一种改进的 BGP 路由源认证机制①

贾 佳[1,2], 延志伟[2], 耿光刚[2], 金 键[1]

[1](中国科学院计算机网络信息中心, 北京 100190)
[2](中国互联网络信息中心 互联网域名管理技术国家工程实验室, 北京 100190)

摘 要: 资源公钥基础设施(Resource Public Key Infrastructure, RPKI)是当前用于保护互联网码号资源分配真实性的技术. 作为一种支撑域间路由安全的体系, 它解决了边界网关协议(Border Gateway Protocol, BGP)缺乏路由源认证的问题. 然而当前 RPKI 体系中的依赖方(Relying Party, RP)与路由器数据同步机制可能会导致路由源授权(Route Originate Authorization, ROA)信息缺乏真实性和有效性, 并且不断查询缓存列表会带给路由器很大的性能负载. 据此, 本文提出一种改进的 BGP 路由源认证方案, 发送端路由器实时申请存储在 RP 中的 ROA 证书, 将其附加到 BGP update 报文中进行传输, 以待对等端路由器申请证书公钥对证书进行验证并完成路由源认证功能. 该方案将原来周期性更新路由器缓存列表机制改为路由器实时申请认证机制, 有效解决了 RP 与路由器数据同步可能导致的 ROA 存在错误的问题, 降低路由器查询缓存列表造成的路由器运行负载. 此外, 本文通过 Quagga 仿真实验表明该方案具有可行性, 并对该方案的适用情形进行了具体分析.

关键词: 边界网关协议; 资源公钥基础设施; 路由源授权; 安全机制; 前缀劫持

Improved Validation Mechanism of Route Origination in BGP

JIA Jia[1,2], YAN Zhi-Wei[2], GENG Guang-Gang[2], JIN Jian[1]

[1](Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190, China)
[2](National Engineering Laboratory for Naming and Addressing, China Internet Network Information Center, Beijing 100190, China)

Abstract: Resource public key infrastructure (RPKI) is a kind of technology which is used to protect the authenticity of Internet code number resources allocation and a kind of system of supporting inter-domain routing security which solves the problem of the lack of validation of route origination in BGP. However, it may result in the lack of authenticity and validity of ROA information due to the current data synchronism mechanism between the relying party of RPKI system and BGP routers. Meanwhile, it will bring a lot of performance load of BGP routes that query the cache lists continuingly. In this paper, we propose an improved method for route origination authentication. The sender routers real-timely apply for ROA certificates from RP and transmit them to the peer routers with the update message. Then the peer routers can apply for the public key to verify the certificates and verify the authenticity of the route originate. The verification mechanism is changed from updating the cache list periodically to real-time application for certification. It can effectively solve the problem that the ROA of the RP and the router data synchronization may be wrong, and reduce the running load of routes caused by querying the cache lists effectively. It is proved that the feasibility of the scheme using the simulation tool of Quagga and we make the detailed analysis for the applicable situation of two mechanisms.

Key words: BGP; RPKI; ROA; security mechanism; prefix hijacking

1 BGP安全分析

BGP 协议是当前互联网中唯一的域间路由协议, 其本身存在的安全漏洞会使整个互联网面临严峻的安全威胁[1-3], 比如路由劫持攻击[4-6]、路由泄露[7]等. 根据 BGP 协议规范, 路由器通过发送 update 报文来通告其他路由器自己发生变更的路由信息, 并且对接收到

① 收稿时间:2016-04-19;收到修改稿时间:2016-05-26 [doi: 10.15888/j.cnki.csa.005541]

的任何 update 报文都采取无条件信任的处理机制, 这种机制就给了攻击者可乘之机.

