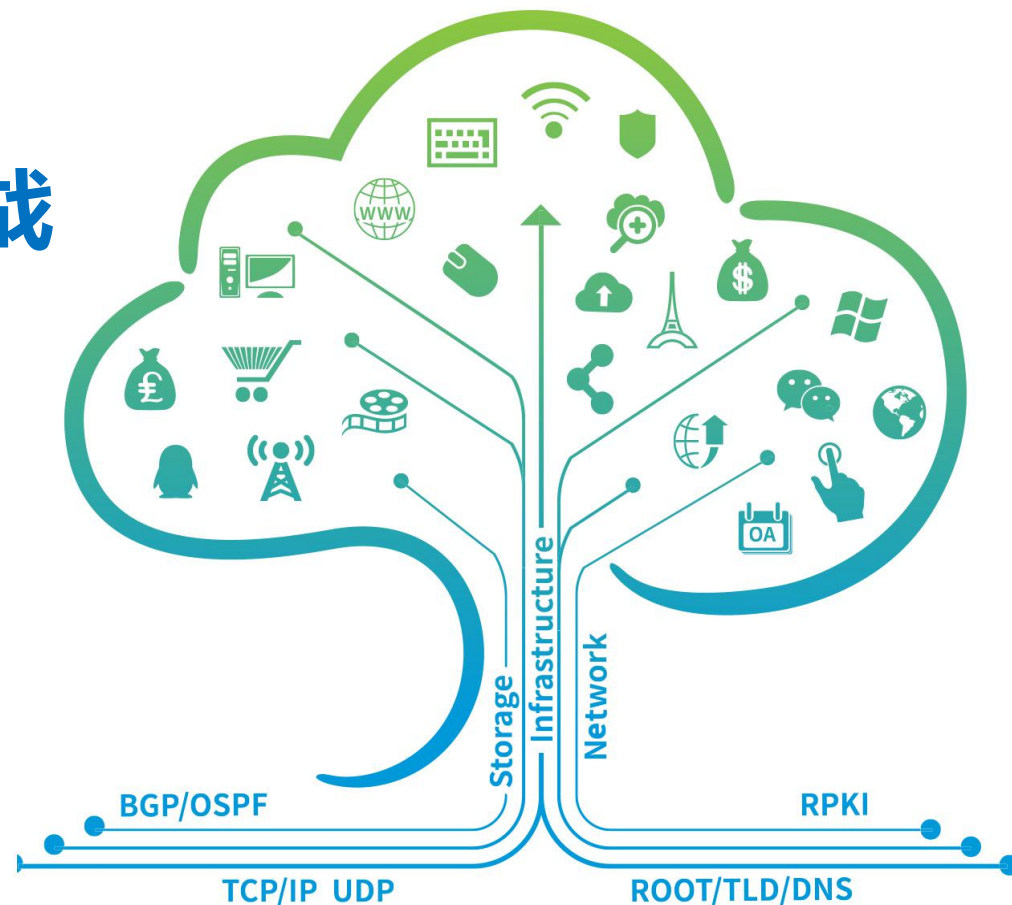


RPKI依赖方系统部署与运维挑战

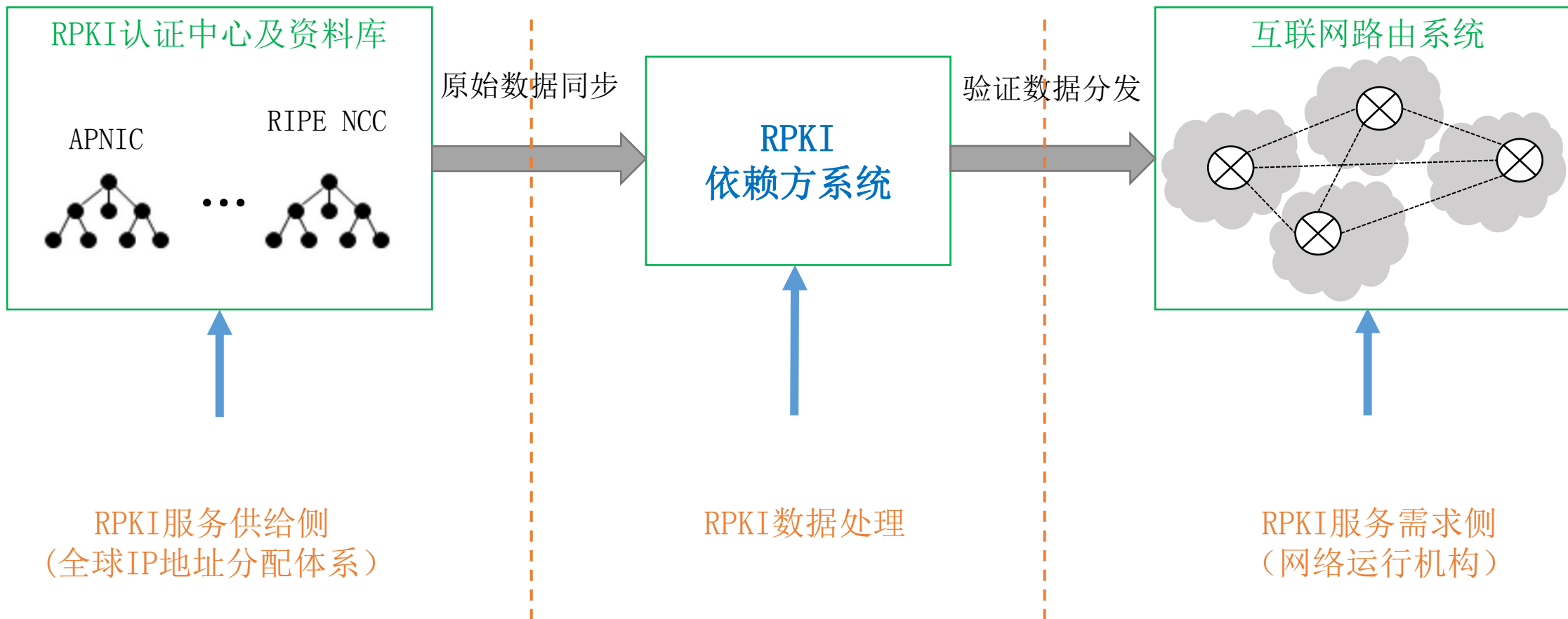
马迪

互联网域名系统国家工程研究中心

madi@zdns.cn



RPKI依赖方系统是连接供给和需求之间的桥梁



RPKI依赖方系统技术标准条款汇总：RFC8897



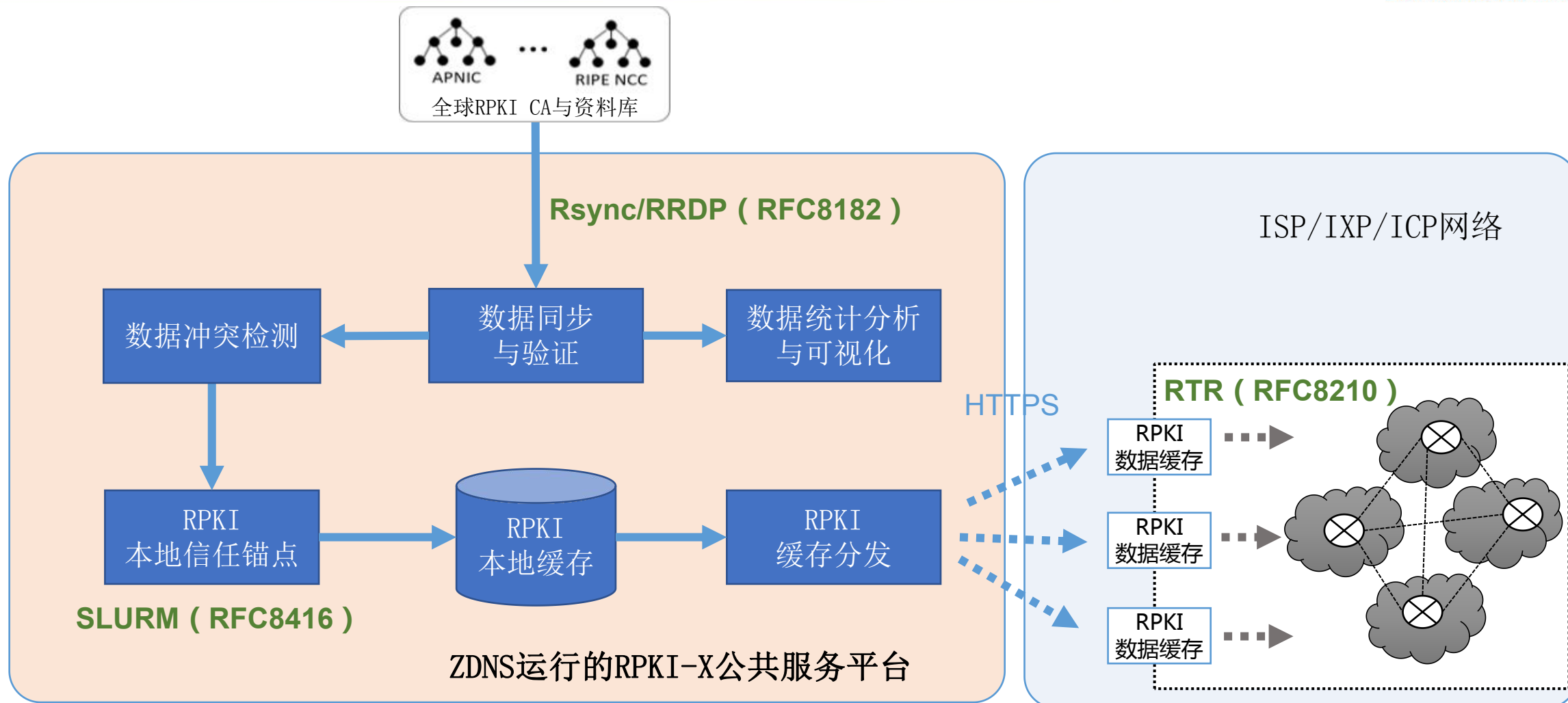
互联网域名系统国家工程研究中心

