

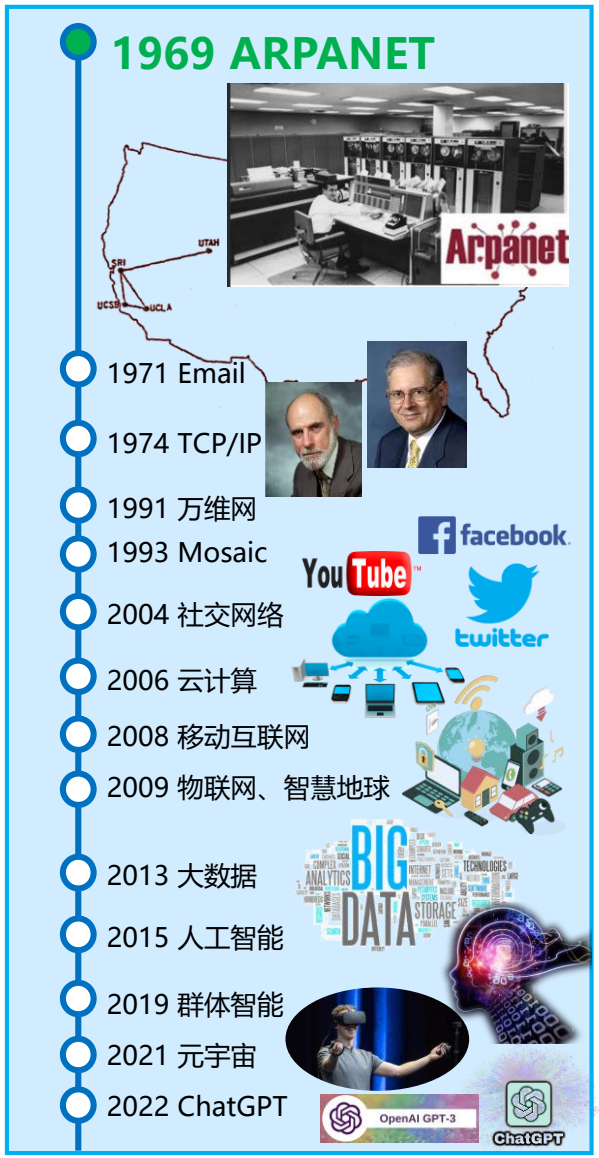
通过可验证的转发承诺实现域间安全路由与数据转发

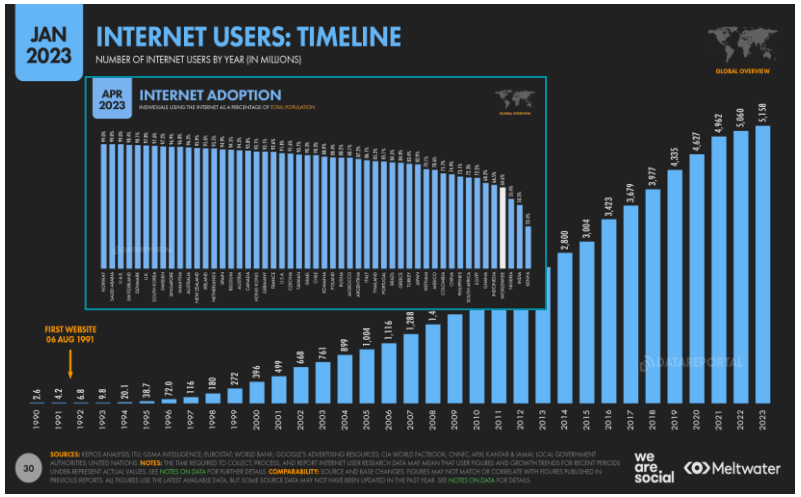
徐 恪

目录
CONTENTS

互联网路由系统安全现状

互联网已经发展成为网络空间





互联网规模持续增长

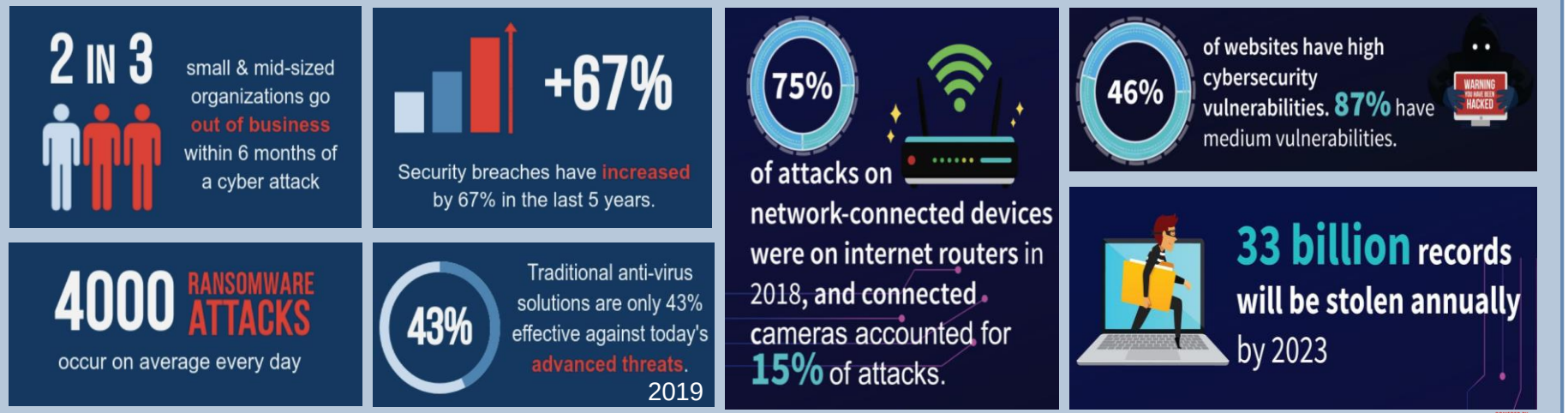
- 截至2023年4月，全球互联网用户数量达到51.8亿人，占世界人口的比重达到64.6% (DataReportal)
- 2021年全球数据储量达到84.5ZB，复合年均增长率为27.5% (IDC)

互联网应用领域普及广泛

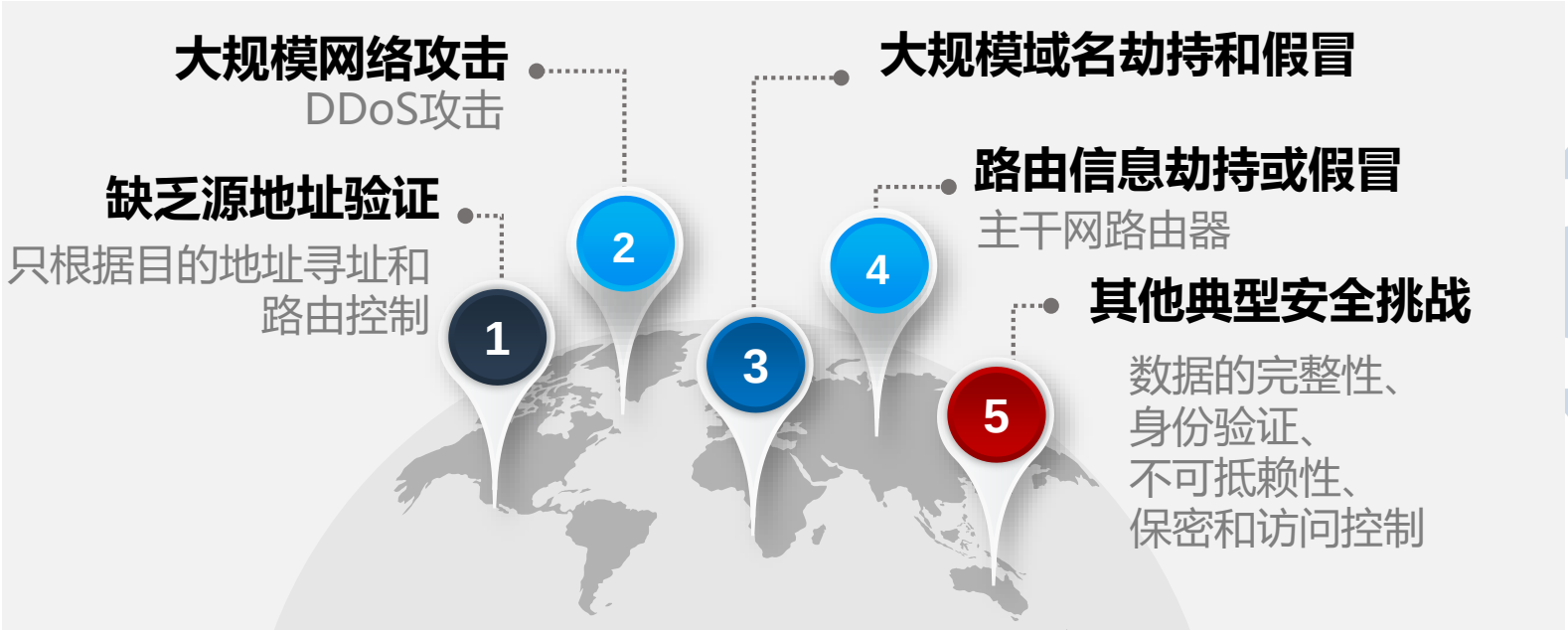
- 互联网经过50多年发展，已经成为继陆、海、空和太空之后的人类第五疆域：网络空间
- 互联网成为承载国家政治、经济、文化、科技、军事的重要基础设施和国家重要战略资源

网络空间安全面临巨大挑战

- 网络空间安全问题复杂化、常态化
- 网络攻击方式趋于智能隐蔽，**传统安全防御手段效果有限**
- 网络数据和用户隐私面临严重威胁



"5-need-to-know-cybersecurity-statistics-for-2019"



国家关键基础设施和网络关键设备面临瘫痪风险

网络数据处理面临泄漏或被窃取的风险

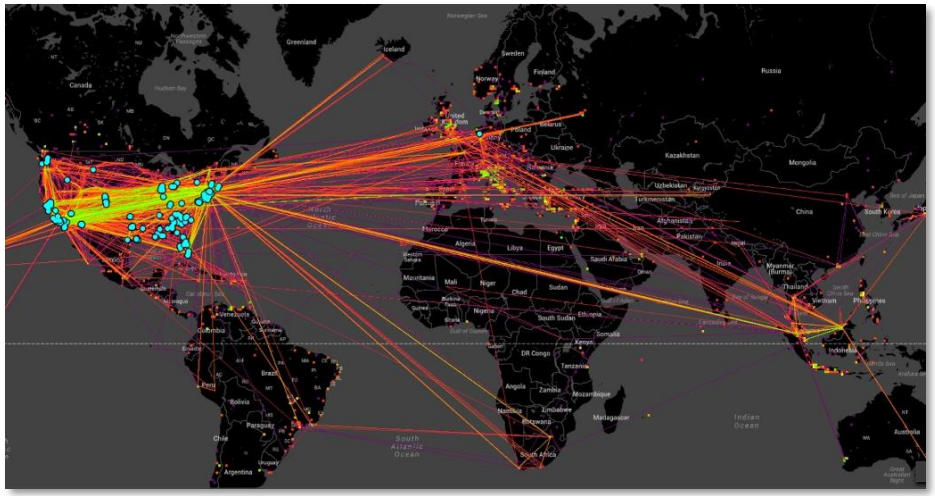
网络应用服务可信性得不到保证

域间路由安全是保障互联网安全运行的关键

“深入贯彻党中央关于**网络强国**的重要思想，切实肩负起举旗帜聚民心、**防风险保安全**、强治理惠民生、增动能促发展、谋合作图共赢的使命任务，坚持党管互联网，坚持网信为民，坚持走中国特色治网之道，坚持统筹发展和安全，坚持正能量是总要求、管得住是硬道理、用得好是真本事，**坚持筑牢国家网络安全屏障**……”

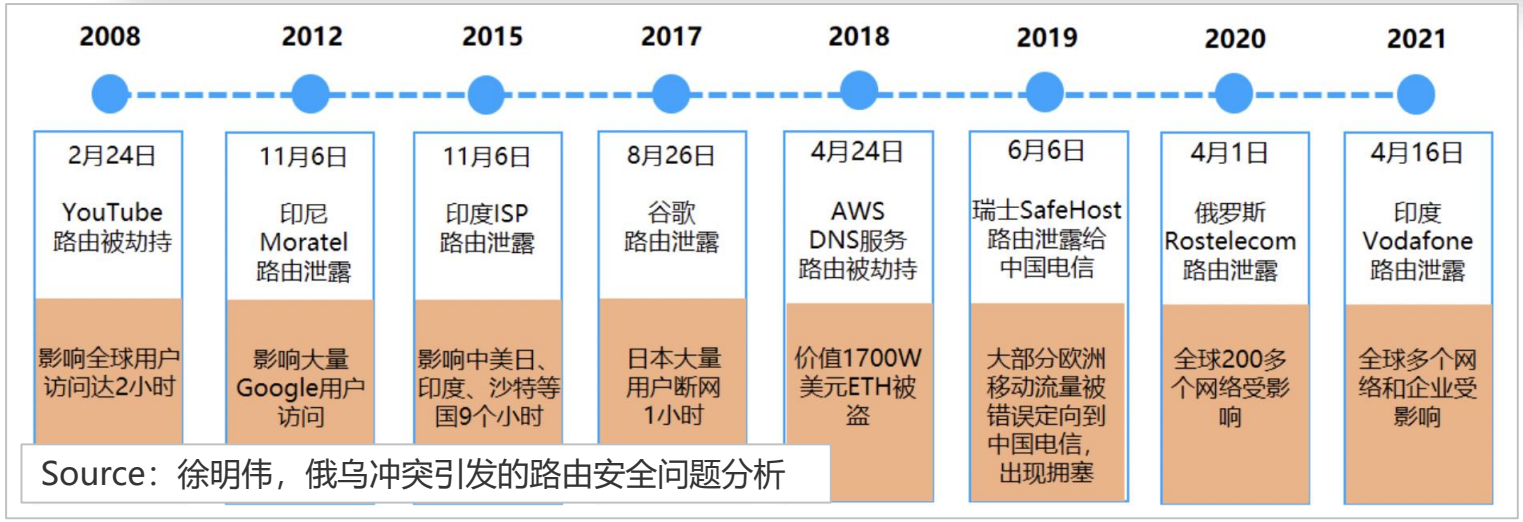
——习近平总书记对网络安全和信息化工作作出重要指示，2023

运行在百万台核心路由器上，连接超十万个自治域和百万个地址前缀，维护近4亿条路由信息的**域间路由系统**，承担着全球互联网网际互通最重要的核心功能 。**域间路由系统安全就是保障互联网安全运行的关键，一旦域间路由系统遭到攻击和破坏，将直接导致互联网无法正常运行**