如图 1 所示, 路由器 R1 向 R2 发送的 update 报文中携带的 IP 地址 10.0.0.0/24 并不属于 R1, 而此 IP 地址真正的持有者 R4 也通过 R3 向 R2 发送路由信息. R2 会收到两个针对该 IP 地址的路由通告 update 报文, 其 AS_PATH 分别为 1 和 3 4. 根据 AS_PATH 路径最短原则[8], R2 优先选择 R1 到达 10.0.0.0/24. 由于 R2 没有任何认证机制证明消息的合法性和真实性, R2 中目的地为 10.0.0.0/24 的流量原本应该路由到 R4 中, 却被劫持到 R1 中, 造成前缀劫持攻击.

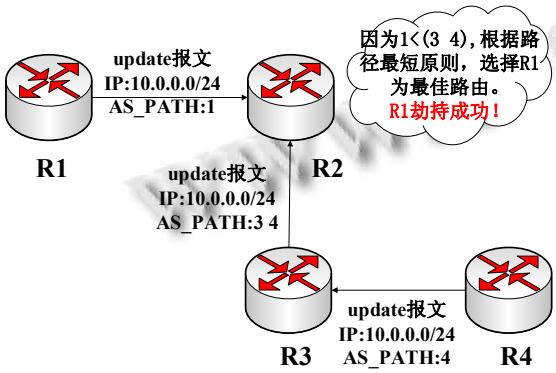

图 1 前缀劫持实例

前缀劫持攻击的结果可能会导致路由黑洞(black hole)和中间人攻击(man-in-the-middle attack), 甚至造成互联网的大规模瘫痪[9]. 前缀劫持的根本原因在于 BGP 协议缺乏一个安全可信的路由源认证机制. 为了弥补 BGP 存在的设计缺陷, 降低域间路由传播中的安全威胁. S-BGP(secure BGP)[10], SoBGP[11]等方法应运而生.

与此同时, IETF SIDR 工作组正在开发的 RPKI[12] 也为解决 BGP 安全问题提供了完整的设计思路. 基于 RPKI 的 BGP 路由安全机制不仅弥补了 S-BGP 计算开销大、部署困难的问题, 还解决了 soBGP 由于缺乏信任锚的地址授权认证体系导致的安全性显著下降的问题[8].

2 RPKI简介及存在的问题

2.1 RPKI 简介

RPKI 是一种公钥基础设施, 用来保障互联网基础码号资源(包括 AS 号, IP 地址)的可信分配和安全使用. RPKI 体系由三部分构成, 分别是资源公钥基础设施(RPKI)、数字签名对象和分布式数据仓库. 其中 RPKI 是本套体系中最核心的组成部分.

如图 2 所示, RPKI 的证书发布体系沿袭传统的地址分配逻辑, 按照互联网数字分配机构(Internet Assigned Numbers Authority, IANA)、地区性互联网注册机构(Regional Internet Registries, RIRs)、本地互联网注册机构(Native Internet Registries, NIRs)/互联网服务提供商(Internet Service Providers, ISPs)逐层向下发布认证权威(Certification Authority, CA)证书. 每一个最底层的资源持有者都拥有一段不可再细分的 IP 地址资源, 资源持有者用所属的 CA 证书继续签发 EE(End-Entity)证书, 用来对路由源 ROA 的信息进行签名[13]. ROA 包含了 IP 地址块以及资源持有者指定用于通告该段地址的 AS 号. 简单来说, 一个 ROA 就是地址所有者 ISP 授权某 AS 发起某 IP 前缀路由的担保, 从而对路由源进行合法性验证.