Stream: Internet Engineering Task Force (IETF)
RFC: 8897
Category: Informational
Published: September 2020
ISSN: 2070-1721
Authors: D. Ma S. Kent
ZDNS Independent

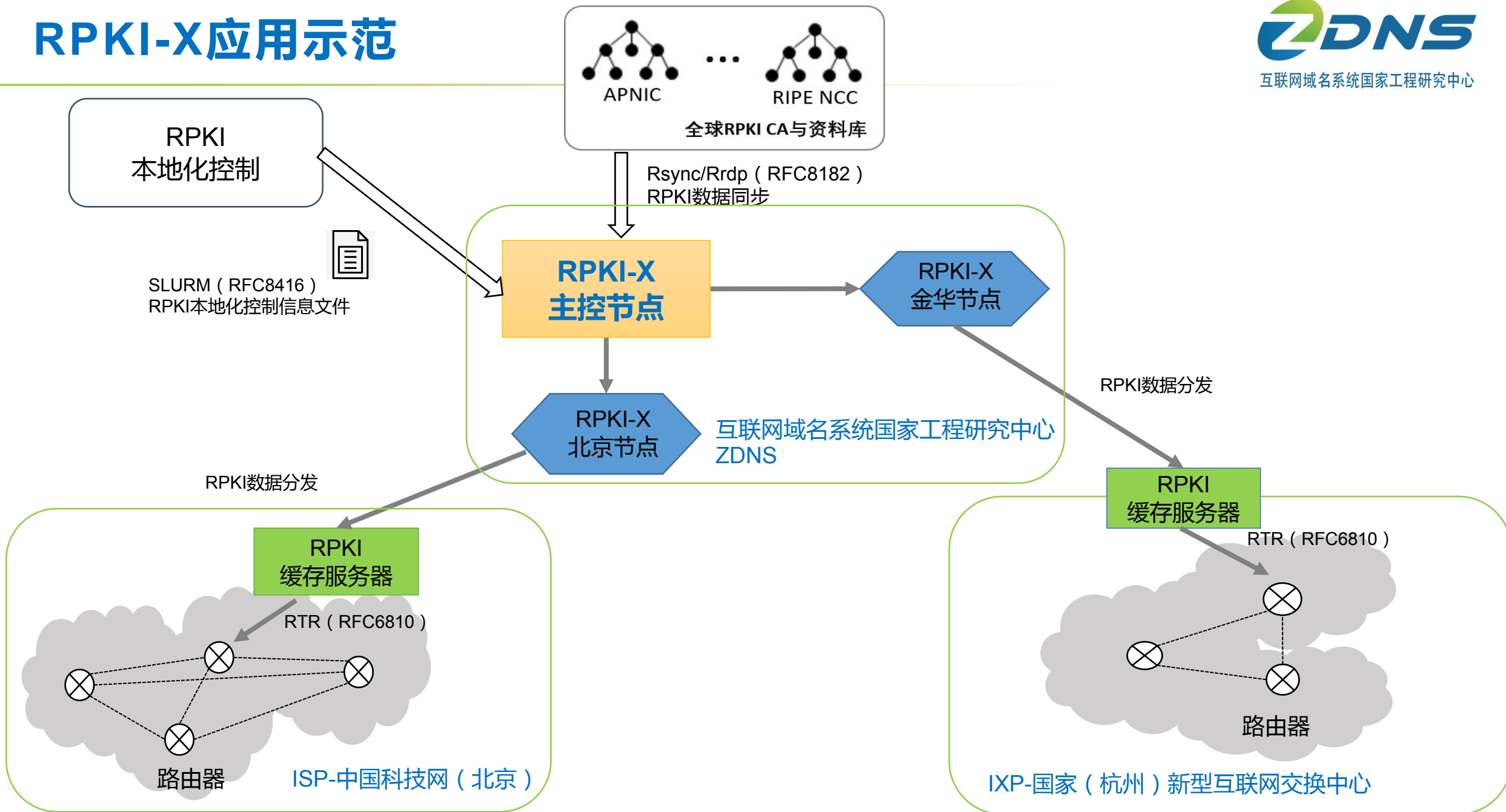
RFC 8897 Requirements for Resource Public Key Infrastructure (RPKI) Relying Parties