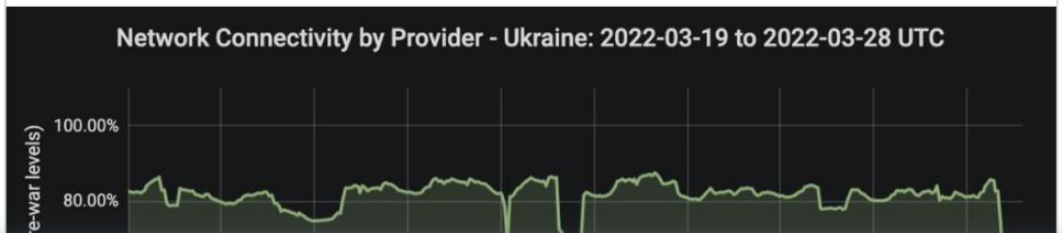
域间路由安全是保障互联网安全运行的关键

域间路由系统诞生于无条件互信的互联网早期，具有高度分布式特性，且缺乏必要的信任基础和有效的表达验证机制，由此产生的路由劫持和泄漏风险，如果不加以控制，使得特定互联网流量激增，最终可能导致全球拥塞、拒绝服务和网络瘫痪

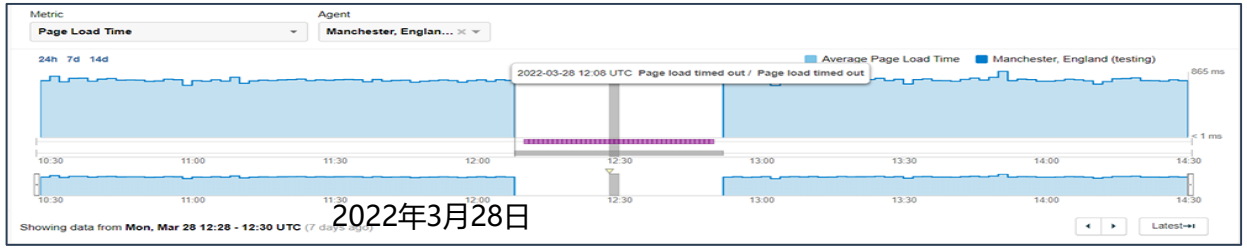


Source：徐明伟，俄乌冲突引发的路由安全问题分析

BGP的这种脆弱性，在遭受恶意攻击或人为变更配置错误时将会变得异常突显，对国家、运营商和企业带来极大威胁，在战争期间，甚至可能成为战役型大规模杀伤性武器



乌克兰互联网运营商Ukrtelecom (AS6849)遭受路由攻击，发生长达 15 小时的全国内服务中断



俄罗斯互联网运营商 RTComm.ru 劫持了属于Twitter的前缀(104.244.42.0/24)，使其面临信息泄漏、流量劫持的巨大风险

域间路由安全是保障互联网安全运行的关键

Secure Internet Routing

A Notice by the Federal Communications Commission on 03/11/2022

Synopsis

1. The Commission plays an important role in protecting the security of America's communications networks and critical infrastructure. The Commission, in tandem with its federal partners, has urged the communications sector to defend against cyber threats, while also taking measures to reinforce our Nation's readiness and to strengthen the cybersecurity of vital communications services and infrastructure, especially in light of Russia's escalating actions inside of Ukraine. Today, the Commission builds on those efforts. With this *Notice of Inquiry* (*Notice*), the Commission seeks comment on vulnerabilities threatening the security and integrity of the Border Gateway Protocol (BGP), which is central to the internet's global routing system, its impact on the transmission of data from email, e-commerce, and bank transactions to interconnected Voice-over Internet Protocol (VoIP) and 9-1-1 calls, and how best to address them.

2022年2月，美国联邦通信委员会FCC发起调查BGP路由安全的通知书

2022年4月，国际互联网协会ISOC和Internet2对此做出回应

INTERNET2 ANNOUNCEMENTS

Internet2 Submits Comments to FCC on Secure Internet Routing

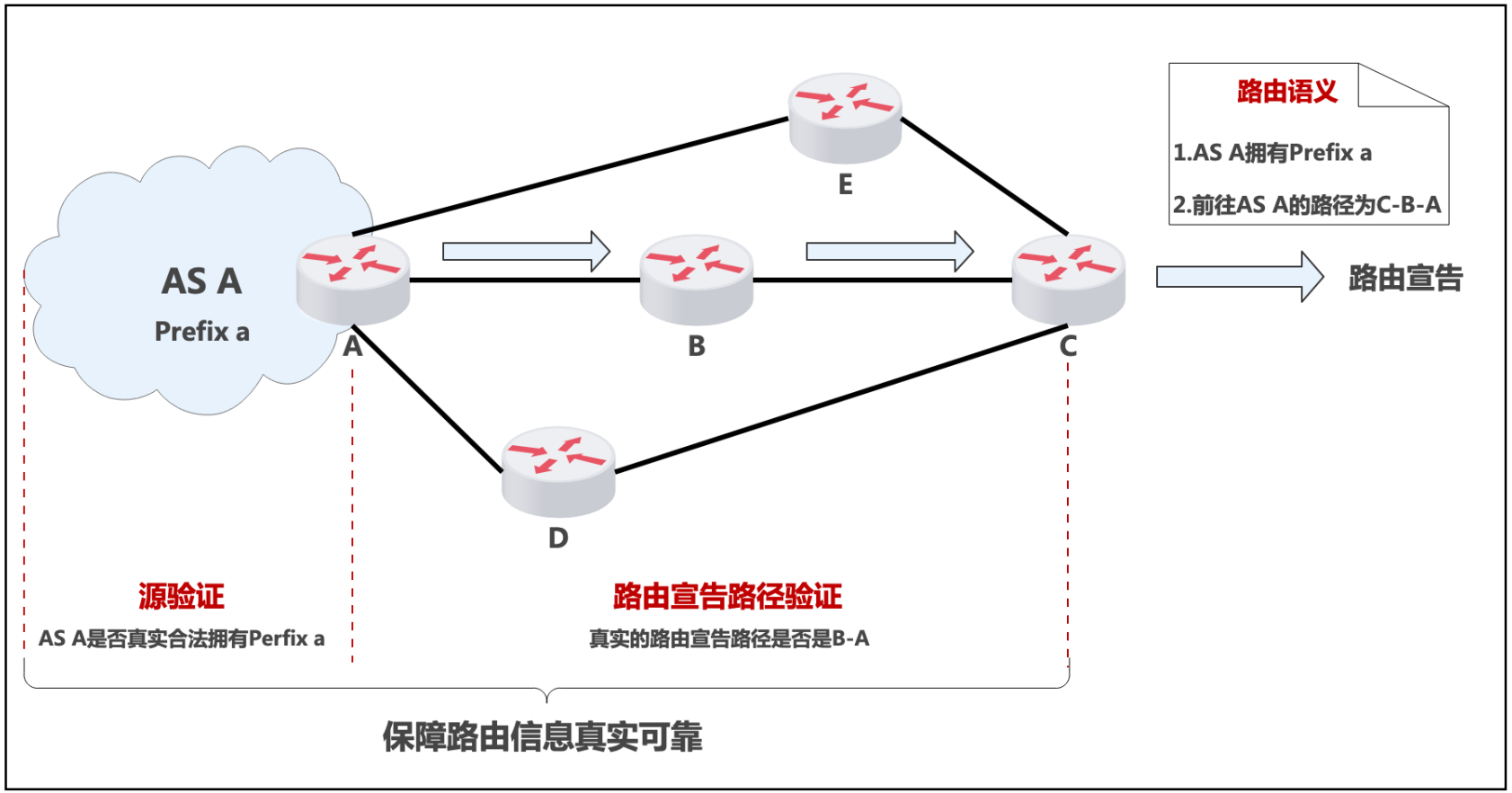
- Five recommendations to improve the state of routing security in the R&E community:
  - Making the concepts of routing security accessible and important.
  - Access to router configuration training.
  - Development and adoption of network configuration tools that will aid in the consistent implementation of the desired routing policy.
  - Development and operation of an R&E routing security observatory to provide the ability to independently measure the alignment with secure route policy.
  - Development and maintenance of an R&E routing security control framework for assessing an organization's routing security.

COMMENTS OF INTERNET SOCIETY

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

增强发现和检测手段，通过技术从本质上提升BGP协议的安全能力，实现有效应用部署，成为解决路由安全挑战、提高互联网安全性的必由之路

域间路由信息的验证体系



路由语义

BGP路由的语义包括当前宣告的**前缀信息**，以及前往该前缀所经过的**AS路径**

路由伪造

由路由语义可知路由伪造包括**起源伪造和路径伪造**，虚假的路由起源和路径信息，都将导致数据面流量劫持的安全威胁

路由源+宣告路径验证组成了当前验证体系，代表机制分别为RPKI和BGPsec

RPKI：域间路由源验证的代表性机制

IETF在路由抗劫持防泄漏方面的已有工作 - RPKI

2006
- sidr工作组成立
- 关注路由源验证和路由路径验证

2012-2014
- sidr工作组
- **RPKI**: RFC 6480 ~6493, 6810, 6811, 6907, 6916, 6945, 7115, 7128, 7318

2016
- sidrops工作组成立
- 指导域间路由安全技术在互联网的部署和操作

2016-2018
- sidr工作组
- RPKI: RFC 7382, 7730, 7909, 7935, 8097, 8181, 8182, 8183, 8210, 8211, 8360, 8416

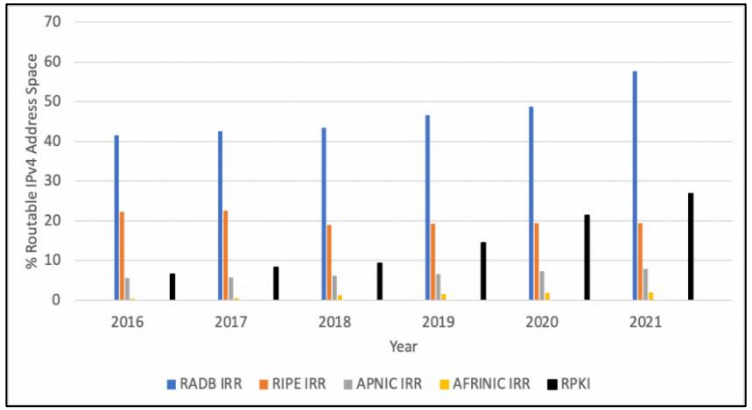
2018-2022
- sidrops工作组
- RPKI: RFC 8481, 8488, 8630, 8893, 8897, 9255, 9286, 9319, 9323, 9324

2020年，ICANN发布RPKI白皮书，明确指出解决路由源劫持问题的RPKI存在诸多问题，这其中的核心问题是**根证书中心化**

RPKI ROA的**部署率并不高**。NIST的实时监测结果表明，互联网IPv4地址中，有45.26%前缀的ROA是Valid，1.00%前缀的ROA是Invalid，**53.74%前缀没有ROA记录**。IPv6地址结果分布相差不多

Source: https://rpki-monitor.antd.nist.gov/

正在sidrops工作组进行标准化的ASPA方案，它的运行原理**需要运营商公布商业关系**



基于IRR的验证，其前缀覆盖率比RPKI更高，达到60%，但存在**大量错误、过时记录**

Source: https://blog.apnic.net/2022/04/07/irr-hygiene-in-the-rpki-era/

BGPsec：域间路由宣告路径验证的代表性机制

IETF在路由抗劫持防泄漏方面的已有工作 - BGPsec

2006
- sidr工作组成立
- 关注路由源验证和路由路径验证

2014-2016
- sidr工作组
- **BGPsec**: RFC 7132, 7353

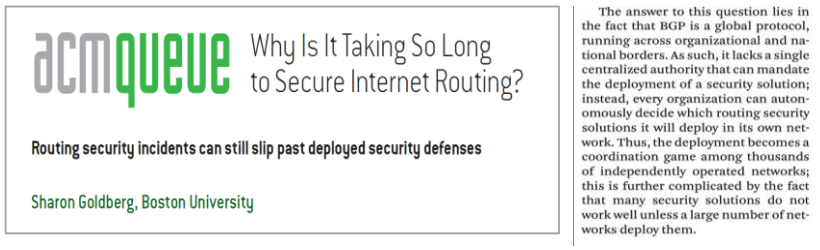
2016
- sidrops工作组成立
- 指导域间路由安全技术在互联网的部署和操作

2016-2018
- sidr工作组
- BGPsec: RFC 8205~ 8209

2018-2022
- sidrops工作组
- BGPsec: RFC 8608, 8634, 8635

BGPsec旨在解决域间路由的AS路径篡改问题，但针对路由泄露问题的处理并不完善

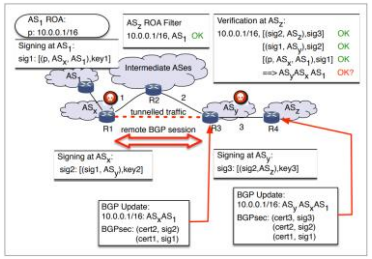
Sharon Goldberg
波士顿大学
教授


acmqueue
Why Is It Taking So Long to Secure Internet Routing?
Routing security incidents can still slip past deployed security defenses
Sharon Goldberg, Boston University

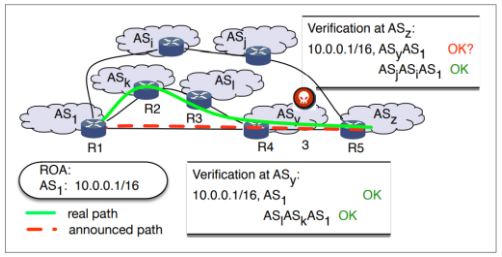
The answer to this question lies in the fact that BGP is a global protocol, running across organizational and national borders. As such, it lacks a single centralized authority that can mandate the deployment of a security solution; instead, every organization can autonomously decide which routing security solutions it will deploy in its own network. Thus, the deployment becomes a coordination game among thousands of independently operated networks; this is further complicated by the fact that many security solutions do not work well unless a large number of networks deploy them.