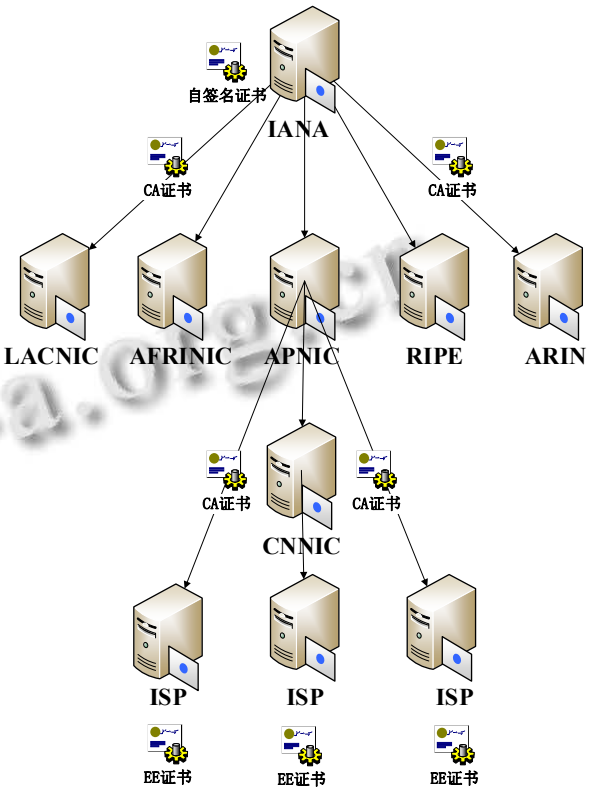

图 2 RPKI 资源分配架构图

如图 3 所示, RP 是连接 RPKI 和 BGP 路由系统的重要桥梁, RP 从 RPKI 体系中获取所有 ROA 证书并进

行验证, 将合法的 ROA 信息存储在 RP 数据库. 当 BGP 路由器向 RP 申请更新时, RP 将最新验证结果反馈给 BGP 路由器. BGP 路由器则根据验证结果构建自己的过滤表项和缓存列表. 当 BGP 路由器接收到来自对等端发送的 update 报文, 首先查询本地缓存列表 update 报文信息是否真实有效, 再进行路由选择.

如果在支持 RPKI 的情况下, 图 1 的路由器 R2 将会周期性地从 RP 获取所有的 ROA 信息, 当 R1 向 R2 发送 IP 地址为 10.0.0.0/24 的 update 报文时, R2 首先查询本地的路由器缓存列表, 检查 R1 是否具有通告当前 IP 地址的权利. 如果匹配正确, 则验证成功. 由此可见 RPKI 路由源认证功能有效地防御了前缀劫持攻击.

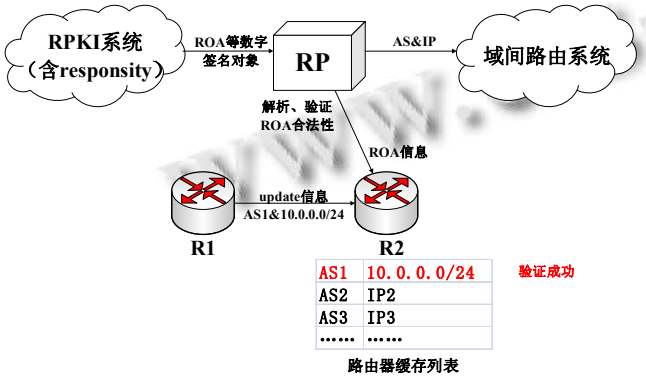

图 3　BGP 路由源认证

2.2 RPKI 存在的问题

在 RPKI 体系中, RP 与 BGP 路由器交互协议设计如图 4 所示[14], 每个路由器要与一个或者多个 RP 建立并保持连接, 以此来建立客户端/服务器关系. 每个路由器都将配置一个缓存列表, 用来接收从 RP 发送来的所有的 ROA 信息.