2. Fetching and Caching RPKI Repository Objects
 - 2.1. TAL Configuration and Processing
 - 2.2. Locating RPKI Objects Using Authority and Subject Information Extensions
 - 2.3. Dealing with Key Rollover
 - 2.4. Dealing with Algorithm Transition
 - 2.5. Strategies for Efficient Cache Maintenance
3. Certificate and CRL Processing
 - 3.1. Verifying Resource Certificate and Syntax
 - 3.2. Certificate Path Validation
 - 3.3. CRL Processing
4. Processing RPKI Repository Signed Objects
 - 4.1. Basic Signed Object Syntax Checks
 - 4.2. Syntax and Validation for Each Type of Signed Object
 - 4.2.1. Manifest
 - 4.2.2. ROA
 - 4.2.3. Ghostbusters
 - 4.2.4. Verifying BGPsec Router Certificate
 - 4.3. How to Make Use of Manifest Data
 - 4.4. What To Do with Ghostbusters Information
5. Distributing Validated Cache
6. Local Control
7. Security Considerations

RPKI依赖方系统的云服务实践：RPKI-X



RPKI-X应用示范



影响RPKI依赖方系统运行效能的四对矛盾

RPKI依赖方系统的核心目标：将RPKI数据尽可能快速、完整、准确地从供给侧扩散至需求侧。

- ✓ **矛盾1**：RPKI资料库（发布点）越来越多，与实时感知全球RPKI数据更新之间的矛盾。
- ✓ **矛盾2**：RPKI数据对象越来越多，与快速同步全球RPKI数据之间的矛盾。
- ✓ **矛盾3**：RPKI认证链越来越复杂，与快速构建全球RPKI数据验证路径之间的矛盾。
- ✓ **矛盾4**：RPKI依赖方系统越来越集中化，与路由器快速获得RPKI验证数据之间的矛盾。

化解RPKI依赖方系统运行效能矛盾的方法

矛盾在“RPKI基本原理范畴”的普遍性

模块组件设计

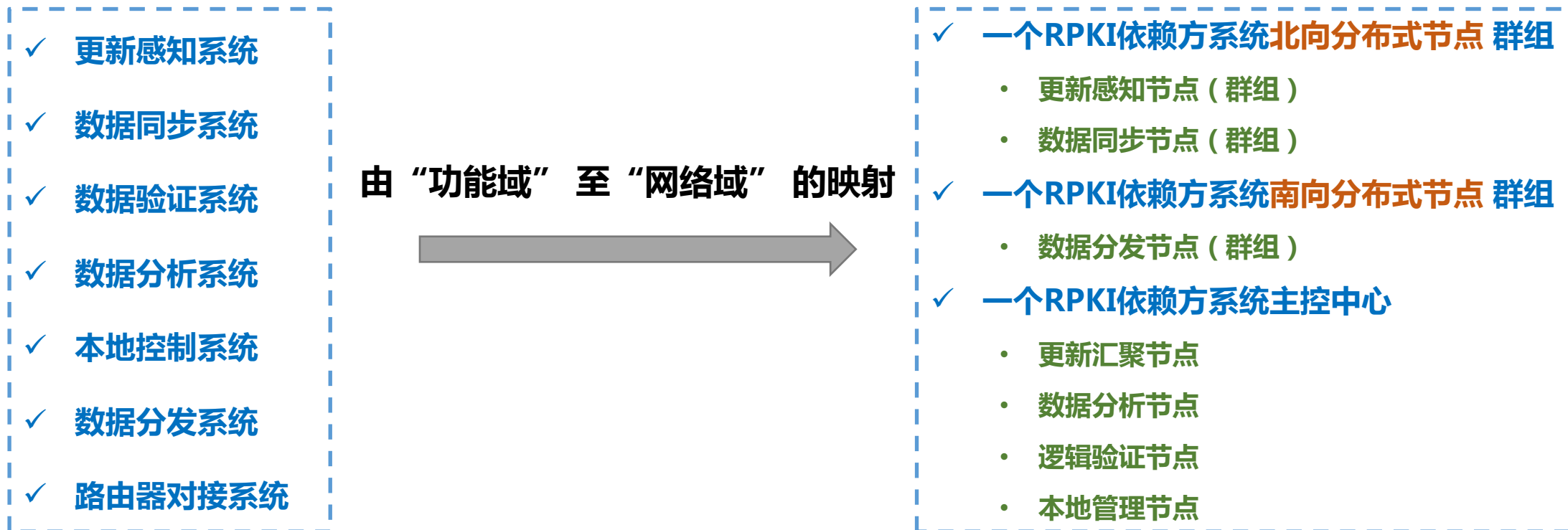
矛盾在“网络互联互通特征范畴”的特殊性

部署方案设计

RPKI依赖方系统应当有哪些组件，
组件如何在网络上分布及以何种
逻辑关系分布。

可扩展的RPKI依赖方系统：功能组件正交 + 编排机制因应网络规模和特征差异

可扩展的RPKI依赖方系统部署机制在“**网络互联互通特征范畴**”的任务：
面向规模网络的一般特征，在RPKI依赖方系统的“**组件颗粒度**”上实施功能模块的分布设计。