Sharon Goldberg在ACM Queue撰文指出目前的BGP安全机制部署困难，大多无法增量部署

BGPsec在机制上依赖于RPKI，且**不支持渐进增量部署**，ISP的部署意愿较低。根据2022年MANRS的调查结果，只有14.89%MANRS成员ISP有意愿部署BGPsec



Wormhole攻击



篡改攻击

BGPsec完全部署仍面临wormhole以及篡改等攻击

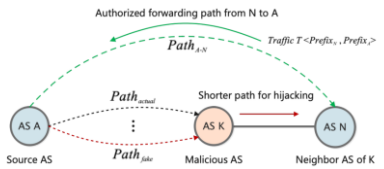
VRO和FC-BGP：新型域间路由安全体系

- 以RPKI为代表的源验证机制，存在**数据不一致、更新滞后、覆盖范围有限**等问题，同时**中心化结构存在潜在的信任风险**，限制了相关机制的进一步推广和部署。

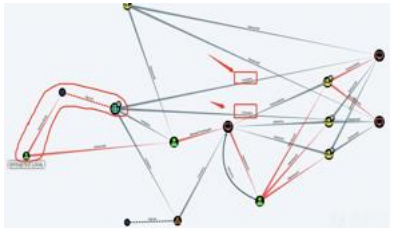
➡ **可验证路由起源:VRO (Verifiable Route Origin)**

- 以BGPsec为代表的路径验证机制，对部署率要求较高，在路径**部分部署**场景下，**难以保障已部署节点的安全收益**。

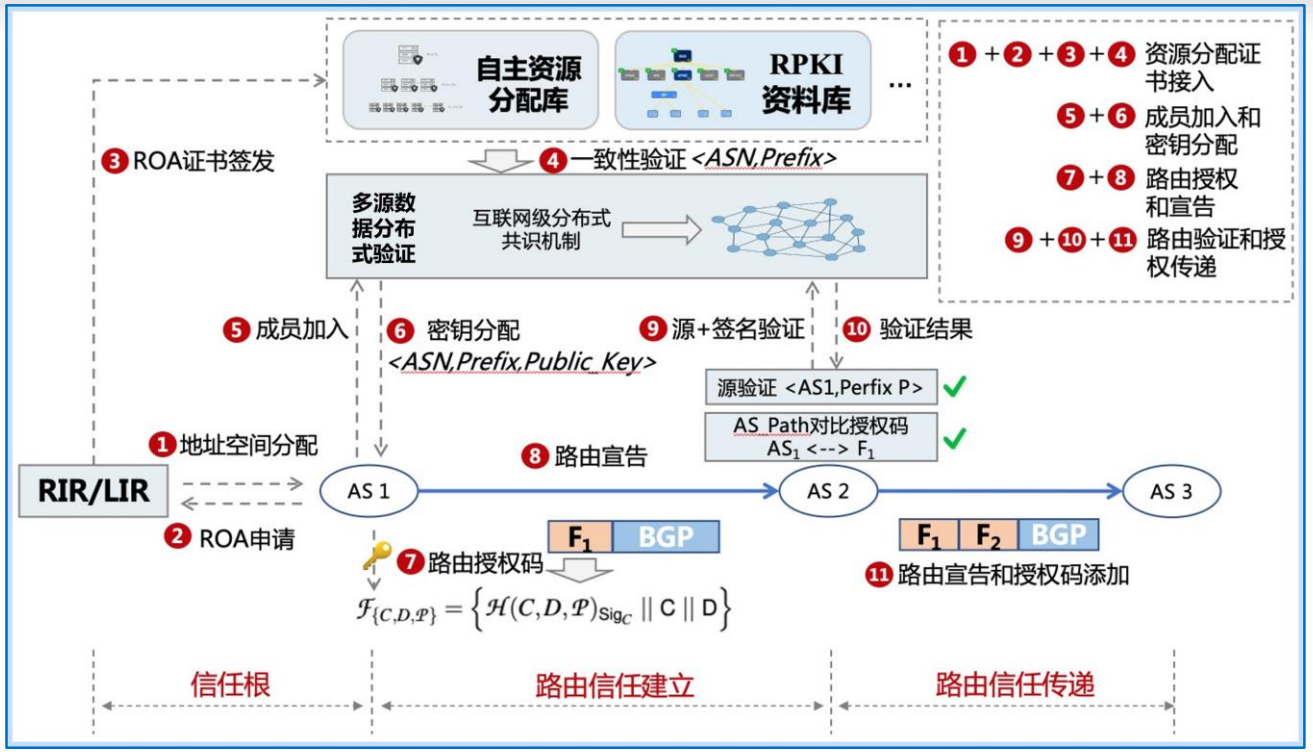
➡ **基于转发承诺的路由和转发路径验证：FC-BGP**



路由起源



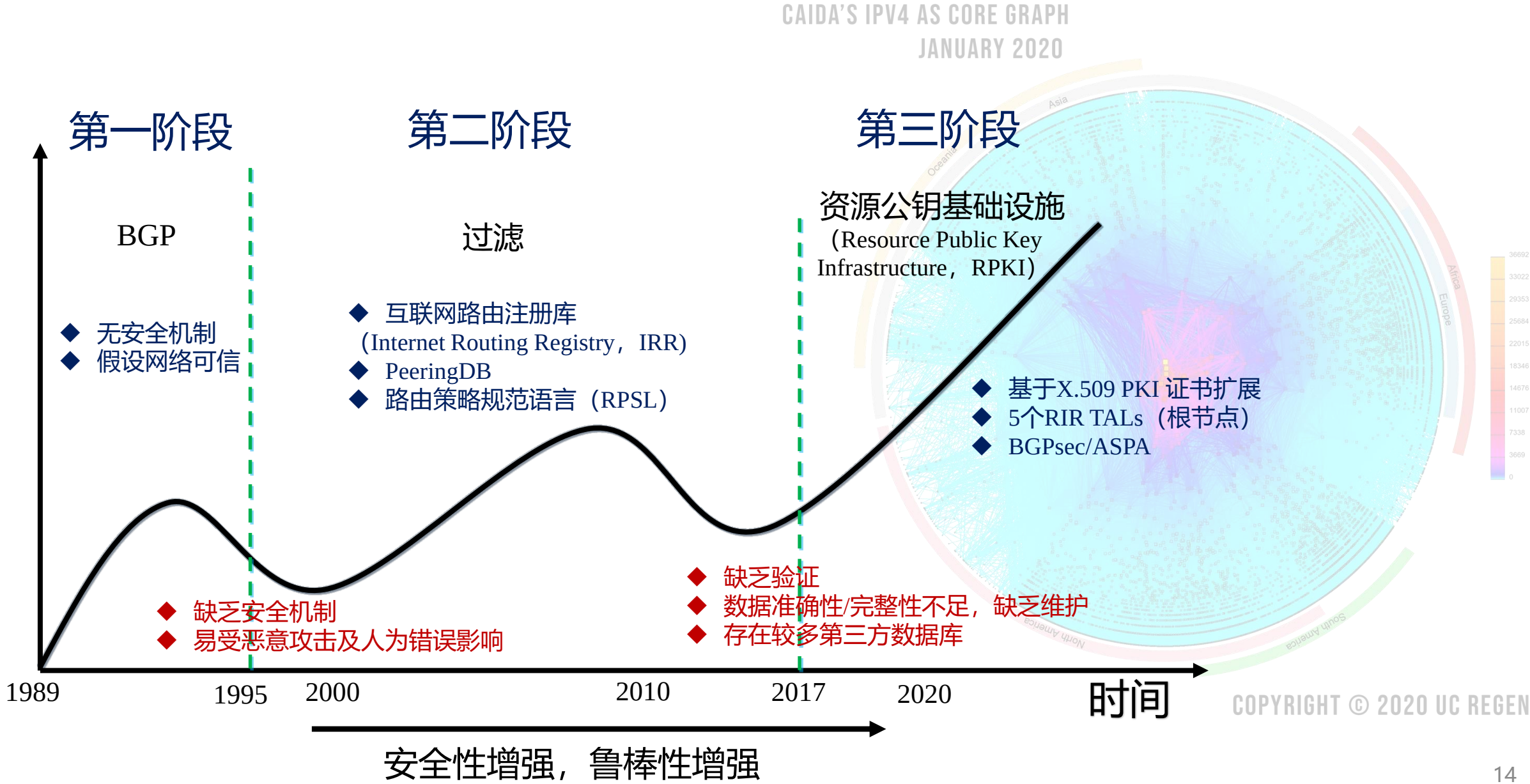
宣告和转发路径



- 通过安全高效的分布式多源验证，**基于多源接入、验证地址分配记录，解决数据源冲突**，构造源验证信任根
- 通过**转发承诺的生成和传递，设计信任建立和验证机制**，完成宣告和转发路径验证

VRO：可验证路由起源

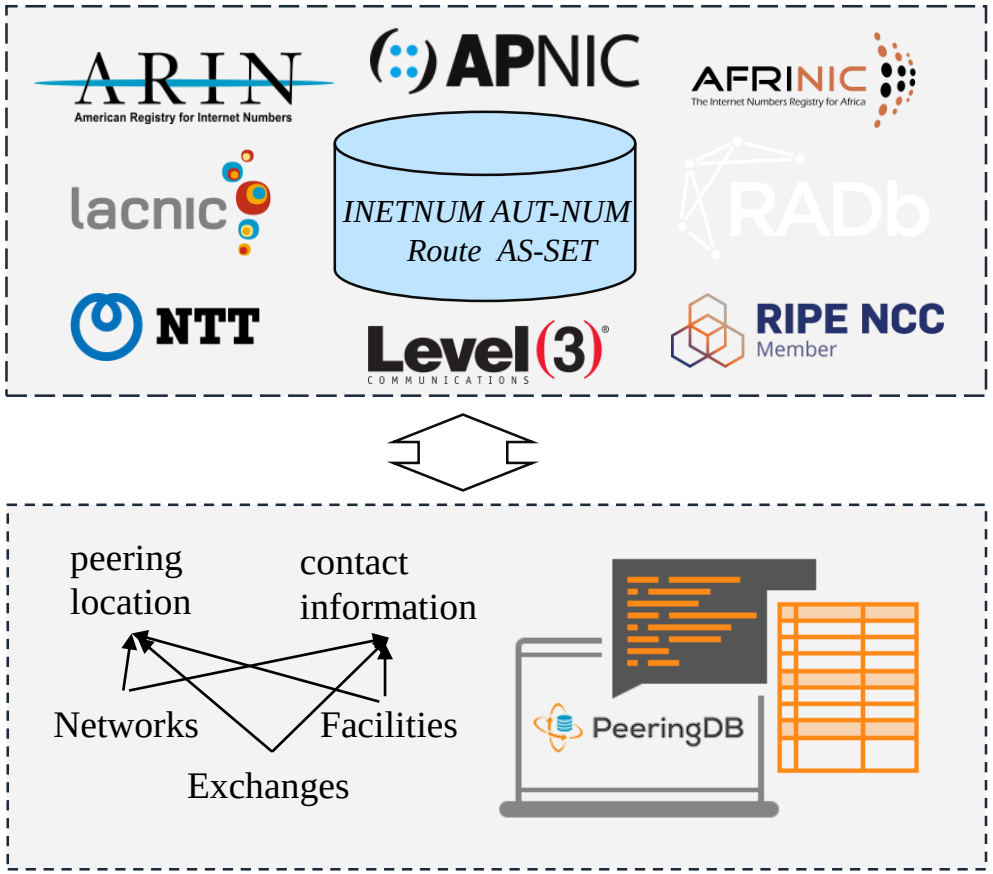
源验证机制发展历程

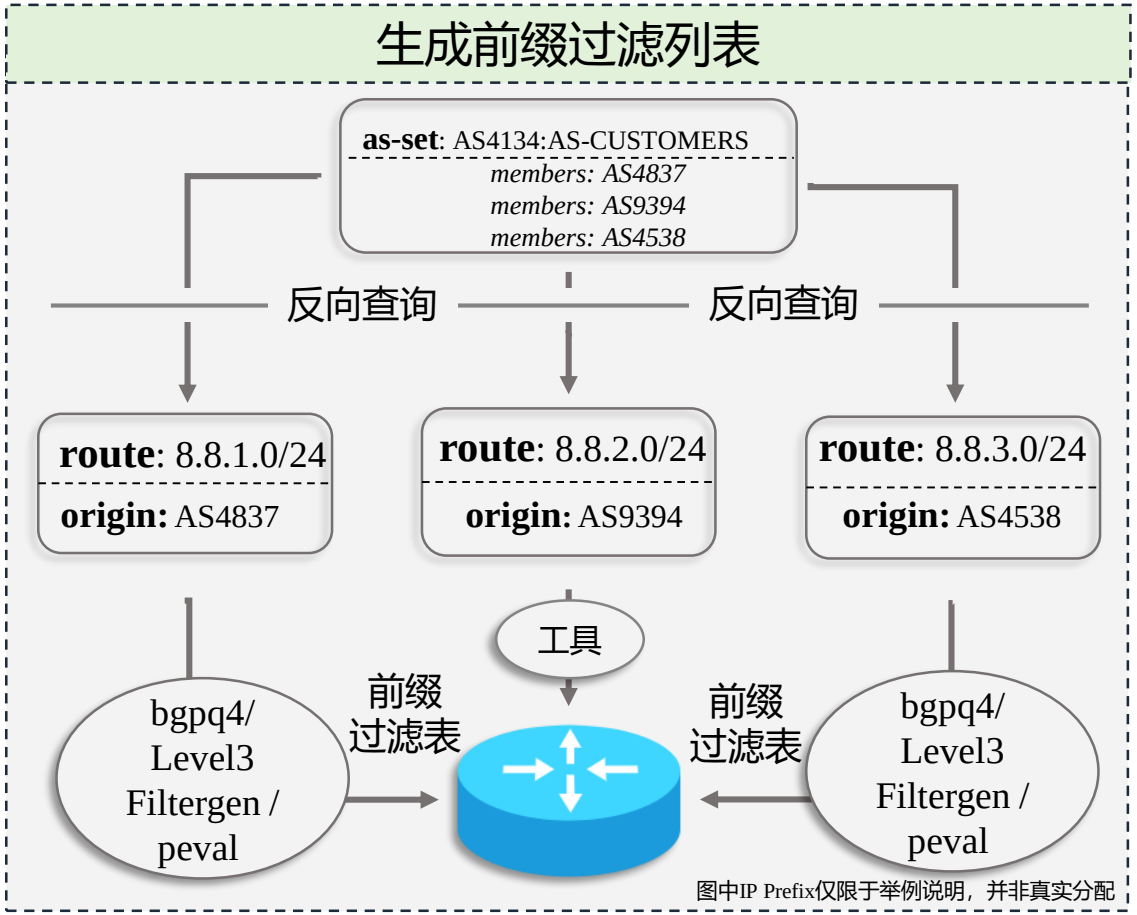


过滤机制

IRR

PeeringDB





决定在路由表或网络中允许哪些路由，以及向邻居宣布哪些路由

IRR现状分析

IRR数据存储形式

可用IRR数据库（≥20个）

AFRNIC ATLDB APNIC ARIN BELL BBOI CANARIE IDNIC JPIRR JPNIC KRNIC LACNIC LEVEL3 NETEGG NTTCOM PANIX RADB REACH RIPE TC TWNIC …