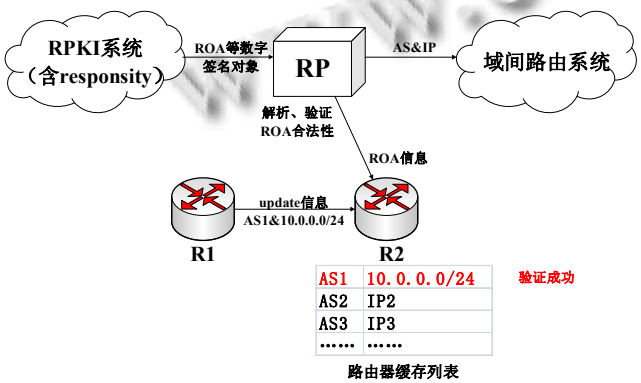

图 4　RP 与路由器交互机制

然而, BGP 路由器通过定期向 RP 发送更新请求机制, 来更新路由器缓存列表信息, 不论 RP 是否已经将数据库进行更新, 由此可能会对 BGP 路由器缓存列表中 ROA 信息的真实性和准确性产生影响. 同时, BGP 路由器缓存列表数量级非常大, 不断查询路由器缓存列表会加重路由器的运行负载.

由此可见, RP 与 BGP 路由器交互机制可能会导致 ROA 信息缺乏真实性和有效性, 并且对路由器造成很大的性能威胁.

3　改进的BGP路由源认证方案

3.1 改进方案介绍

为了解决 RP 与 BGP 路由器数据同步机制导致的安全和性能问题, 本文提出了一种改进的 BGP 路由源认证方案: 发送方将从 RP 申请的 ROA 证书附加到 update 报文中进行传输, 接收端路由器实时申请证书公钥对 ROA 证书合法性与真实性进行验证, 并用合法 ROA 信息对 update 报文中 IP 与 AS 信息进行路由源验证. 路由器验证成功后, 将合法的 ROA 信息存储到本地缓存列表并采用定期清空的处理机制. 该方案中提到的证书公钥经由 RP 验证可以保证其正确性.

此缓存列表数量级非常小并且清空缓存周期短, 其本身带来的查询消耗可以忽略不计, 旨在减小路由器实时申请和验证 ROA 证书带来的额外流量负载. 同时, 实时申请和定期清空缓存列表的机制保证了验证 ROA 信息的真实性和准确性, 有效解决了当前机制中 RP 与路由器数据同步可能导致的 ROA 存在错误的缺陷.

改进方案的详细设计流程如图 5 所示.

① 路由器 R1 向 RP 申请 ROA 证书.

② R1 将 ROA 证书作为 update 报文路径属性的一部分附加到 update 报文中.

③ R1 将 ROA 证书发送到对等端路由器 R2.

④ R2 接收到 ROA 证书后, 向 RP 申请 ROA 证书公钥并解密证书.

⑤ 通过查看证书所携带的 AS 号与 IP 前缀信息来验证当前 update 报文中的 AS 是否有通告当前 IP 的权利.

⑥ 如果验证正确则继续传递, 否则将此包丢弃.

⑦ BGP 路由器将申请到的 ROA 信息保存到本地缓存列表, 以待下一次验证. BGP 路由器缓存列表采用定期清空的机制, 以防止更新不及时导致的信息错

误.

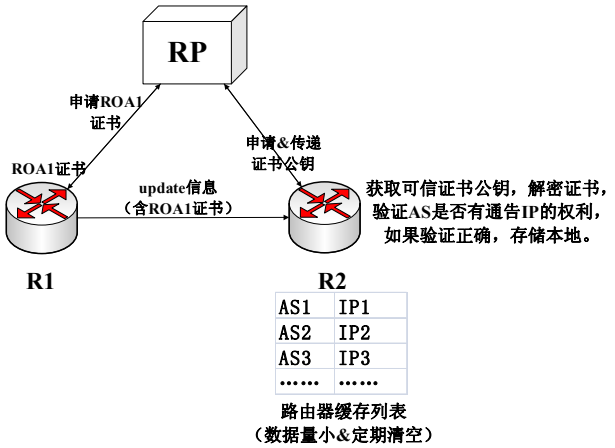

图 5 改进方案交互机制

3.2 改进方案可行性仿真过程

Quagga[15]是一种能够将 Linux 系统打造成一台功能完备的路由器的开源软件. 其能够同时支持 RIP、OSPF、BGP 等诸多 TCP/IP 协议. Quagga 拥有模块化设计、运行速度快、可靠性高等特性. 由于 Quagga 采用了模块化设计, 所以在其运行时要运行多个守护进程. 其中 zebra 进程用来更新内核的路由表, bgpd 进程则负责进行 BGP 协议的路由更新.

