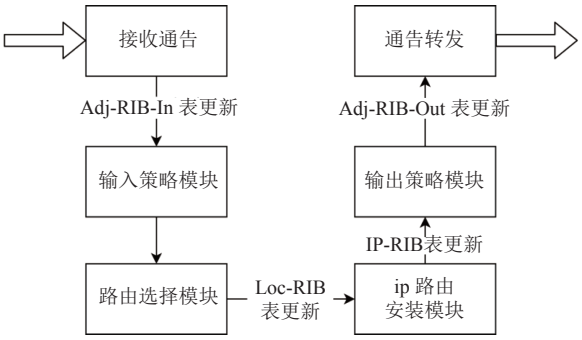

图 12 BGP 数据处理流程

表 2 实验环境

实验环境	参数
CPU	6 Westmere E56xx/L56xx/X56xx (Nehalem-C)
内存	8 GB
操作系统	Ubuntu 16.0
虚拟容器	Docker 18.09.2 image alpine

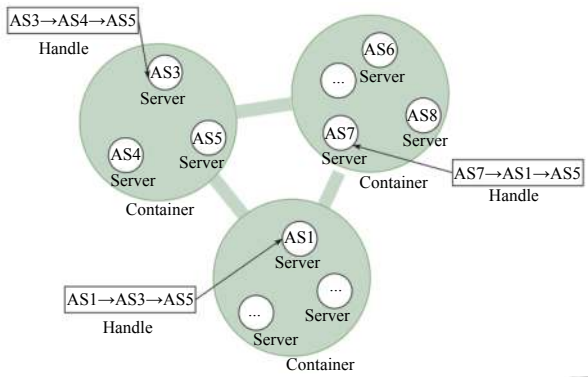

图 13 实验架构图

全网 BGP 路由器实时产生路由通告, 是一个动态收敛的过程. 该实验使用 BGPStream 项目收集的 3 个收集器的 update 数据集. 采用最近的 12 月 1 日的数据集. 全网 AS 数量大约 6 万个, 经过数据清洗操作后, 该数据集合剩下 3 万个 AS 接近 500 万条路由通告.

为描述签名数量导致的收敛速率的差异, 在仿真逻辑与数据一致的基础上, 分别在 1 千、10 千、100 千、500 千、1 000 千、2 000 千、2 500 千、3 000 千、3 500 千、4 000 千条前缀通告基础上进采样行测量, 进行收敛时间对比, 同时, 在数据处理转发的过程中, 对几个连接数较大的 AS 进行签名处理数量的统计.

在考虑全局部署的情况下, 实验结果如图 14 与图 15.

据图 14 收敛时长对比可知, 改进方案场景下的收敛时长明显短于 BGPSec 场景下的收敛时长, 并且随着网络拓扑规模的增加, 前缀数量的增多, 收敛时长的差距会愈加明显. 相比之下, 优化方案在引入少量签名之后, 收敛时长在原有 ASPA 机制的基础上增长有限.

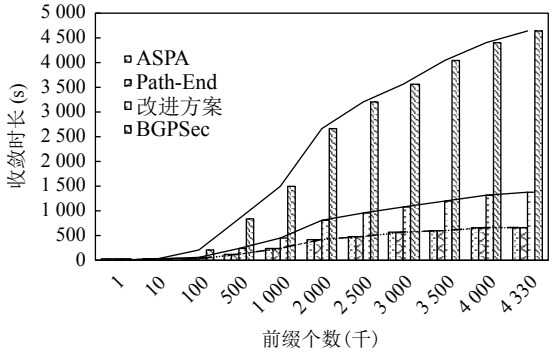

图 14 收敛时间

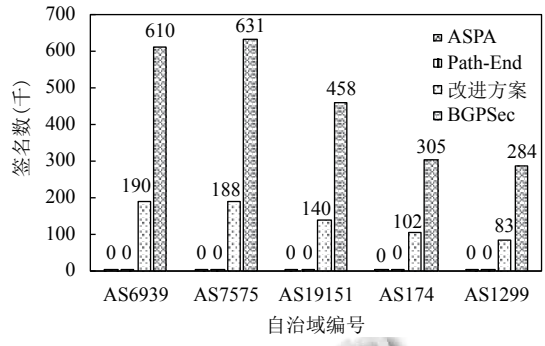

图 15 实际签名处理个数

据图 15 可知, 在相同网络拓扑中, 对于路由器来说, 改进方案签名缓存数量远少于 BGPSec, 根据上文推测的签名数量与内存消耗的线性关系, 可知改进方案签名缓存的内存消耗也明显小于 BGPSec, 高于原生 ASPA 与 Path-End 机制.

3.2 路径篡改过滤实验

在保证路由源认证的前提下, 路径篡改行为主要包括路径内容的增加与删除. 根据攻击者对全局路由拓扑的掌握情况, 本实验把篡改分为有意与随机两类. 其中有意篡改为攻击者在对路径信息进行删除与增加后, 路径仍然“合法”, 仍能满足“Valley-Free”模型[12]; 而随机篡改则是对路径内容进行随机添加与删除, 篡改后的路径不构成有效链路, 即篡改部分与原有部分节点间无直接物理连接.