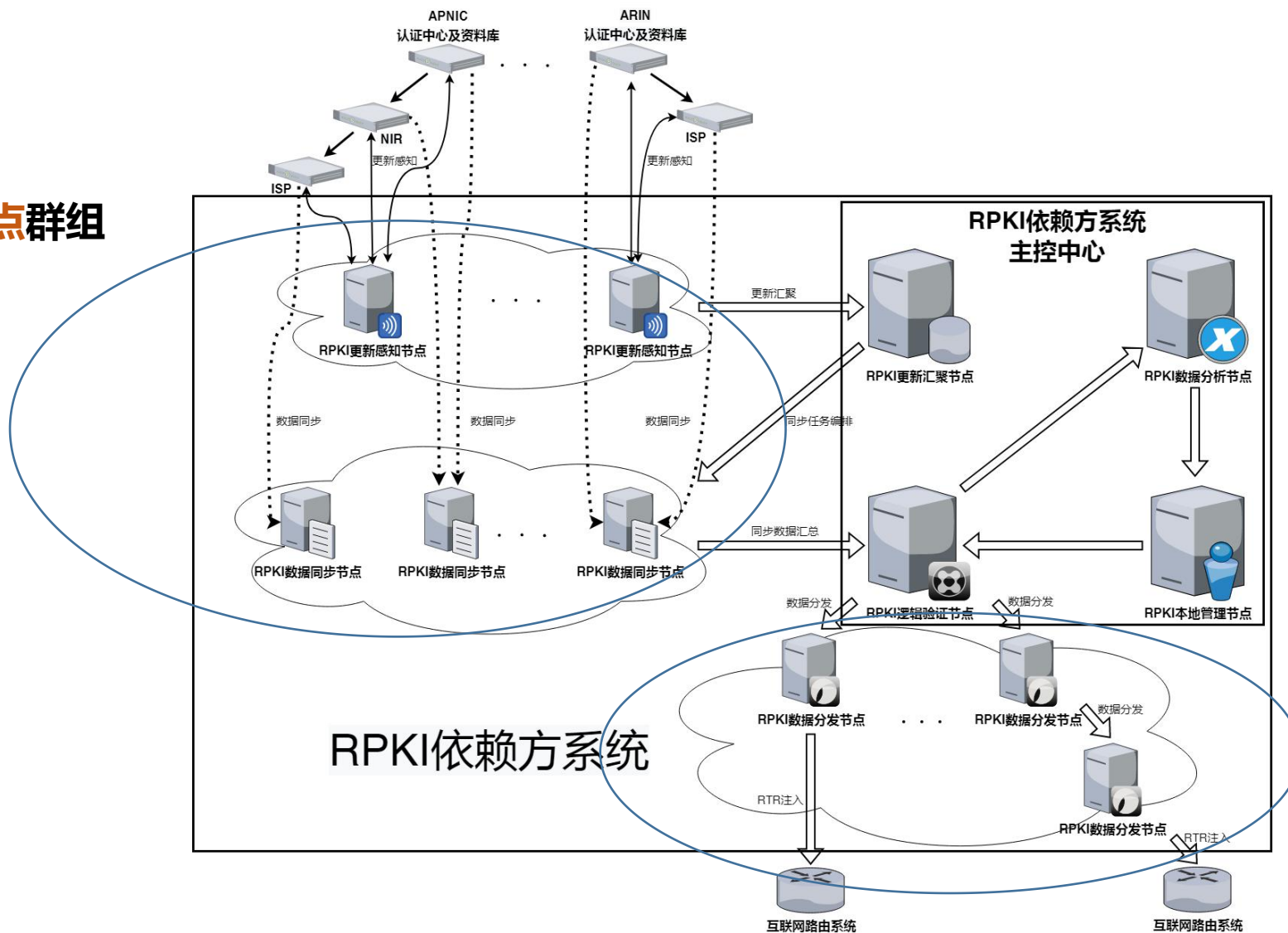


RPKI依赖方系统组件在网络上的编排机制 2/2



互联网域名系统国家工程研究中心

北向分布式节点群组



南向分布式节点群组

让网络根基更安全 更高效 更智能

让同步更快：高性能联合并发同步机制

关键问题：RPKI数据同步瓶颈，更新不及时，存在单点风险。

影响RPKI依赖方系统运行效能的四对矛盾

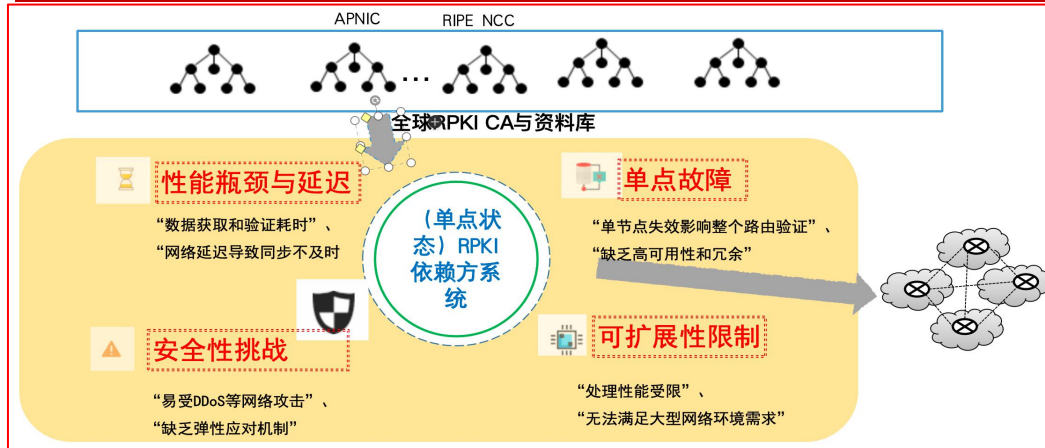
- ✓ 矛盾1: RPKI资料库（发布点）越来越多，与实时感知全球RPKI数据更新之间的矛盾。
- ✓ 矛盾2: RPKI数据对象越来越多，与快速同步全球RPKI数据之间的矛盾。
- ✓ 矛盾3: RPKI认证链越来越复杂，与快速构建全球RPKI数据验证路径之间的矛盾。
- ✓ 矛盾4: RPKI依赖方系统越来越集中化，与路由器快速获得RPKI验证数据之间的矛盾。

项目	组织	架构
Routinator	NLnet Labs	单体
Validator3	RIPE NCC	单体
OctoRPKI	Cloudflare	单体
Fort	NIC.MX	单体
rpki-prover	Mikhail Puzanov	单体