包含类型（13个）

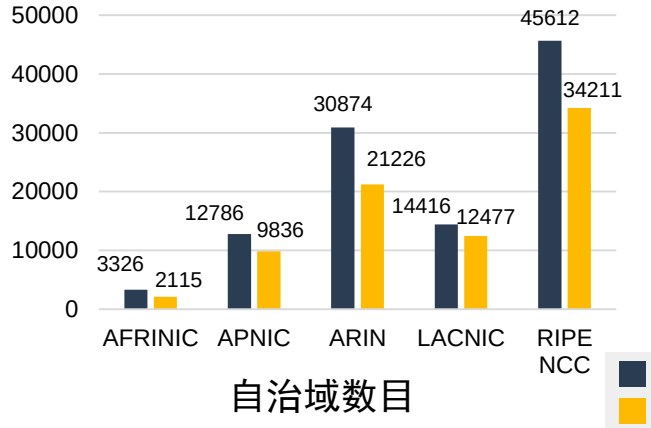
as-set, aut-num, filter-set, inet-rtr, key-cert, mntner, peering-set, person, role, route, route6, route-set, rtr-set

对象属性（41个）

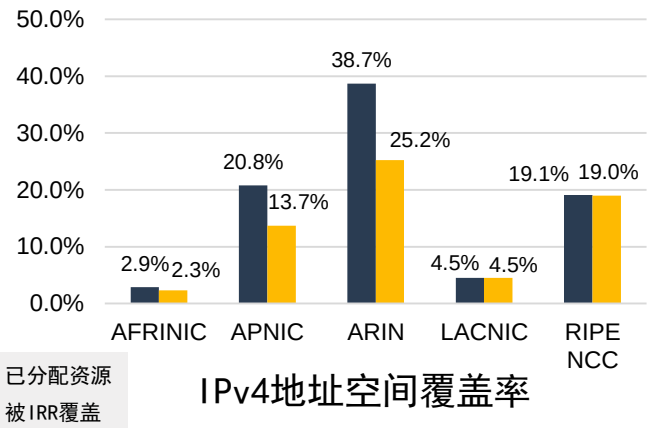
descr, tech-c, admin-c, remarks, notify, mnt-by, changed, source, upd-to, mnt-nfy, auth, as-name, import, export, default, alias, local-as, ifaddr, peer, origin, components, aggr-bndry, aggr-mtd, export-comps, holes, inject, filter, address, phone, fax-no, e-mail, nic-hdl, trouble, member-of, members, mbrs-by-ref, method, owner, fingerpr, certif, geoidx

注：上述IRR数据库为后面实验验证所用的数据库；列举的包含类型和对象属性为RADB中支持的类型和属性

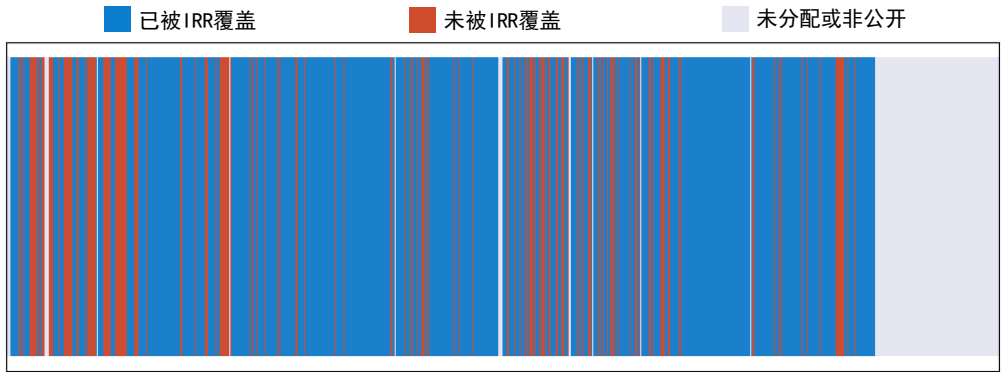
IRR对互联网号码资源覆盖情况



自治域数目



IPv4地址空间覆盖率



地址分配情况在IPv4地址空间的分布

覆盖情况总结

已分配自治域：107014
IRR覆盖自治域：79865
IRR相对已分配自治域覆率：
79865/107014=75%
已分配地址覆盖率：86%
IRR全地址空间覆盖率：65%
IRR相对已分配地址覆盖率：65/86=76%

数据来源、类型与属性多样，对互联网号码资源的覆盖率较高

IRR现状分析

IRR验证分类

IRR记录：AFRNIC ATLDB APNIC ARIN BELL BBOI CANARIE JPIRR JPNIC KRNIC LACNIC LEVEL3 NETEGG NTTCOM PANIX RADB REACH RIPE TC TWNIC

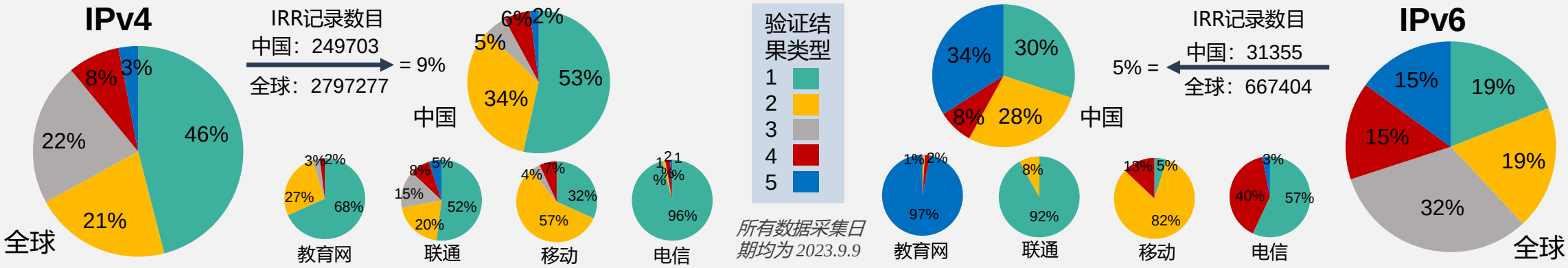
route/route6 → **route**: 8.8.1.0/20, **origin:** AS4837

注1：图中IRR记录和BGP宣告仅限于举例说明，并非真实数据
注2：下面验证使用的BGP宣告采集自 Route Views 和 RIPE NCC

BGP宣告：

route: 8.8.1.0/20, **origin:** AS4837	**route**: 8.8.1.0/24, **origin:** AS4837	**route**: 8.8.1.0/20, **origin:** AS9394	**route**: 8.8.1.0/24, **origin:** AS9394	不在IRR记录中的BGP宣告
验证结果：**1. 前缀完全匹配且合法**	**2. 子前缀被覆盖且合法**	**3. 前缀完全匹配且非法**	**4. 子前缀被覆盖且非法**	**5. 未知**

IRR验证结果

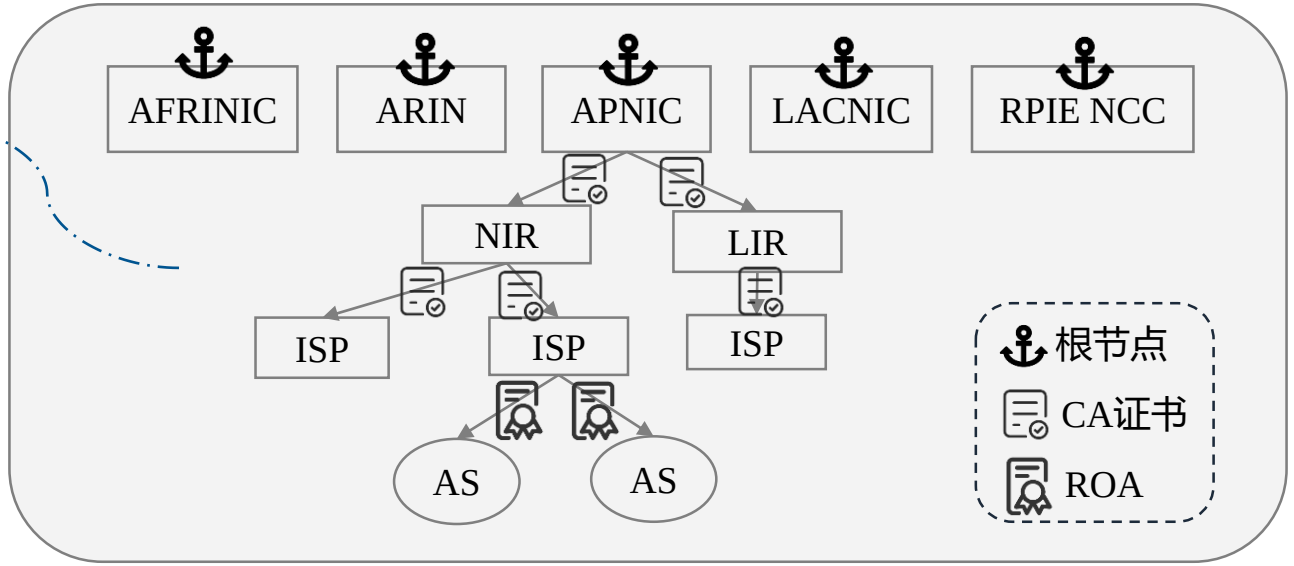


验证结果分类复杂，不同组织的验证效果差异较大

RPKI机制

证书下发

- 逐级签发数字证书
- 通过EE证书，授权AS签发ROA
- 通过撤销EE证书，撤销ROA



RPKI全球数据库

资料库发布点

- CA证书
- ROA
- CRL：证书撤销列表
- 清单

上传

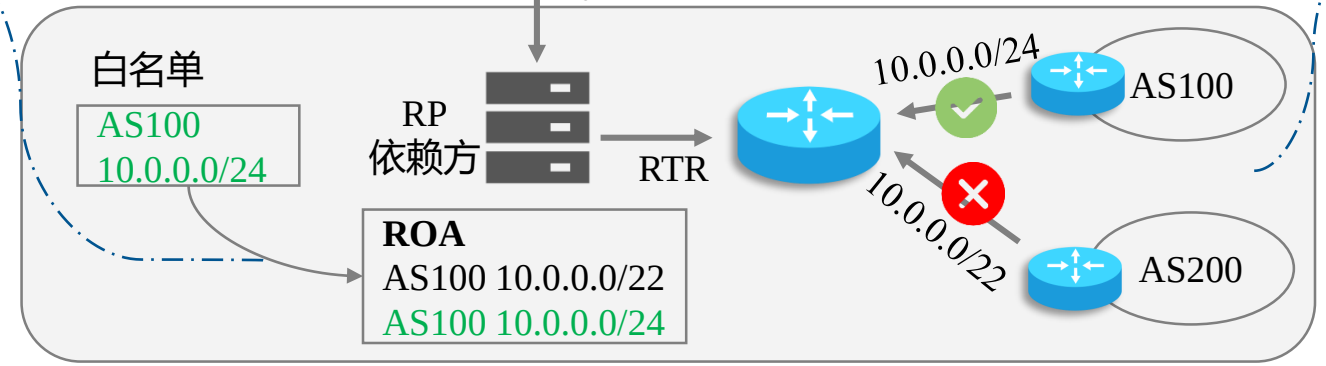
RPKI全球资料库

rsync/RRDP

本地资源管理

本地互联网资源管理（SLURM，RFC846）

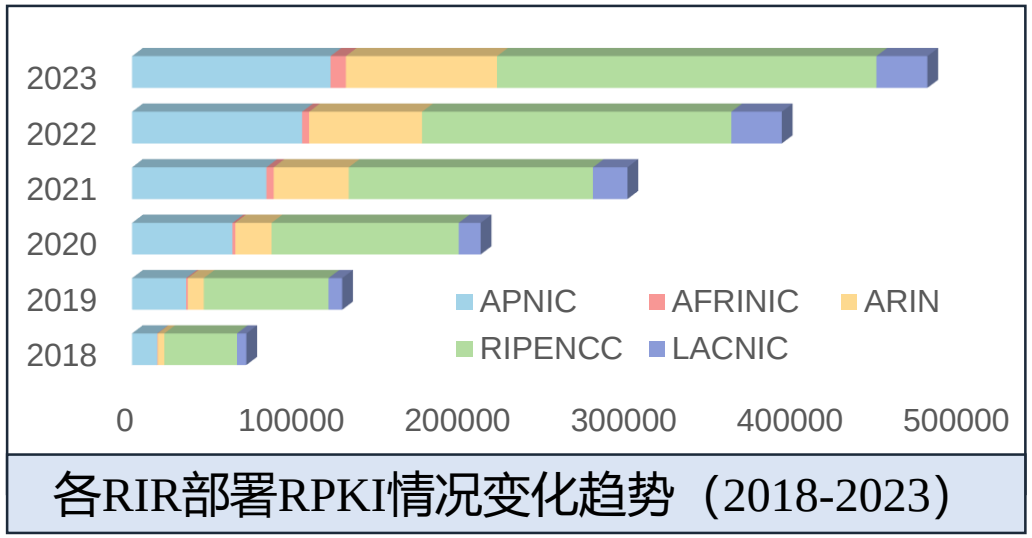
- 通过本地策略，添加/过滤相关条目
- 优先服从“本地策略”