该实验选取上述收集器收集的真实路由路径信息与 relationship 静态路由拓扑信息[14]. 在真实路径信息的基础上, 进行有意与随机的路径增删篡改. 在攻击者

序列后选取同样的 AS 作为观测点, 统计在多种方案下观测点识别篡改行为的次数, 并在相同拓扑的情况下进行了多次试验. 平均数值统计如图 16.

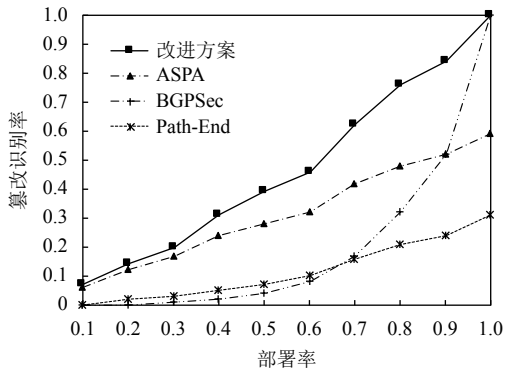

图 16 路径篡改识别

通过图 16 可知, BGPSec 方案是“严格”的方案, 在全局部署的情况下, BGPSec 路径保护力度最强, 但随着部署率降低, 即一旦路径中存在“断链”的情况, BGPSec 保护失效, 性能便会骤降. ASPA 方案根据转发关系进行验证, 所以有意篡改的路径能够绕过 ASPA 的验证, 因此即使在全量部署的情况下, ASPA 也无法对所有篡改行为进行都有效识别. Path-End 只对离源头最近一跳路径进行验证, 故其余复杂篡改均无法进行有效识别.

改进方案吸纳了 ASPA 与 BGPSec 方案的优势, 在保证路径合理的同时, 通过签名提升了路径篡改限制粒度, 故改进方案安全性能最强. 同时改进方案也尽力追求对路径“相对严格”的保护. 故改进方案在部署率为 1 的情况下, 改进方案安全性能接近于 BGPSec.

4 结束语

AS_PATH 是 BGP 协议中关键的路径属性之一, 路径验证也一直是路由安全领域研究的热点, 本文开始对路径验证现有解决思路及缺陷进行了阐述, 并提出了一种 RPKI 体系下的路径保护改进方案. 改进方案将授权数据与路径签名进行结合, 同时继承了 ASPA 与 BGPSec 优点, 能对路径信息进行有效保护, 实验表明, 在引入相对有限的时间与空间消耗的情况下, 改进方案在不同部署率均能对路径进行更为有效的保护. RPKI 的时代已经来临, 如何利用 RPKI 体系对 BGP 内容进行保护与验证, 仍有很大的探索与研究空间.

参考文献

1 Chang RKC, Lo M. Inbound traffic engineering for multi-homed ASes using AS path prepending. 2004 IEEE/IFIP Network Operations and Management Symposium (IEEE Cat. No. 04CH37507). Seoul: IEEE. 2004. 89–102. [doi: 10.1109/NOMS.2004.1317645]

2 McDaniel T, Smith JM, Schuchard M. Flexsealing BGP Against route leaks: Peerlock active measurement and analysis. arXiv: 2006.06576, 2020.

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 TG, *et al*. Working around BGP: An incremental approach to improving security and accuracy in interdomain routing. Proceedings of the Network and Distributed System Security Symposium. San Diego: DBLP, 2003. 156.

6 National Institute of Standards and Technology. NIST RPKI monitor. https://rpki-monitor.antd.nist.gov/. [2021-05-03].

7 Huston G, Bush R. Securing BGP with BGPsec. The Internet Protocol Forum. 2011, 14(2): 1–10.

8 Tanaka K, Yanai N, Okada M, *et al*. APAT: An application of aggregate signatures to BGPSEC. The 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Toulouse: IEEE, 2016.

9 Hohenberger S, Sahai A, Waters B. Full domain hash from (leveled) multilinear maps and identity-based aggregate signatures. 33rd Annual Cryptology Conference on Advances in Cryptology. Santa Barbara: Springer, 2013. 494–512.

10 Cohen A, Gilad Y, Herzberg A, *et al*. Jumpstarting BGP security with path-end validation. Proceedings of the 2016 ACM SIGCOMM Conference. Florianopolis: Association for Computing Machinery, 2016. 342–355.

11 Azimov A, Bogomazov E, Bush R, *et al*. Verification of AS_PATH Using the Resource Certificate Public Key Infrastructure and Autonomous System Provider Authorization. Internet Engineering Task Force, 2018: 1–8.

12 Sriram K, Montgomery D, McPherson D, *et al*. Problem definition and classification of BGP route leaks. RFC 7908, 2016.

13 Bush R, Turner S, Patel K. Router keying for BGPsec. RFC8635, 2019.

14 CAIDA. AS relationships. https://www.caida.org/catalog/datasets/as-relationships/. [2021-05-01].

15 Kühne M. Update on AS path lengths over time. https://labs.ripe.net/author/mirjam/update-on-as-path-lengths-over-time/. [2021-05-08].