现网的 RPKI 依赖方同步链路，收敛速度慢、更新不及时；单点瓶颈突出；分布式调度缺乏有效算法



跨洲同步：影响同步效率，导致更新周期过长

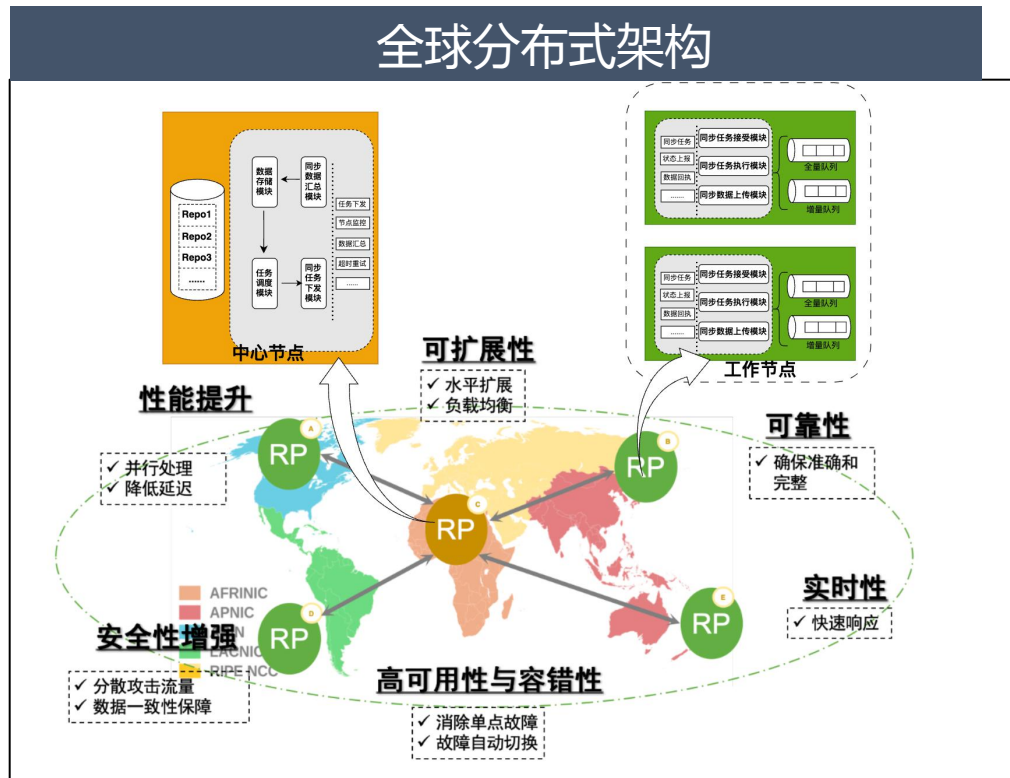


单体架构的矛盾与局限：单体性能、可拓展性存瓶颈

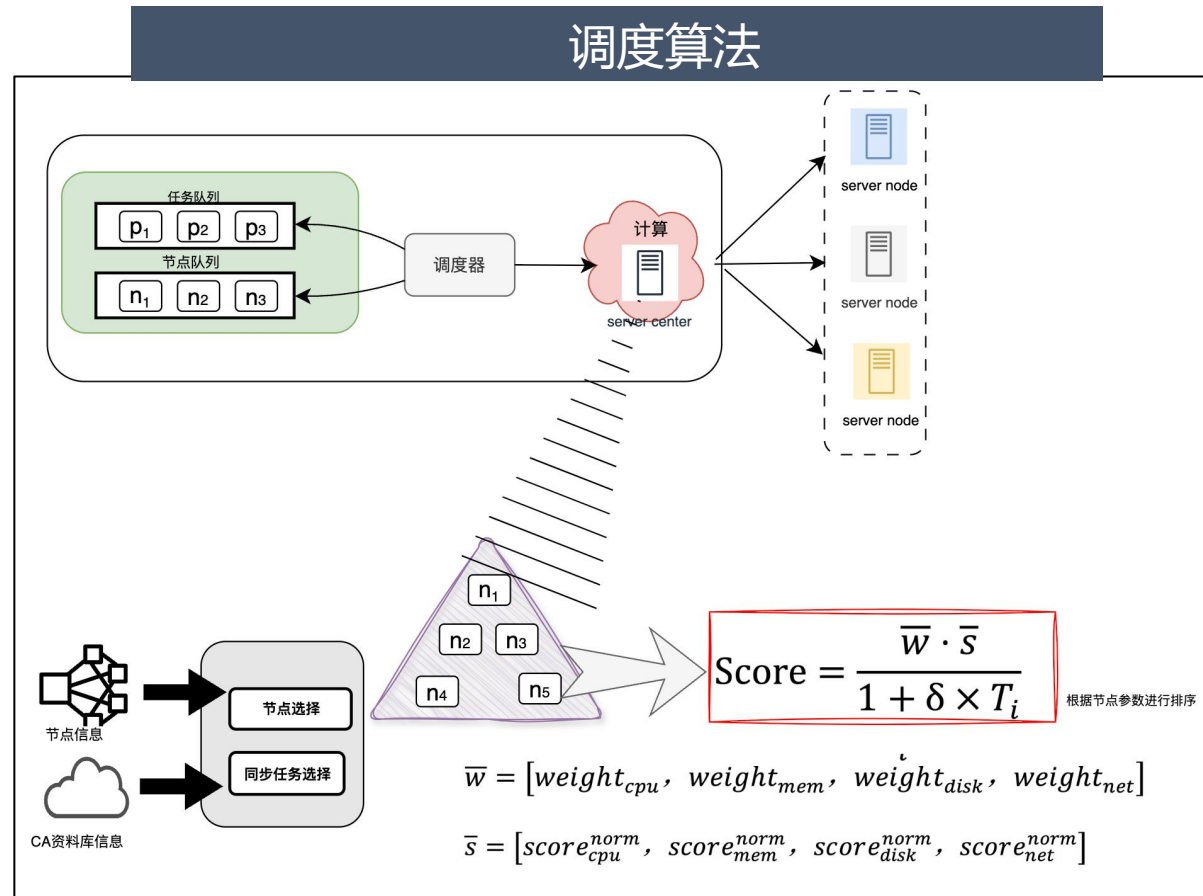
目标：
分布式并发同步

让同步更快：高性能联合并发同步机制

技术路线：设计高性能 RPKI 数据同步机制，提出并实现多种任务调度算法。



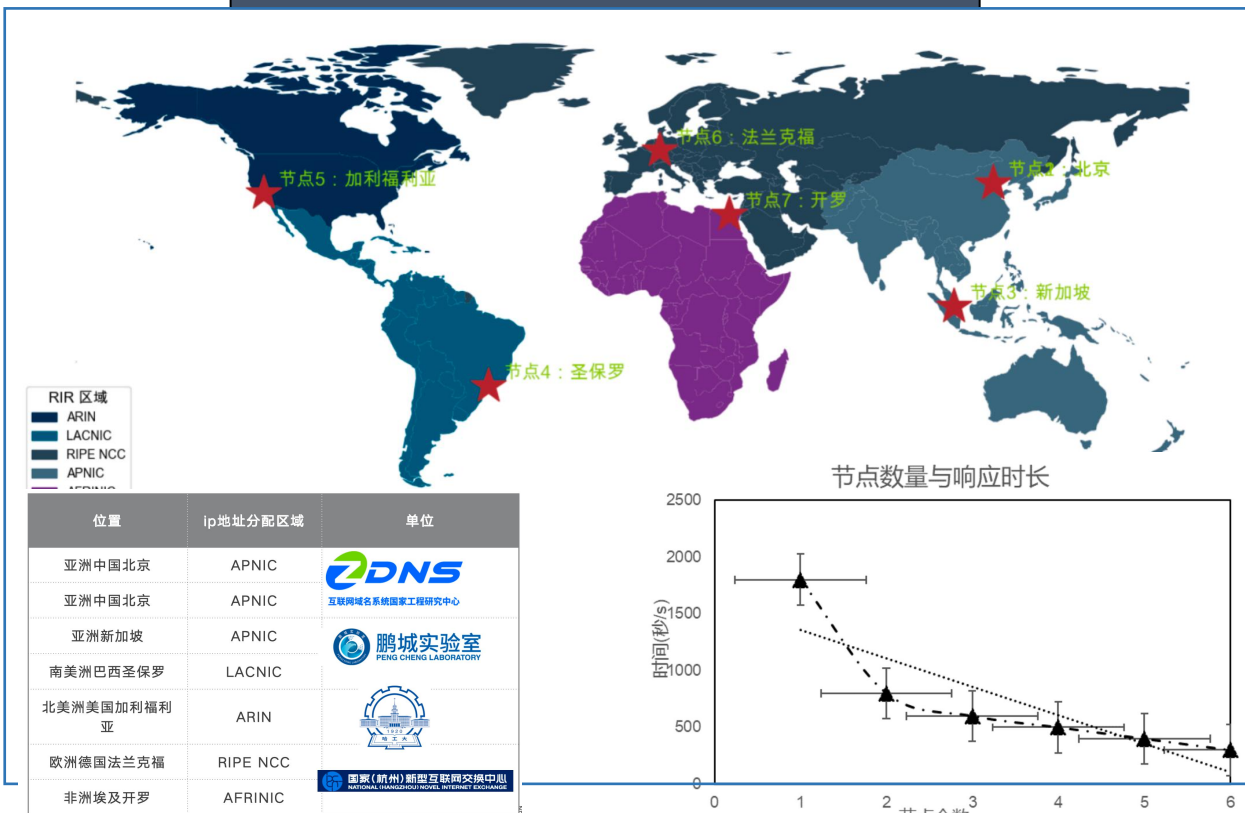
全球分布式架构，全面提升RPKI同步的性能、可靠性与实时性



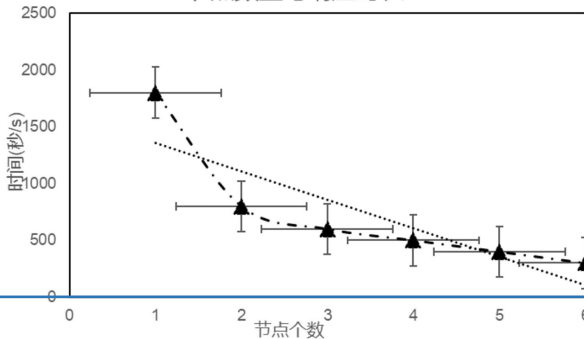
让同步更快：高性能联合并发同步机制

阶段性成果：部署了全球分布式RPKI数据同步系统，设计实现了并发同步机制及配套的动态调度算法，基本实现了秒级的RPKI增量同步。

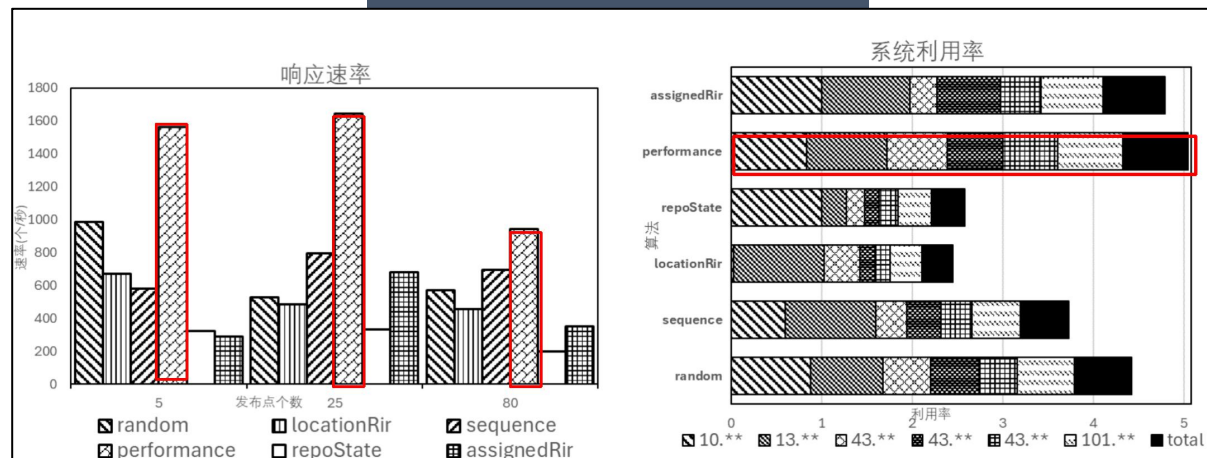
全球分布式试验床



节点数量与响应时长



调度算法多维度对比



动态调度算法显著提升同步性能与系统利用率

**“增量同步”时间约75%控制在1分钟以内，
92%控制在2分钟以内，基本实现秒级同步更新。**

显著缩短同步时长

让验证更快：高性能证书链验证算法

关键问题：RPKI证书链验证效率低、更新不及时。

- 现有 RPKI 数据对象验证遵循 RFC6487 的验证机制，有新对象更新，会重新加载并验证所有数据对象，以确保层级结构下复杂的资源包含关系不被破坏，这种验证方式带来了严重的性能负担

数据量剧增

	31/12/2021	31/12/2022
Total cache size (KiB)	996,216	1,240,572 (+24%)
Total number of files (objects)	192,503	242,969 (+26%)

	2023-12-31	2024-12-31	Growth