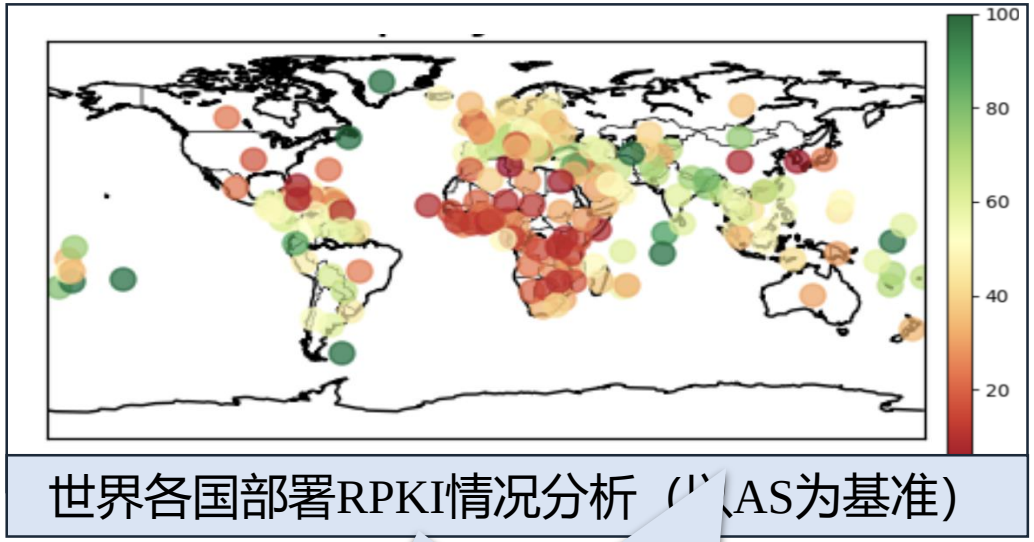
路由验证过程

1. 通过rsync/RRDP同步证书和签名对象
2. 沿证书链验证ROA有效性
3. 生成路由过滤表
4. 通过RTR协议下发到边界路由器

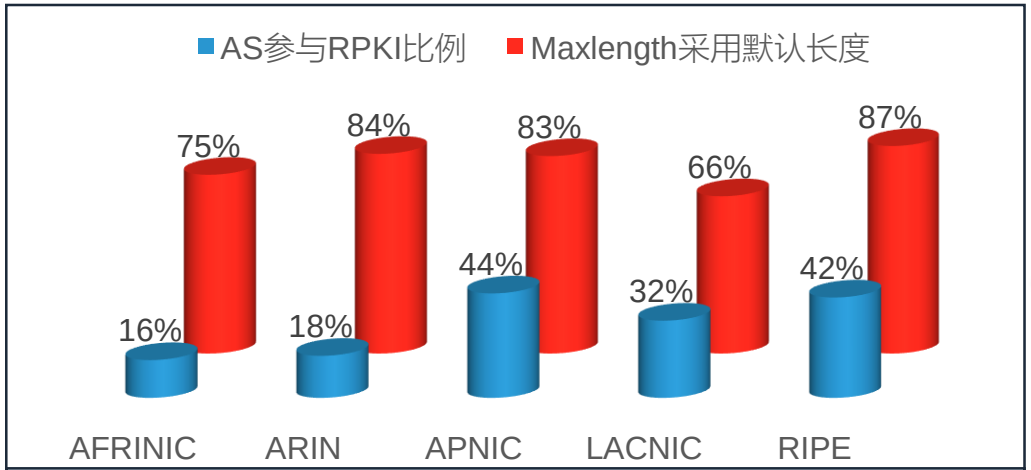
RPKI部署情况



各RIR部署RPKI情况变化趋势（2018-2023）



世界各国部署RPKI情况分析（以AS为基准）



各RIR部署RPKI详情（2023）

-
- 超过
- 绝大 据，仅8个（含NIC 的VRP占比仅12.2%

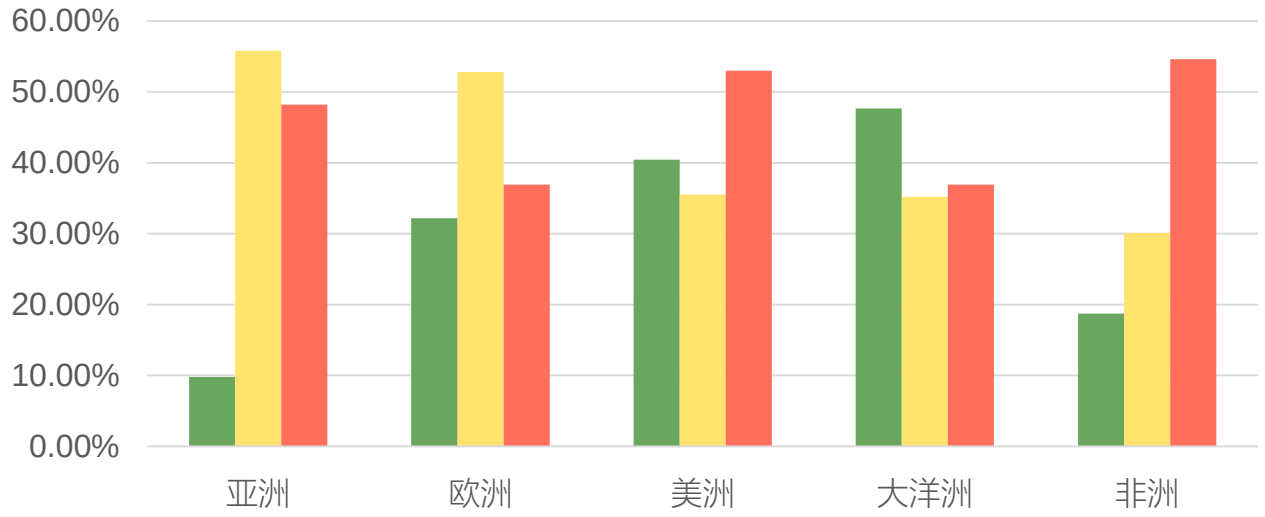
RPKI部署情况仍不乐观；

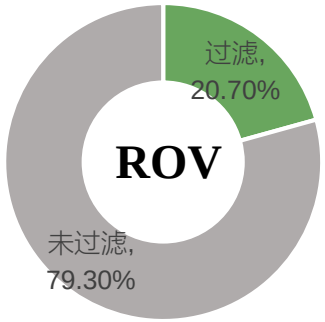
绝大多数ISP采用RIR代理模式，带来新的安全因素。

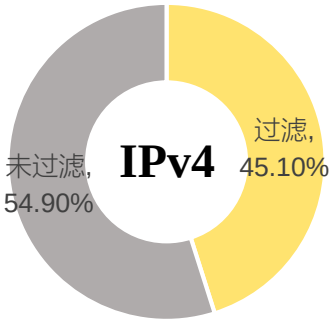
数据源：RIR地址分配数据，RPKI数据

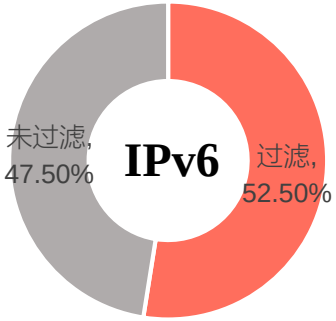
数据截止：2023.11.08

RPKI验证情况





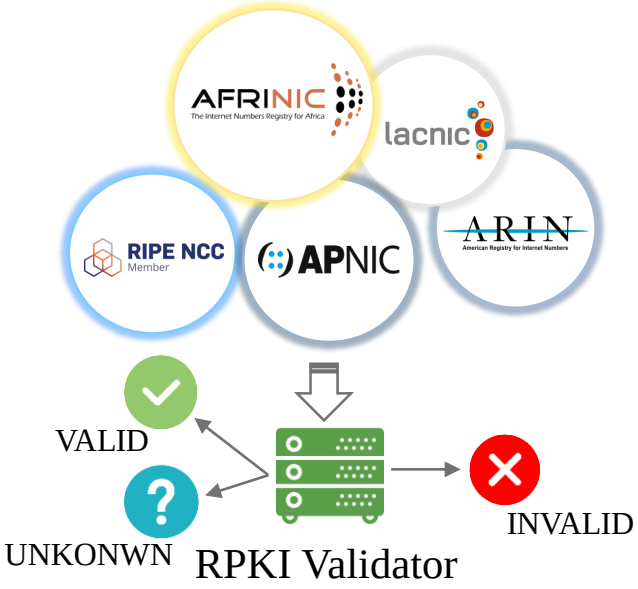




数据来源：APNIC Lab / MANRS
数据截止日期：2023.11.08

RPKI验证情况

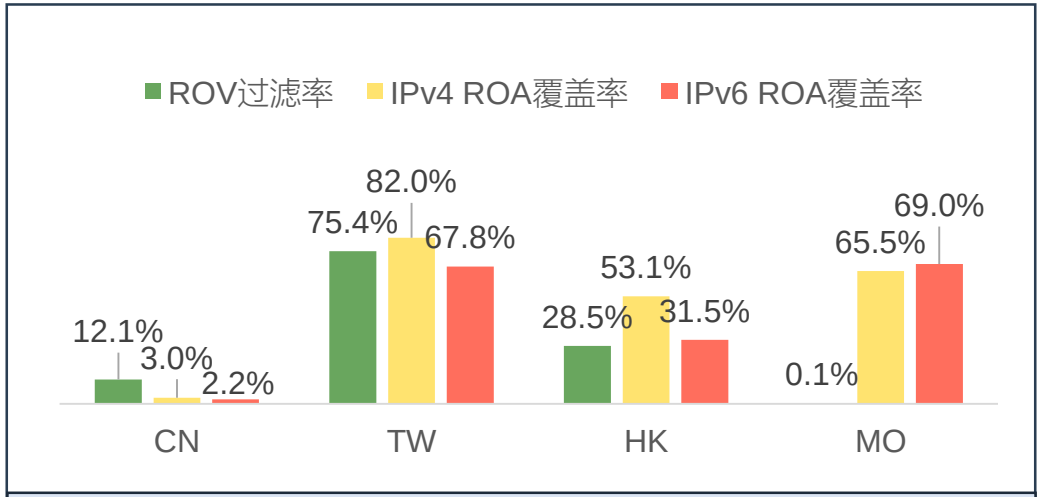
- 根据APNIC、MANRS、NIST报告，IPv4通告RPKI验证有效率，分别能达到45.1%、38.81%和49.21%；
- 各机构报告中，不合法所占比例数据，MANRS相对较高为12.64%，APNIC及NIST中不合法率则未超过5%。



RPKI过滤有效率

- APNIC及RoVista通过测量不合法ROA的可达性，从而验证RPKI过滤有效率；
- 根据APNIC报告，全球整体过滤有效率约为20.7%；
- 受上游供应商部署影响，部分未部署RPKI的ISP也具有一定的过滤有效率。

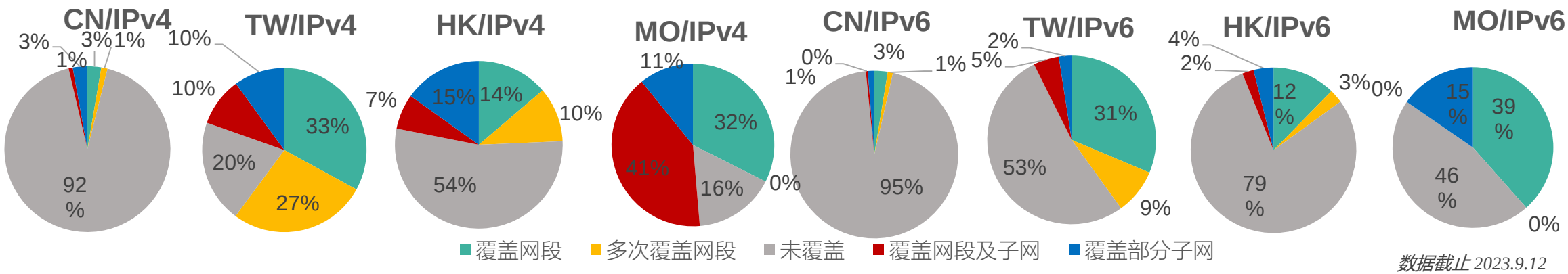
我国RPKI基本情况



我国RPKI过滤及验证情况分析

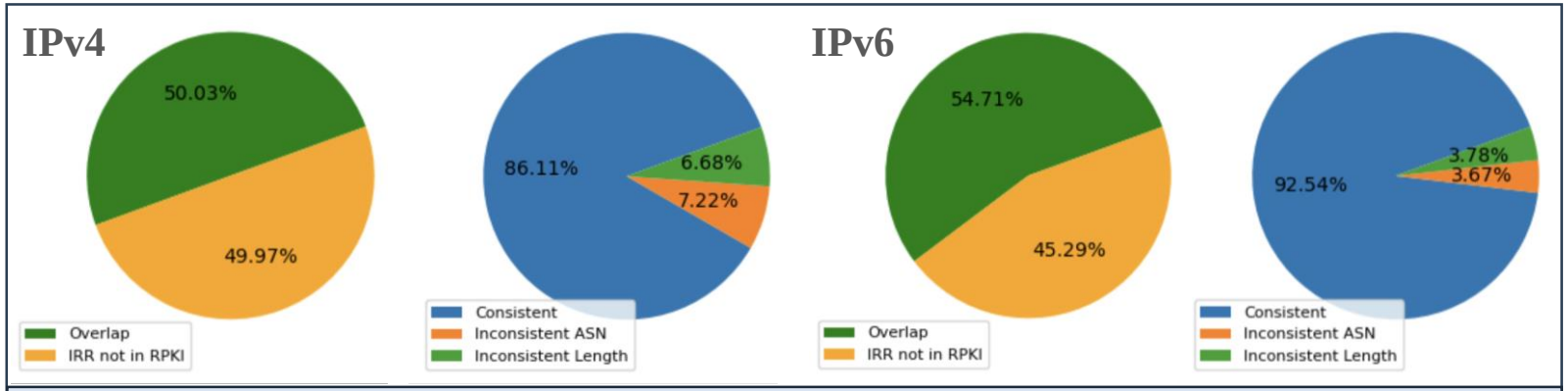
- CNNIC发布点仅包含810条VRP数据，TWNIC包含3538条，CNNIC自维护发布点发布数据量很少;
- ROV验证情况，台湾最高为75.4%，受上级节点部署过滤规则影响，大陆具有12.1%过滤率;
- ROA生成情况，大陆IPv4和IPv6分别只有3%和2%，部署率较低，台湾、香港、澳门部署率较高;
- 基于分配的地址信息，大陆覆盖率最低，有92%未被任何验证；澳门，覆盖率最高。