本文通过修改 Quagga 开源代码, 将静态的 ROA 信息(包括 AS 号, IP 地址及前缀)添加到 BGP 协议的 update 报文中. ROA 作为路径属性的一部分传递到对等端路由器, 并在对等端完成路由源认证. 当验证失败时, 错误日志中记录 ROA 信息无效并将此包丢弃.

本文提到的 Quagga 实验旨在验证将 ROA 证书附加到 update 报文中进行传输, 并在接收端进行验证的方案具有可行性, 可以将此方案部署到更复杂的路由拓扑结构.

实验步骤:

① 发送端从模拟的 RP 中获取 ROA 静态信息添加到 update 报文中.

② 将 ROA 信息通过 update 报文传递到对等端路由器.

③ 对等端路由器接收到更新信息后, 也从 RP 获取相应的 ROA 信息, 并将两者进行比较, 验证接收到的 ROA 信息是否真实有效.

④ 通过合法的 ROA 信息, 验证当前 AS 是否有通告当前 IP 前缀的权利, 即进行路由源认证.

仿真实验拓扑图如图 6 所示.

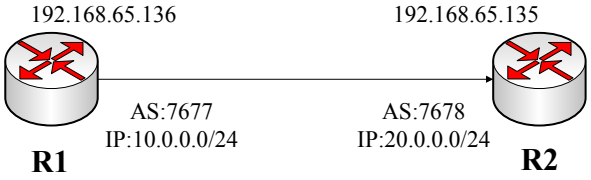

图 6 仿真拓扑图

3.3 改进方案可行性仿真结果

路由器 R2 接收到传递的 ROA 信息如图 7 所示.

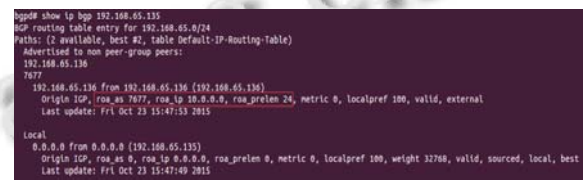

图 7 路由器 R2 信息接收图

当验证失败时, R2 路由器错误日志记录显示如图 8 所示.

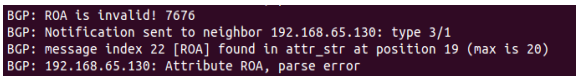

图 8 错误日志记录图

本文通过 Quagga 仿真技术模拟 BGP 路由器, 成功将静态的 ROA 信息传递到对等端, 并完成了路由源认证功能.

4 两种机制适用性分析

当前方案与改进方案对比分析如下:

① 当前机制如图 9 上侧所示: 假设从 RP 到路由器传输的<AS,IP>对象共有 m 个, 每个对象的平均传输速率为 0.628s/object[16]. 所以当前机制中 RP 与路由器的数据同步时间 $t_1=(0.628\times m)s$. 设 update 报文的传输速率为 v, 假如路由器发送、接收报文时间为 1s, 即 1s 发送、接收 v 个报文.