Total cache size (KiB)	1,546,728	2,021,784	(+31%)
Total number of files (objects)	309,802	415,384	(+34%)

部署早期数据量小，全局验证尚可，部署扩大数据量爆炸，全局验证难以承受

验证方式（全局验证 vs 增量验证）

Reduce CPU usage per tree validation

- Incremental tree validation
 - Validate fully only newly downloaded objects
 - Be smart about which manifest children to revalidate
 - For already validated objects only re-check validity time

Reduce CPU usage per tree validation

- Pro: about 9-10 times less CPU usage for tree validation
- Cons:

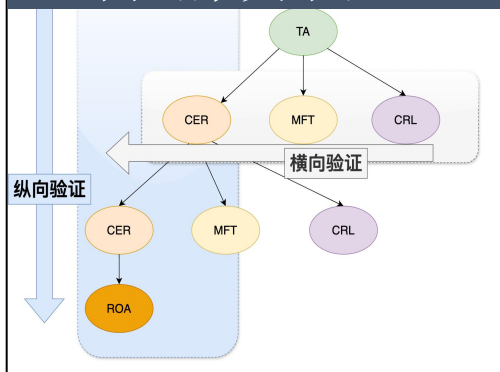
全局验证意味着高开销
增量验证则可控

让验证更快：高性能证书链验证算法

技术路线：面向RPKI数据之间的关系，设计基于RPKI数据关联关系的局部验证算法。

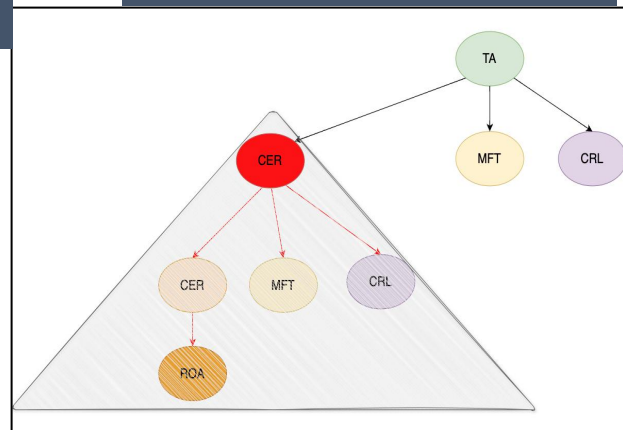
- 快速分析不同RPKI数据对象之间的纵向认证关系和横向管控关系、以及增量更新时变动的数据项，通过缩小待验证RPKI数据对象集合，从而提高验证效率

RPKI数据对象的横纵向约束关系验证



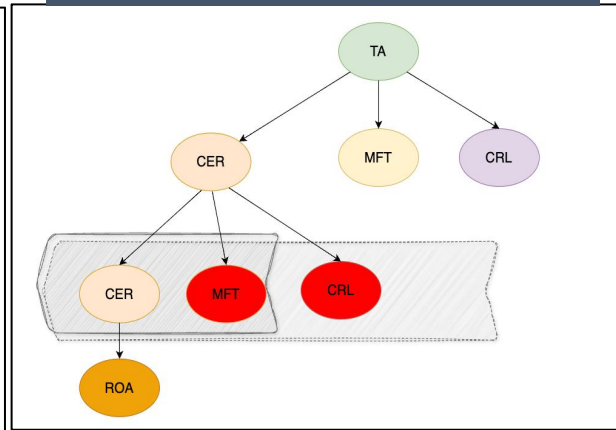
RPKI数据对象的横纵向约束关系验证，包括：自身验证、横向验证和纵向验证

更新CER文件



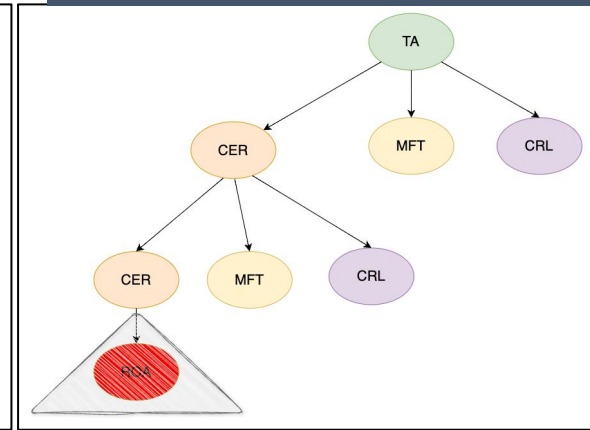
情况一：更新CER文件：验证并更新对应CER文件，同时验证并更新其签发的CER/CRL/ROA/MFT文件