数据源：APNIC LAB



我国部署RPKI情况分析（以ICANN分配的IP号段为基准）

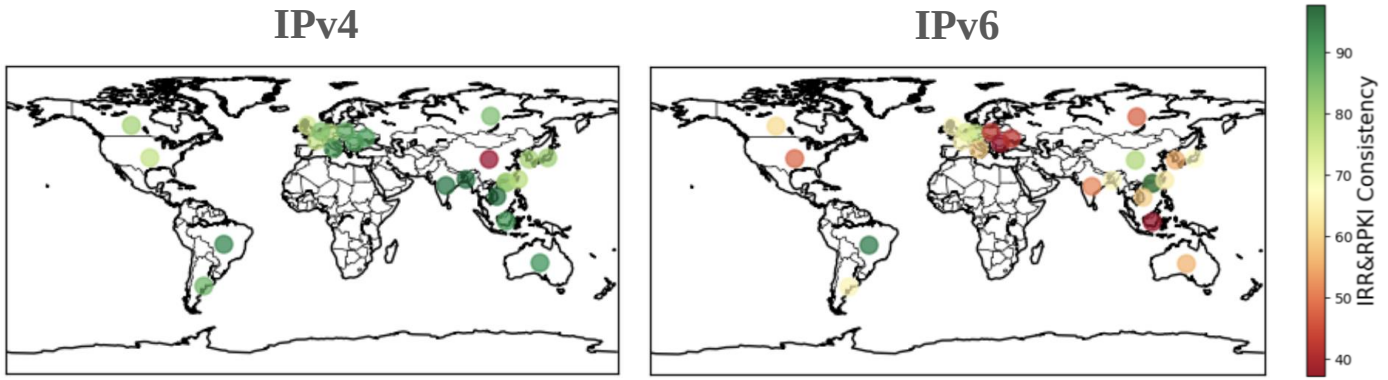
RPKI数据和IRR数据的不一致问题



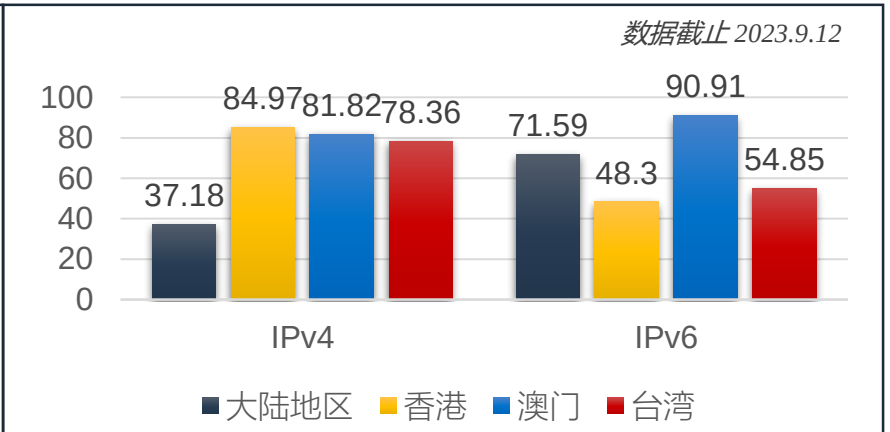
RPKI数据和IRR数据的重叠和冲突情况

- RPKI数据库较IRR数据库前缀覆盖率低
- IRR数据质量较低，针对IPv4和IPv6数据，与RPKI不一致率分别为13.9%和7.45%
- **亟需覆盖率高、准确度高的源验证数据库**

方法参考: IRR Hygiene in the RPKI Era (PAM'22)



RPKI数据和IRR数据的一致性分布情况（AS数量Top20国家/地区）



国内详细数据

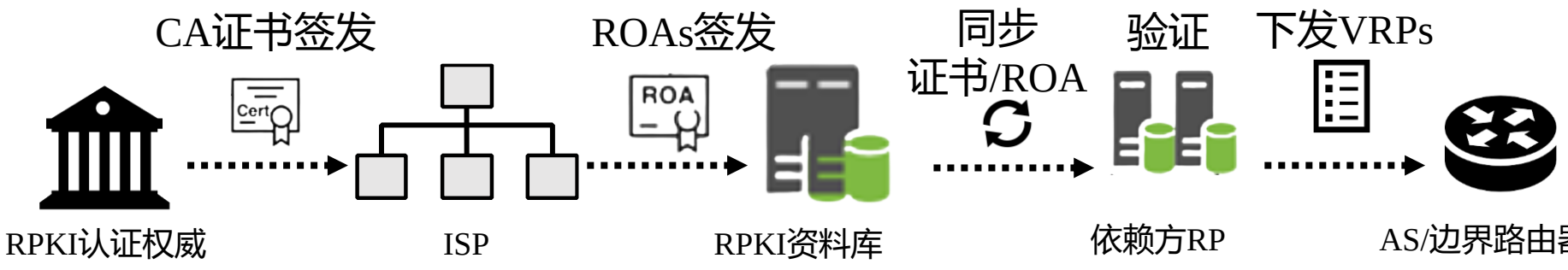
RPKI现存问题

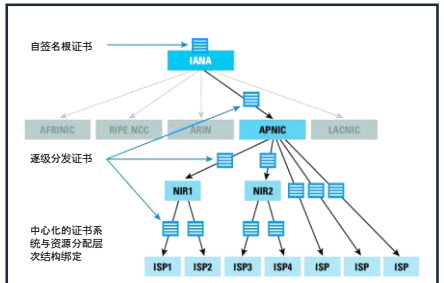
体系结构的固有缺陷 + 尚处于部署初期存在未暴露的安全隐患

安全问题

效率问题

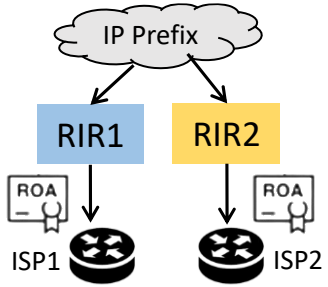
管理问题



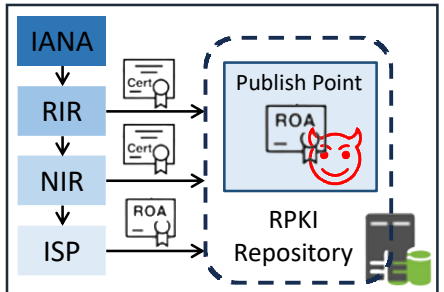


中心化授权

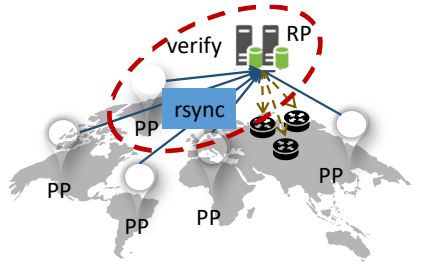
商业关系/MOAS



重复/未授权分配



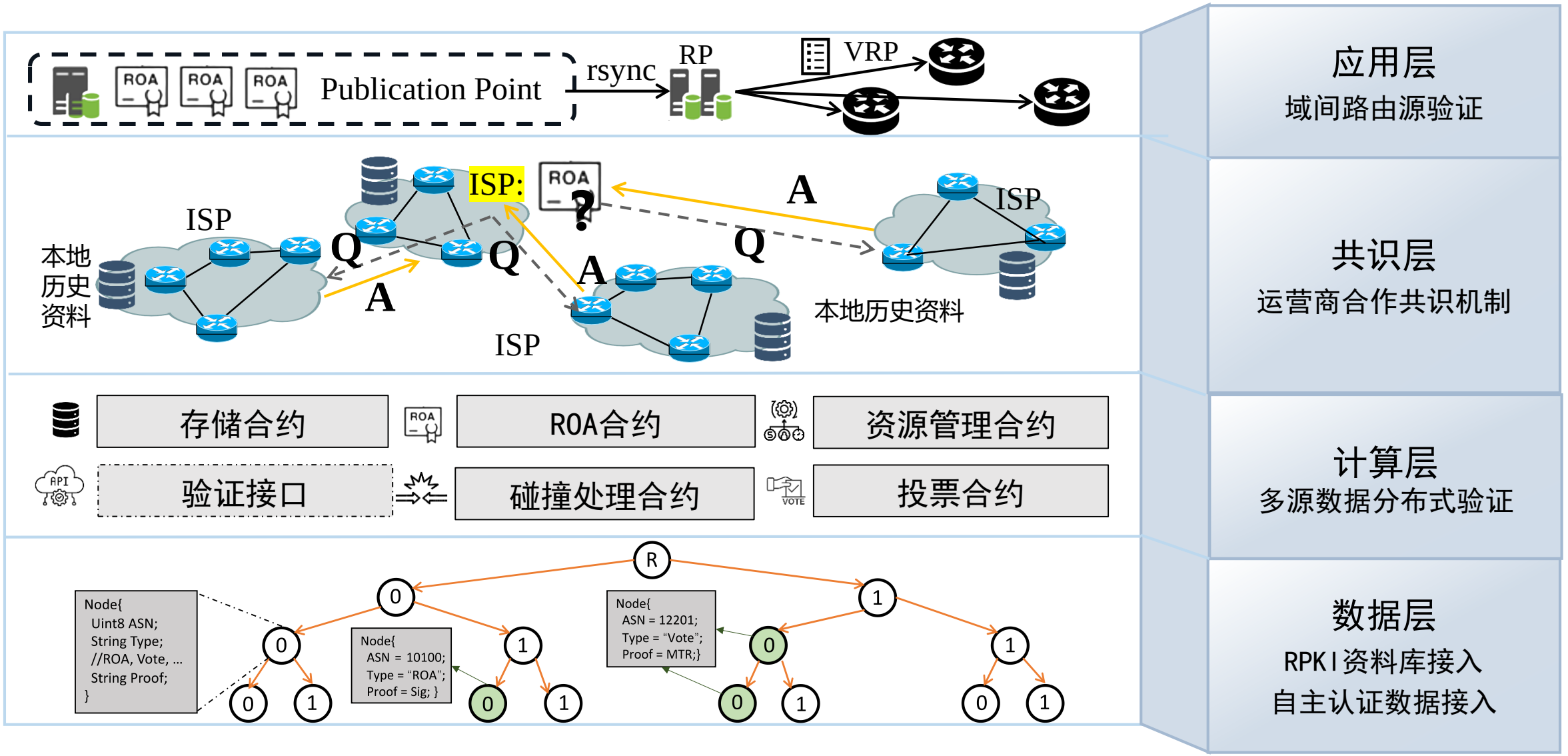
资料库不可信



可扩展性差

目标：通过去中心化的分布式信任机制，实现路由源验证的证书多接入与验证性能扩展，降低对中心化信任根的依赖，提升互联网基础设施的自主可控程度，同时避免路由源验证机制中的单点失效风险，对大规模并发验证提供可扩展的性能支撑。

可验证的路由起源：VRO (Verifiable Route Origin)



冲突解决方案

基于优先级的冲突解决策略

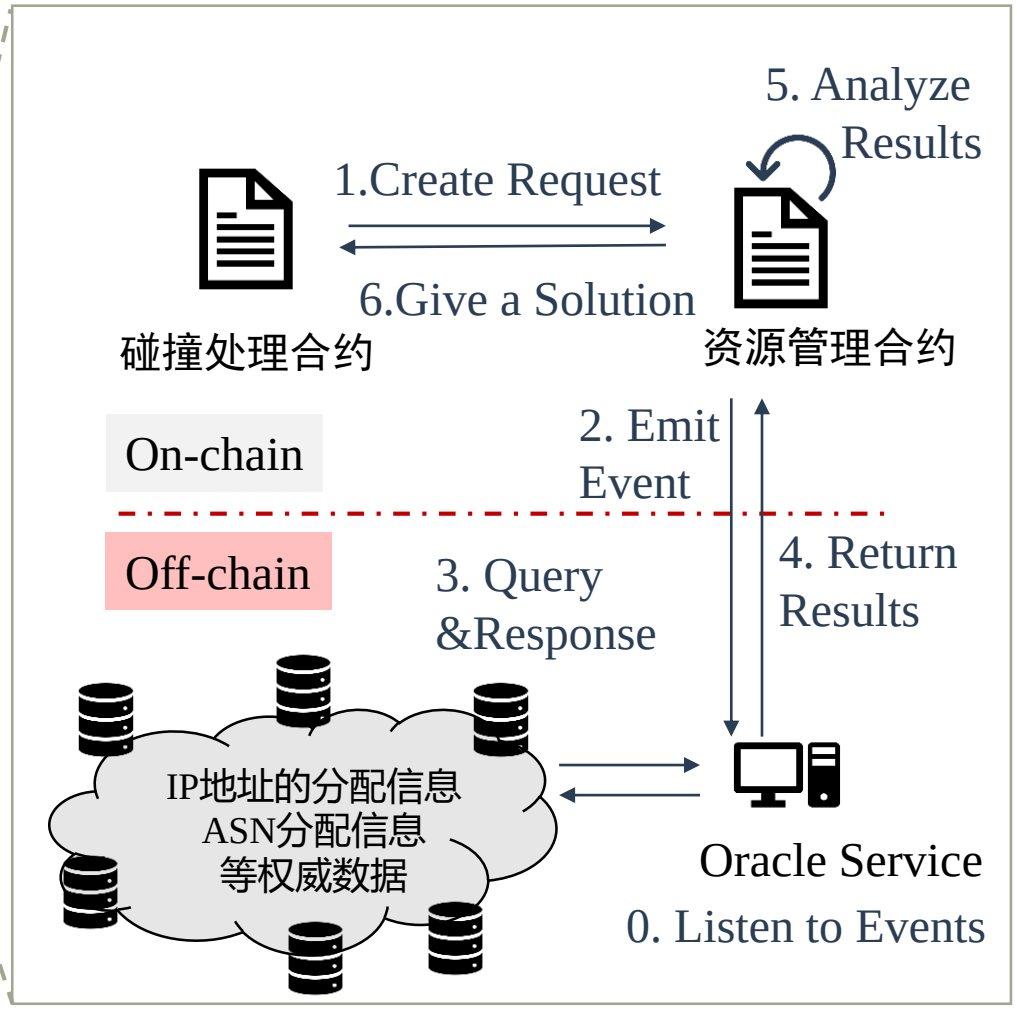
初始化
- IP地址树中节点的初始状态NULL
- 任何合法策略可以修改节点信息