当 v=1/s(每秒有 1 个报文发送到路由器), 路由器缓存列表长度为 m(因为有 m 个对象, 每个对象为一行). 假设使用穷举法进行表查询, 查询每一行需要 1s, 验证时间为 1s. 则平均查找时间为 O(m), 由于最优情况查询时间为 1s, 最差情况查询时间为 ms, 所以平均查找时间为 $t_2=[(1+m)/2]s$, 验证时间 $t_3=1s$. 所以当 v=1/s 时, 所需时间为:

$$T_1 = t_1 + t_2 + t_3 = 0.628 \times m + (1+m)/2 + 1$$
$$= (1.128m + 1.5)s$$

当 v=n/s(每秒有 n 个报文发送到路由器), 所需时间为:

$$T_1 = t_1 + t_2 + t_3 = 0.628 \times m + [(1+m)/2] \times n + n$$
$$= [0.5m + 1.5]n + 0.628 \times m]s$$

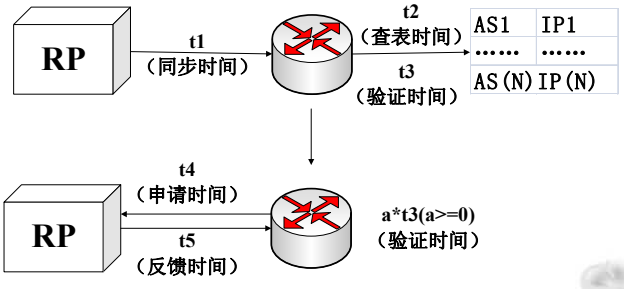

图 9　性能对比图

② 改进方案(不考虑本地存储ROA)如图9下方所示: 发送端路由器仍从 RP 获取 ROA 证书. 设路由器向 RP 申请 1 个 ROA 证书的时间为 $t_4 = 1s$, RP 向路由器反馈时间为 $t_5 = 1s$.

由于接收端路由器需要获取证书公钥并对证书进行解密, 所以改进方案中 ROA 证书验证时间相较于直接验证 AS 和 IP 需要消耗更长时间(不考虑申请公钥所导致的与 RP 的交互负载). 设对 ROA 证书验证时间为 $t_6 = (a \times t3)s(a \geq 0)$.

当 v=1/s, 所需时间为:

$$T_2 = (t_4 + t_5 + t_6)s = (t_4 + t_5 + a \times t3)s$$

当 v=n/s, 理想情况下为:

$$T_2 = [n(t_4 + t_5 + t_6)]s = [n(t_4 + t_5 + a \times t3)]s$$

假设发送端路由器每个 update 报文携带的 ROA 证书都需要重新申请, 由于其频繁访问 RP 数据库, 会加重路由器和 RP 的运行负载, 使得申请和反馈时间增长. 当速率为 n/s 时, 申请和反馈时间为 $[\beta \times n(t_4 + t_5)]s$, 并且假设 $\beta = bn(b \geq 0)$, 所以所需时间为:

$$T_2 = bn^2(t_4 + t_5) + an \times t3 = (2bn^2 + an)s$$

通过以上数据分析, 可以得出两种机制查询和验证时间分别为:

$$T_1 = [(0.5m + 1.5)n + 0.628 \times m]s$$
$$T_2 = (2bn^2 + an)s$$

设:

$$S = T_2 - T_1 = 2bn^2 + an -$$
$$[(0.5m + 1.5)n + 0.628 \times m]$$
$$= 2bn^2 + (a - 0.5m - 1.5)n$$
$$- 0.628 \times m$$

因为

$$\Delta = (a - 0.5m - 1.5)^2 -$$
$$4 \times 2b \times (-0.628 \times m) > 0$$

所以, T1 与 T2 有两个交点, 由于 m>=0, a>=0, b>=0, 所以 T1 与 T2 有一个交点, 如图 10 所示.

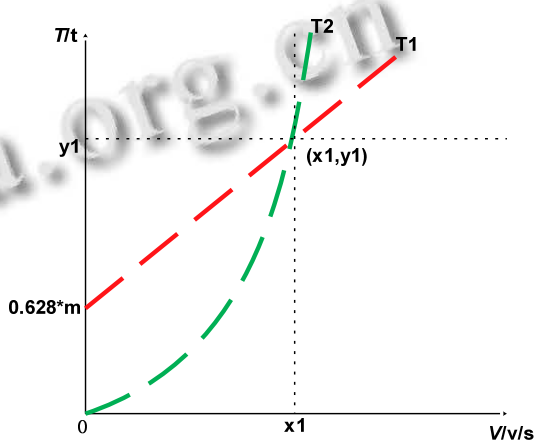

图 10　时间对比图

综上所述:

$$x1 = [-a + 0.5m + 1.5] + \Delta^{1/2}]/4b$$

当 v<x1 时, 由于当前方案中数据同步和查询缓存列表耗时大, 所以改进方案完成路由源认证所需要的时间更短. 当 v>x1 时, 由于 RP 与路由器交互次数过于频繁导致时间延迟, 超过了路由器数据同步的时间, 这种情况下当前机制所需的时间更短.

5　结论

RPKI 针对 BGP 协议存在的安全缺陷, 通过引进 ROA 证明源 AS 对某 IP 前缀拥有通告的权利, 对路由源进行认证, 从而有效解决了 BGP 协议中对源认证缺失的安全问题. 但是在路由源认证模块中, 由于路由器要定期更新本地的路由器缓存列表, 从而导致 RP 数据库与路由器缓存列表在数据同步方面存在安全隐患和性能缺陷. 路由器缓存列表更新周期直接影响着缓存列表中 ROA 信息的正确性与真实性.

本文在此基础上, 提出了一种改进的 BGP 路由源认证方案. 将从 RP 获取的 ROA 证书附加到 update 报文中, 接收端路由器从 RP 申请可信的 ROA 证书公钥

并进行解密, 与 update 报文信息进行比较从而验证路由源信息的真实性. 本文通过 Quagga 仿真技术模拟 BGP update 报文传输, 验证静态的 ROA 信息附加到 update 报文的方案切实可行, 同时分析了当前方案和改进方案的适用情况和时间开销.

参考文献

1 Kuhn R, Sriram K, Montgomery D. Border gateway protocol security[Technical Report], 800-54, Gaither-sburg: NIST, 2007.

2 Murphy S. BGP security vulnerabilities analysis. RFC 427 2, 2006.

3 Nordstrom O, Dovrolis C. Beware of BGP attacks. ACM SIGCOMM Computer Communication Review, 2004, 34 (2): 1–8.

4 Andy G. Hacker Redirects Traffic from 19 Internet Providers to Steal Bitcoins. http://www.wired.com/2014/08/isp-bitcoin-theft/. 2014.

5 Matsuzaki Y. Prefix hijacked. https://conference.apnic.net /data/41/apricot-2016-maz-hijack_1456100828.pdf. 2016.

6 Chika Y. BGP Hijack Issue in 2015. https://conference.apnic.net/data/41/janog37-chika-rev7-en_1455078267_1456002602.pdf. 2016.

7 Massive route leak causes Internet slowdown. http://www.bgpmon.net/massive-route-leak-cause-internet-slowdown/#comments-wrap.

8 Matthew C, Jennifer R. BGP routing policies in ISP networks. IEEE Network, 2005.

9 黎松,诸葛建伟,李星.BGP 安全研究.软件学报,2013,24(1): 121–138.

10 Secure BGP project (S-BGP).2004. http://www.ir.bbn.com/sbgp/.

11 White R. Securing BGP through sec ure origin BGP (SoBGP). The Internet Protocol Journal, 2003, 6(3): 15–22.

12 Lepinski M, Kent S. An infrastructure to support secure Internet routing. RFC 6480, 2012.

13 Huston G, Michaelson G. Validation of route origination using the resource certificate public key infrastructure (PKI) and route origin authorizations (ROAs). IETF RFC 6483, 2012.

14 Bush R, Austein R. The resource public key infrastructure (RPKI) to router protocol. RFC 6810, 2015.

15 Quagga Routing Suite. http://www.ourg/quagga /.

16 Osterweil E, Manderson T, White R, et al. Sizing estimates for a fully deployed RPKI. Verisign Labs, TR, 2012, 1120005.