更新CRL、MFT文件



情况二：更新MFT或CRL文件：验证并更新对应MFT或CRL文件，同时验证并更新同级的CER、MFT或CRL文件

更新ROA文件

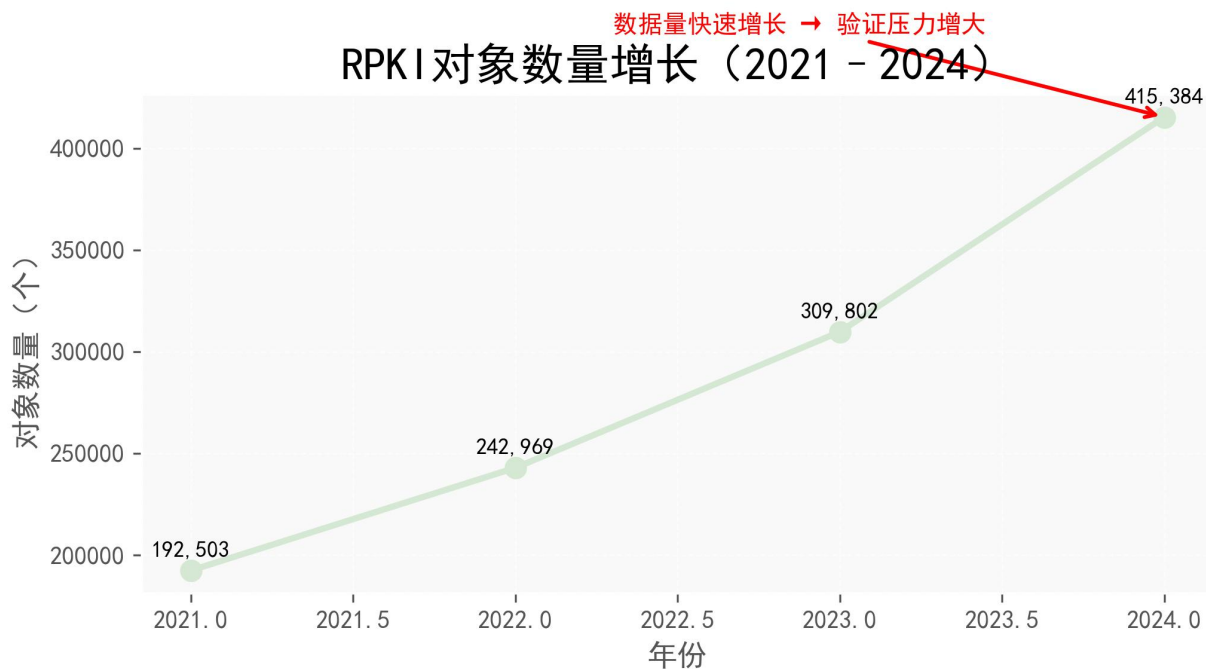


情况三：更新ROA文件：验证并更新对应ROA文件即可

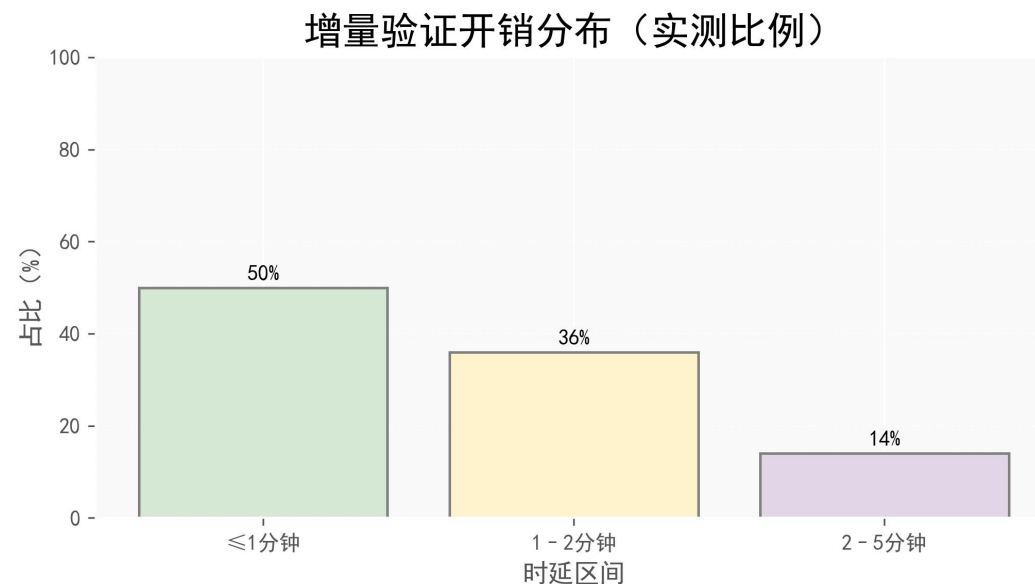
让验证更快：高性能证书链验证算法

阶段性成果：突破RPKI证书链验证算法的关键技术，实现了基于智能按需验证的高性能证书链验证算法，在全球RPKI分布式实验床应用中得到了应用。

RPKI数据增长趋势



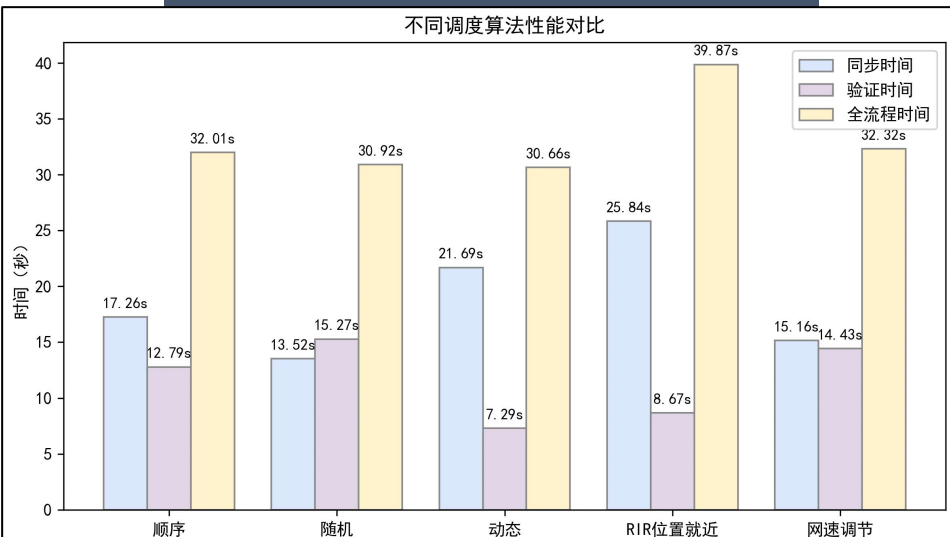
降低RPKI数据验证处理时间



全球分布式节点测试结果

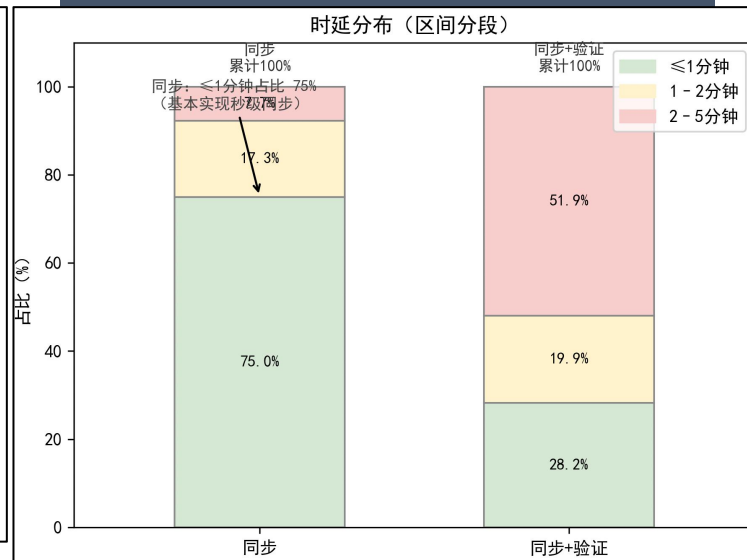
不同调度算法性能对比

不同调度算法性能对比



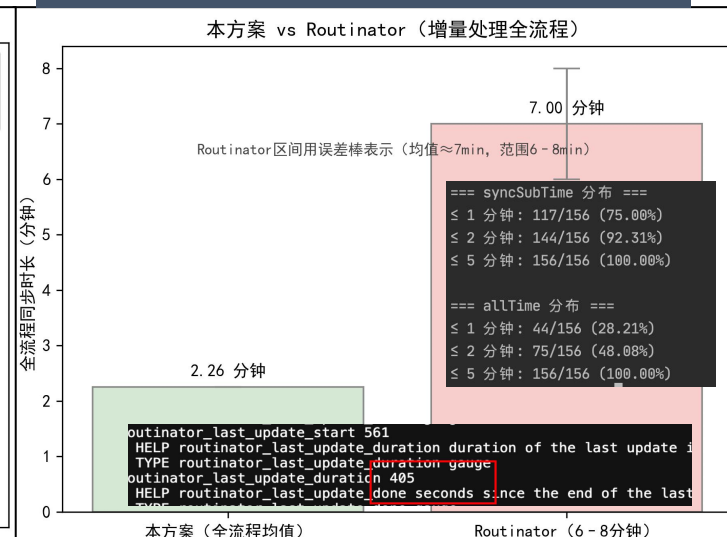
各阶段时延分布

时延分布 (区间分段)



横向对比

本方案 vs Routinator (增量处理全流程)



增量同步已基本实现秒级更新

性能优于Routinator

“增量同步+验证”时间，约28%控制在1分钟以内，约48%控制在2分钟以内，100%控制在5分钟以内，超过Routinator 6~8分钟的性能。

构建可扩展的RPKI依赖方系统部署机制

Scaling RPKI Relying Party System



马迪/MA Di

(互联网域名系统国家地方联合工程研究中心, 中国 北京 100102)
(Internet Domain Name System National Engineering Research Center,
Beijing 100102, China)

DOI: 10.12142/ZTETJ.202301008

网络出版地址: <https://kns.cnki.net/kcms/detail/34.1228.TN.20230227.1253.004.html>

网络出版日期: 2023-02-27

收稿日期: 2022-12-15

摘要: 互联网号码资源公钥基础设施 (RPKI) 依赖方系统是各类网络运行机构开展 RPKI 应用实践的一个关键环节。RPKI 依赖方系统的研发和部署, 既需要处理 RPKI 核心功能的“普遍性”问题, 又需要兼顾网络互联互通特征的“特殊性”问题。相关解决方案需要考虑 RPKI 依赖方系统应当有哪些组件, 各个组件如何在网络上分布, 以及以何种逻辑关系分布。面向 RPKI 依赖方系统的核心功能, 梳理了影响 RPKI 依赖方系统运行效能的 4 对矛盾, 并提出了一种可扩展的 RPKI 依赖方系统部署机制, 包含软件层面的解耦机制和硬件层面的部署机制。

Workgroup: SIDROPS
Internet-Draft: draft-madi-sidrops-rp-dssn-01
Published: 22 February 2025
Intended Status: Informational
Expires: 26 August 2025

D. Ma
ZDNS
Y. Li
CNIC-CAS
Y. Zhang
Peng Cheng Laboratory
S. Zhang
China Mobile

RPKI Relying Party with Distributed Systems of Synchronization Nodes

Abstract