ROA
- ISP提交相关ROA修改节点信息
- 合作方根据RPKI密钥验证ROA并提交证明

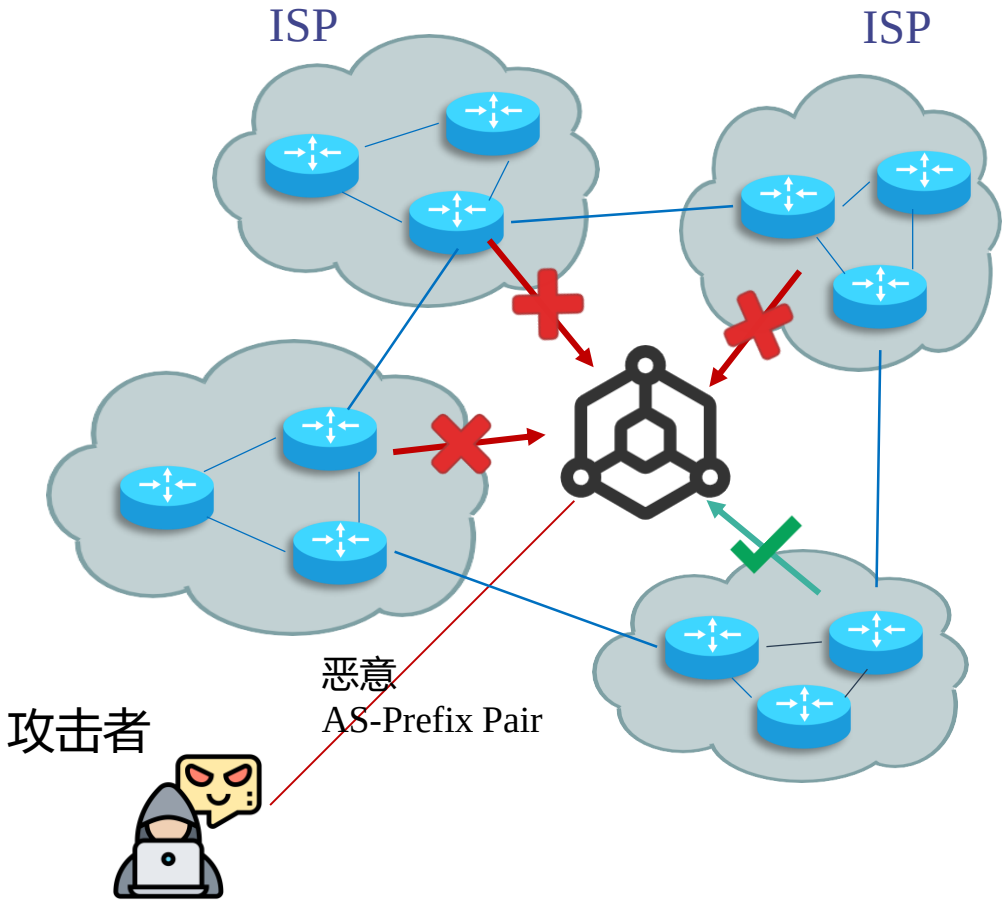
资源
- 智能合约向预言机发出查询请求
- 预言机查询权威数据并给出结论

投票
- ISP提交碰撞信息及相关问题
- 合作方根据私有数据或非权威公开数据提交答案

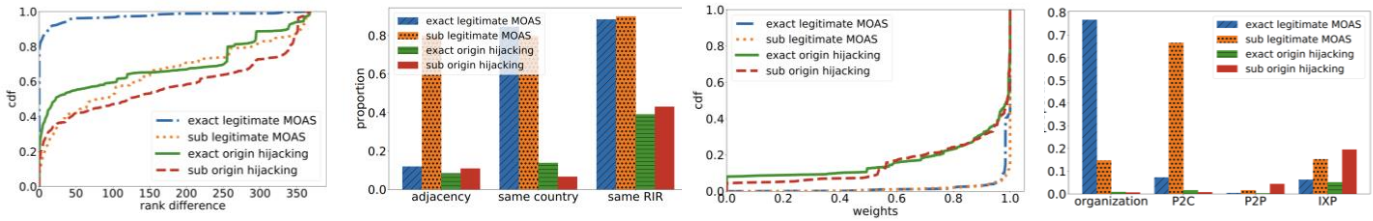
预言机：针对中心化权威数据的查询



运营商合作共识机制：针对私有数据



编号	投票特征
1	AS规模：AS规模大小及AS之间的规模差异
2	商业关系：AS是否属于同一组织或存在P2C关系
3	地理关系：AS是否属于同一国家/同一RIR
4	路由宣告：AS是否在最近一段时间宣告过该路由
5	Anycast：是否为IPv4_to_IPv6前缀/DNS前缀
6	历史信誉：AS在历史路由宣告中是否可信
7	IP可达性：IP地址是否可达

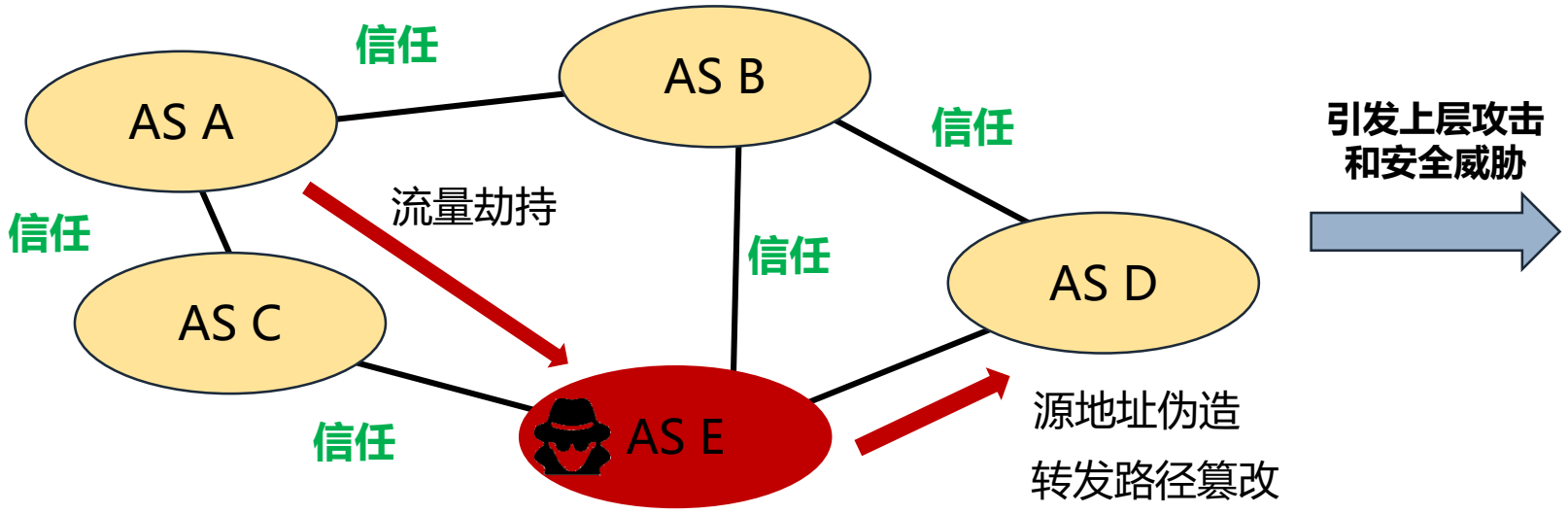


Qin, Lancheng, et al. "Themis: Accelerating the Detection of Route Origin Hijacking by Distinguishing Legitimate and Illegitimate MOAS." *31st USENIX Security Symposium (USENIX Security 22)*. 2022.

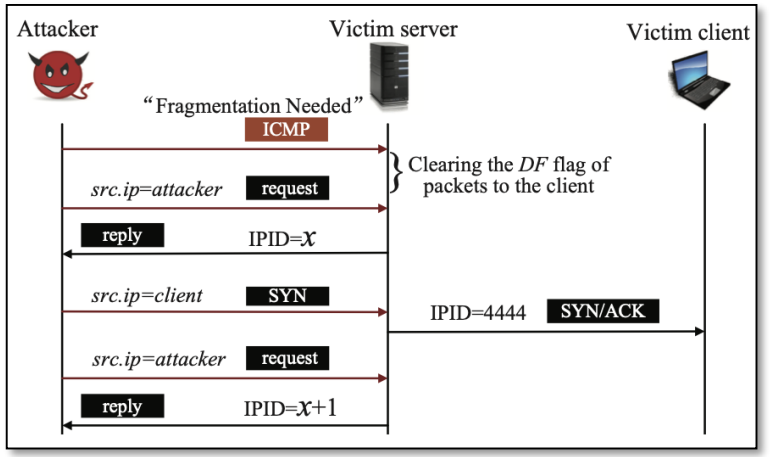
FC-BGP：基于转发承诺的路由路径和转发路径验证

域间路由和转发的弱信任缺陷

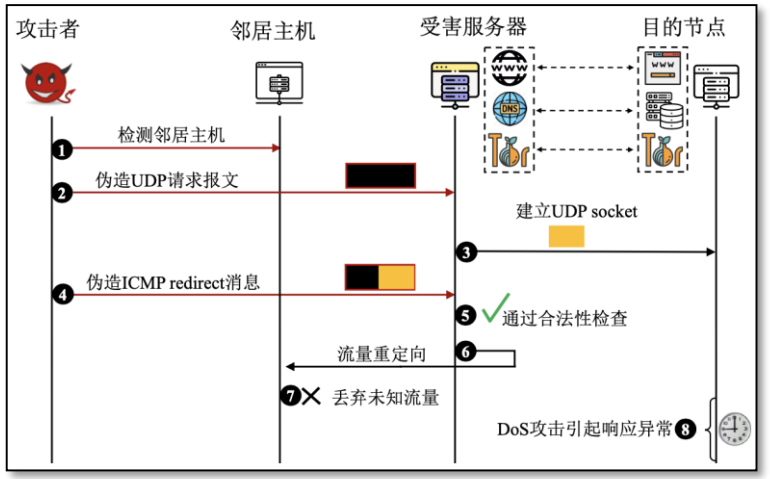
当前的互联网域间路由系统，建立在**自治系统间的弱信任模型**基础上，**默认**所有参与的自治系统是**诚实和可靠**的。这一设计缺陷越来越多的被攻击者利用，引发控制面、数据面以及上层应用的各类安全威胁。



引发上层攻击和安全威胁



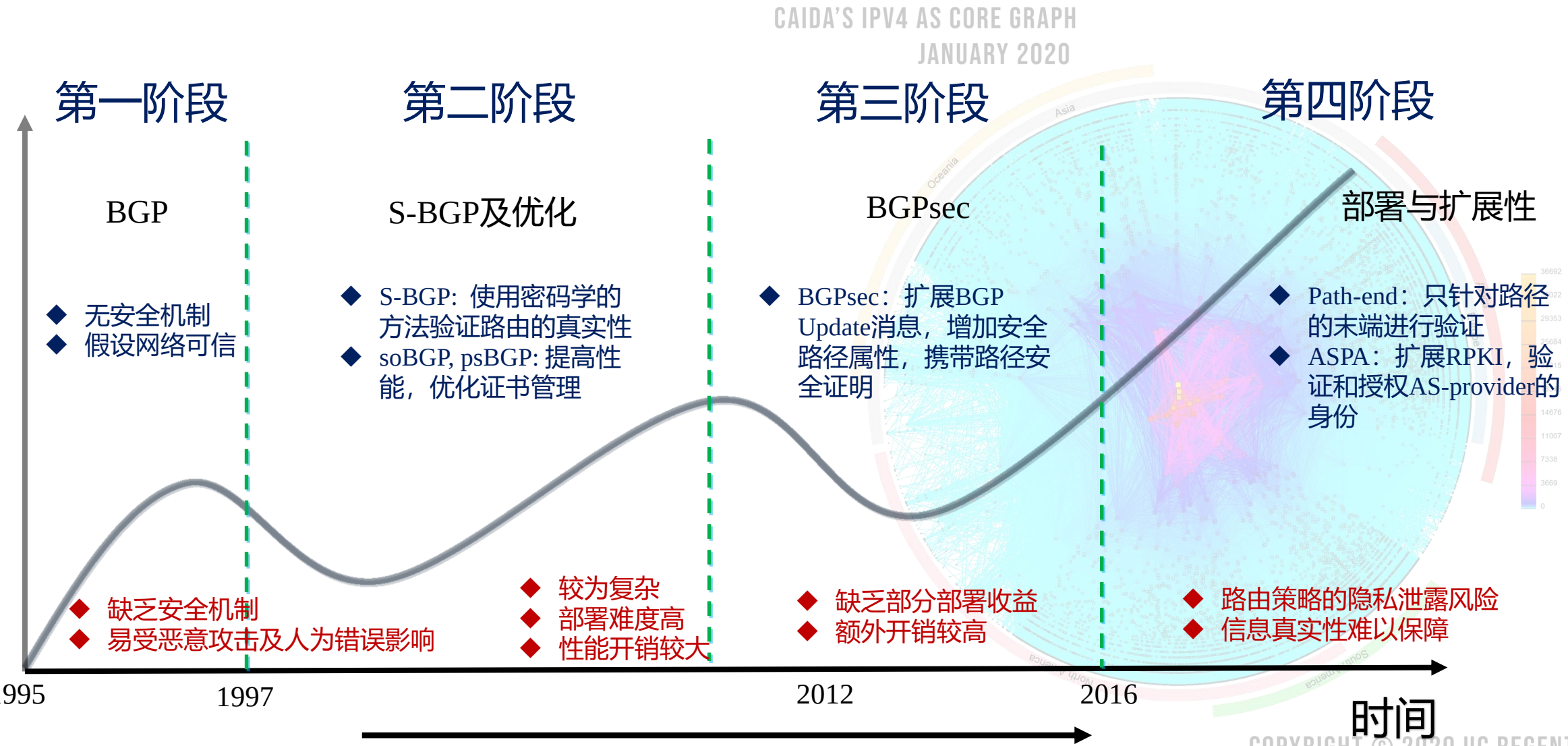
Off-path的TCP攻击



利用ICMP的网络流量重定向

根本原因之一，就是当前域间路由和转发协议的设计中，缺乏**有效的分布式验证机理和机制**。

域间路由宣告路径的验证机制



威胁模型与设计目标

前提假设

- 参与FC-BGP的自治系统均**接入**了互联网范围的**路由源验证**系统，例如RPKI或VRO，其中存储了关于自治系统ASN与合法前缀以及可验证公钥的映射信息。
- 不考虑域间的多径转发机制，例如域间TE、ECMP等。