This document describes a current practice of establishing an RPKI relying party with distributed systems of synchronization nodes.

计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
2025, 34(4):125-135 [doi: 10.15888/j.cnki.csa.009818] [CSTR: 32024.14.csa.009818]
©中国科学院软件研究所版权所有。

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

RPKI 依赖方分布式同步系统^①

邵 晴, 包 卓, 马 迪

(互联网域名系统北京市工程研究中心有限公司, 北京 100102)

通信作者: 包 卓, E-mail: baozhuo@zdns.cn



摘 要: 近年来互联网号码资源公钥基础设施 (resource public key infrastructure, RPKI) 部署率逐年上升, 这对依赖方软件原有单体同步的架构在性能与效率方面提出了挑战-其架构设计需要进行重新考量, 以适应 RPKI 技术的演进。本文对 RPKI 同步任务进行了梳理与分析, 并基于此设计了一个 RPKI 依赖方任务同步系统。相比单体架构, 该系统的分布式架构有着较高的同步性能及节点容错性。同时, 本文为该系统设计了多种调度算法, 同时, 为进一步优化该系统性能, 本文对这些调度算法及任务调度策略进行了多组对照分析实验。从实验结果看, 该分布式系统在大作业优先 (large job first, LJF) 任务调度策略下的动态调度算法表现性能最佳。

Workgroup: SIDROPS
Internet-Draft: draft-madi-sidrops-rush-08
Published: 21 April 2023
Intended Status: Standards Track
Expires: 23 October 2023

D. Ma
ZDNS
H. Yan
CNCERT
M. Aelmans
Juniper Networks
S. Zhang
NNIX

RPKI validated cache Update in SLURM over HTTPs (RUSH)

Abstract

This document defines a method for transferring RPKI validated cache update information in JSON object format over HTTPs.

- ✓ **关键问题**：RPKI依赖方系统连接RPKI供给侧和RPKI需求侧，是各类网络运行机构开展RPKI应用实践的一个关键环节。使用RPKI依赖方系统实施路由认证，不仅是简单的软硬件集成，更需要设计能够“因地制宜”涵盖功能编排、部署方法及运行机制的一揽子解决方案。
- ✓ **应对对策**：研究RPKI依赖方系统应当有哪些组件，各个组件如何在网络上分布及以何种逻辑关系分布，分析面向RPKI数据的分布式发布机制（宏观特征）和RPKI数据的牵连验证关系（微观特征）。
- ✓ **当前成效**：突破了RPKI依赖方核心技术，研发了RPKI依赖方关键系统及其部署机制，全面提升了RPKI数据同步、验证2个制约RPKI数据效用的关键环节。

让网络根基更安全 更高效 更智能

Thanks !

欢迎关注官方微信
了解更多行业信息