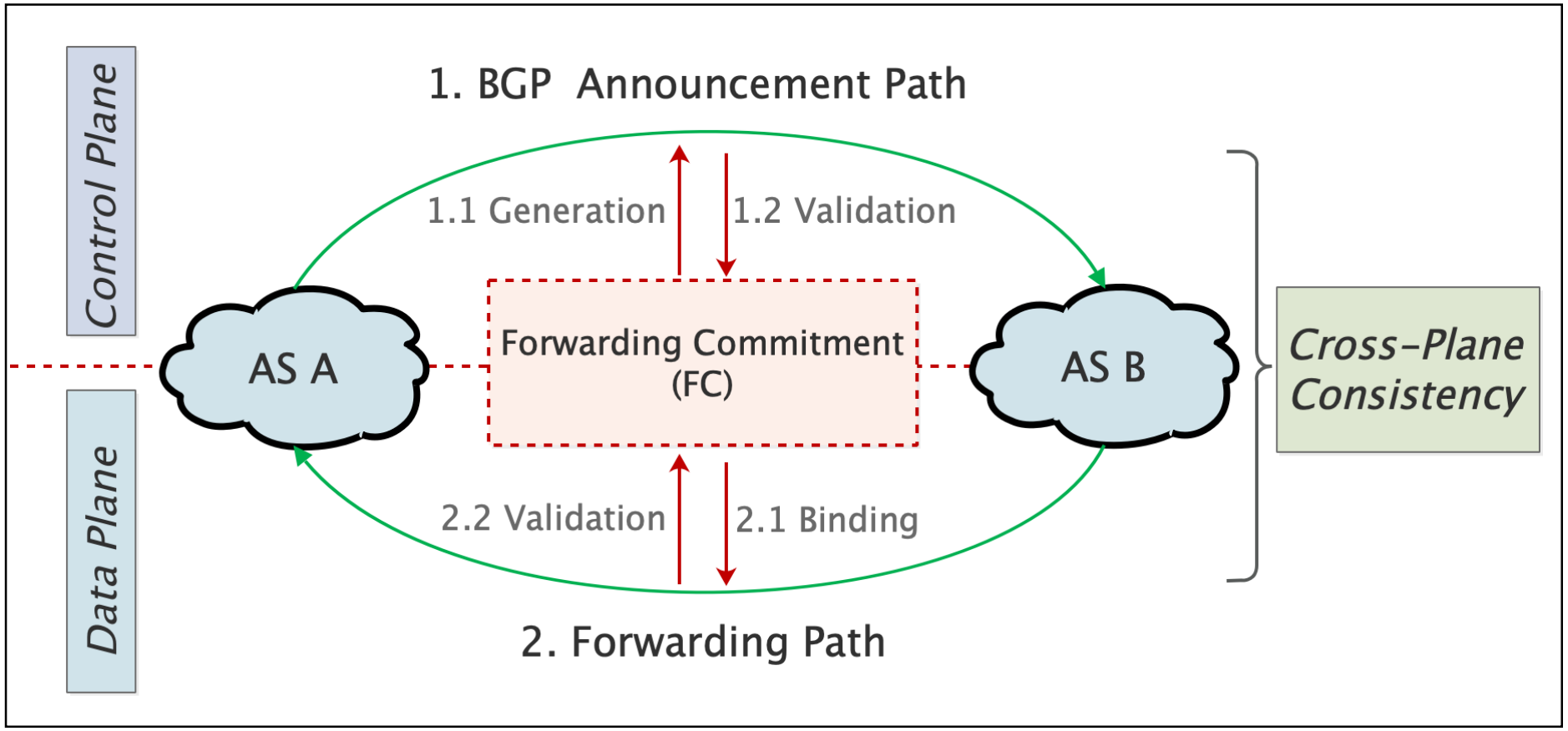
敌手模型

- 攻击者可以截获**全网范围内的任意BGP Update报文**（强敌手假设）。
- 攻击者可以**篡改**经过的BGP Update报文中的**AS-Path**，例如通过修改为更短的AS-Path进行流量劫持攻击。
- 攻击者可以发送**伪造源地址**的流量或**篡改**数据面流量的**转发路径**。
- 不考虑多个攻击者合谋的情况。

设计目标

- **控制面：** 当一条路由宣告路径上的所有节点均支持FC-BGP时，称为完全部署，否则为部分部署。当完全部署时，FC-BGP可以**保障AS-Path属性的真实性**（与BGPsec安全性相同）；当部分部署时，从源开始的**完全部署子路径越长**，整条路径**安全性越高**。
- **数据面：** 任何经过已部署FC-BGP节点的**伪造流量**（包括源地址伪造和转发路径篡改），**均能被识别**并按管理策略进行进一步处理（如标记或丢弃等）。

FC-BGP的核心设计思想



转发承诺：一种可验证路由编码

控制面跟随路由传播并验证FC

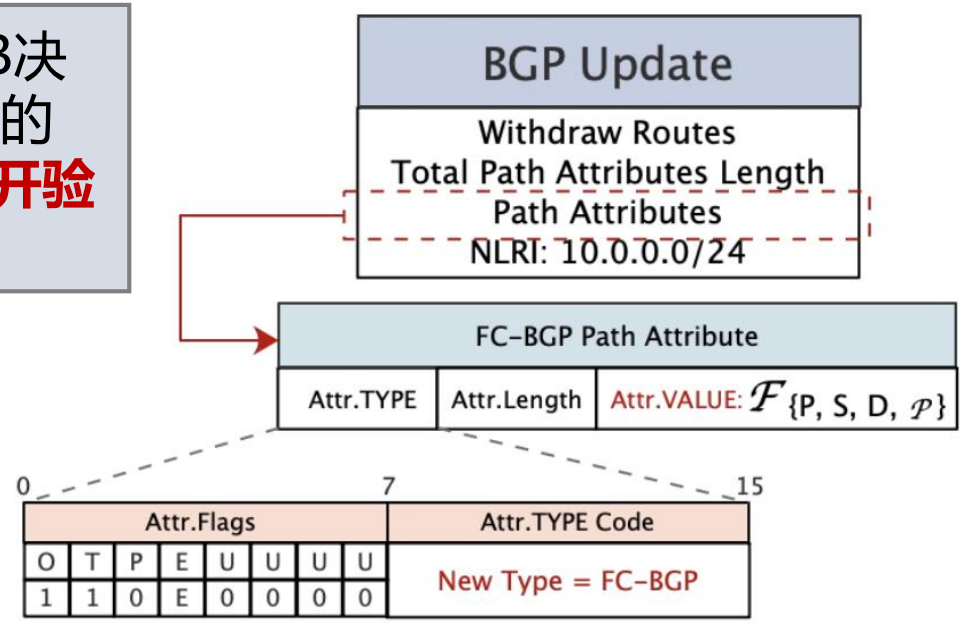
数据面根据路由选择反向传播FC

通过一种**可验证的路由信息编码**，在控制面**验证路由宣告路径**，在数据面**绑定**路由选择的**转发路径**，实现**跨层的一致性验证**能力。

转发承诺与双向验证

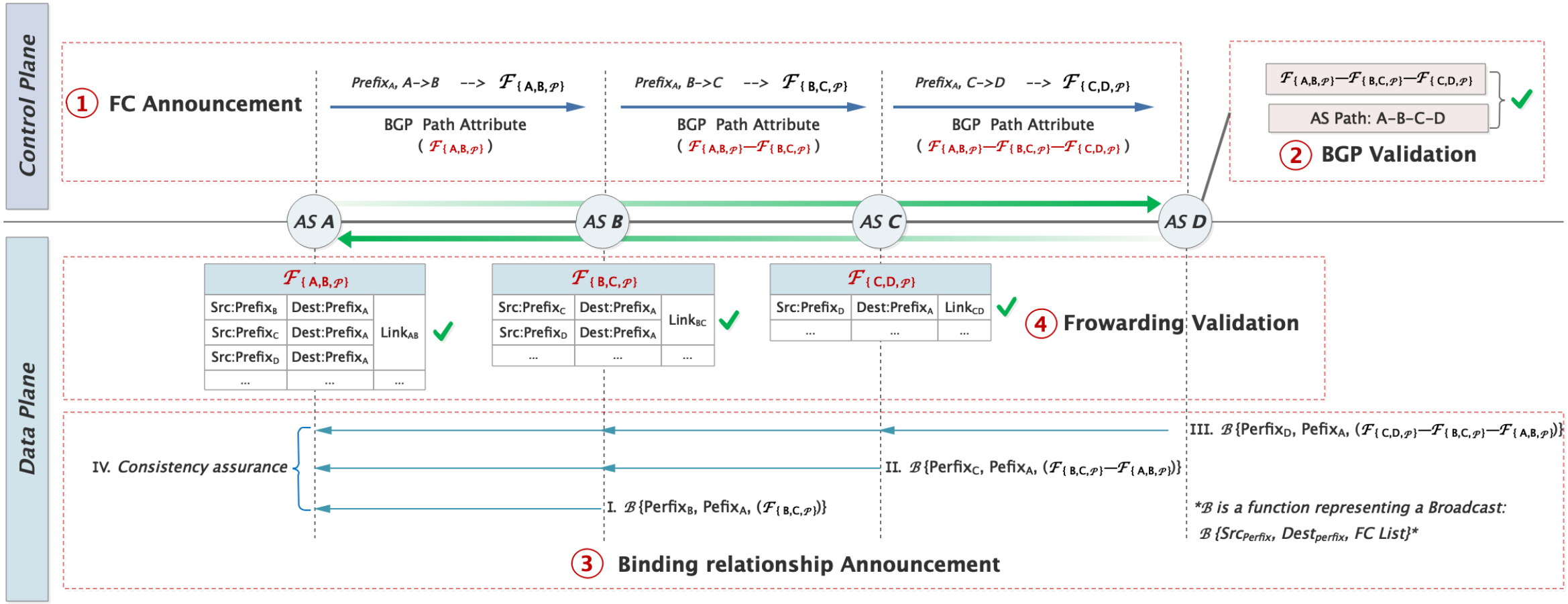
假设AS B收到一个BGP Update报文： P:$S \leftarrow A \leftarrow$ B，AS B决定将此路由继续传播给自己的邻居AS C。AS B将生成如下的**FC（Forwarding Commitment）**来向其它AS提供**可公开验证的路由意愿**。

$$\mathcal{F}_{\{A,B,C,\mathcal{P}\}} = \left\{ \mathcal{H}(A,B,C,\mathcal{P})_{\mathrm{Sig}_B} \,||\, \mathrm{A} \,||\, \mathrm{B} \,||\, \mathrm{C} \right\},$$



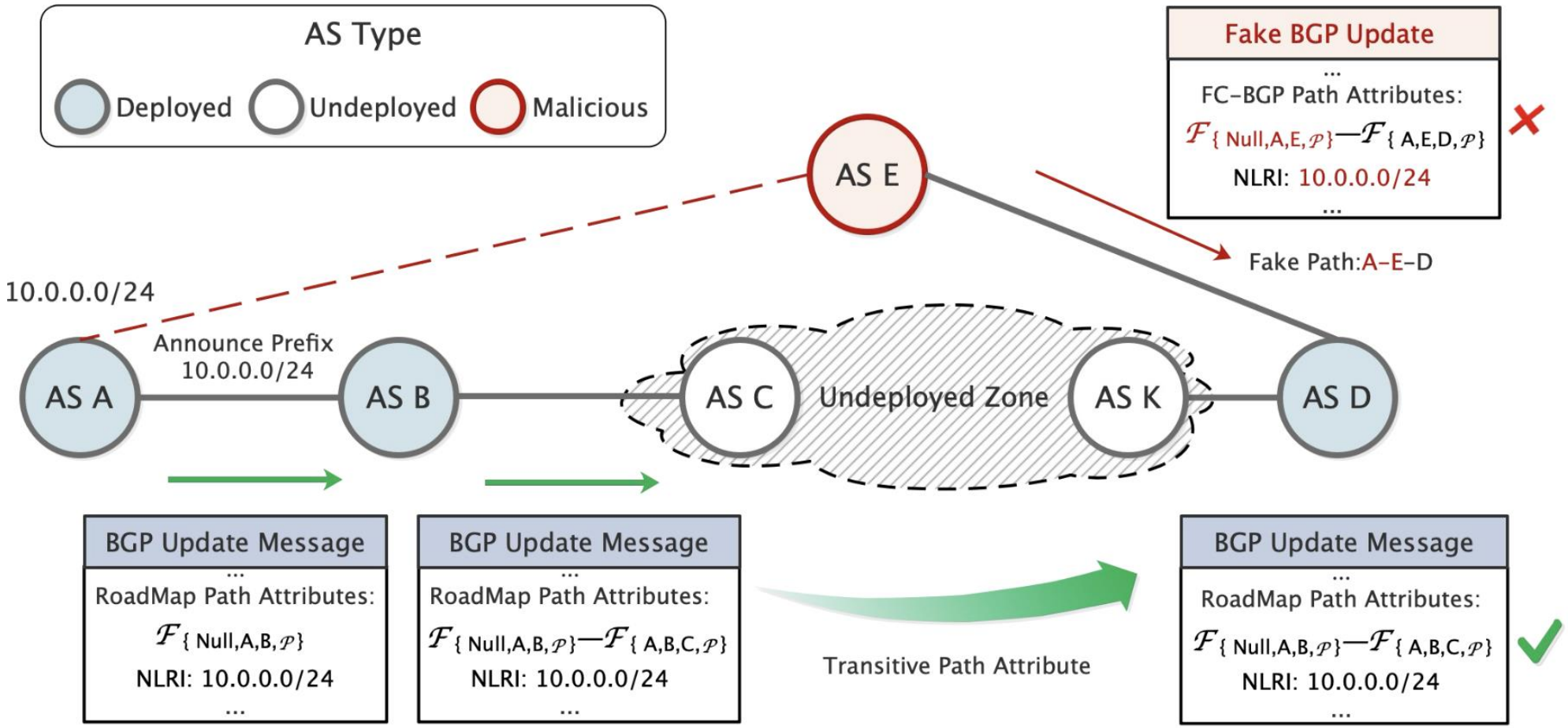
- FC-BGP设计了一种**逐段验证**路由宣告路径的机制，相比以BGPsec为代表的全路径验证机制，具备以下优势：
  - ✓ 完全部署时**相同的安全收益，与更低的验证开销**
  - ✓ **兼容部分部署场景**，提供此场景下明确的安全收益
- FC并**不会造成**额外的**路由策略隐私泄漏**

转发承诺与双向验证



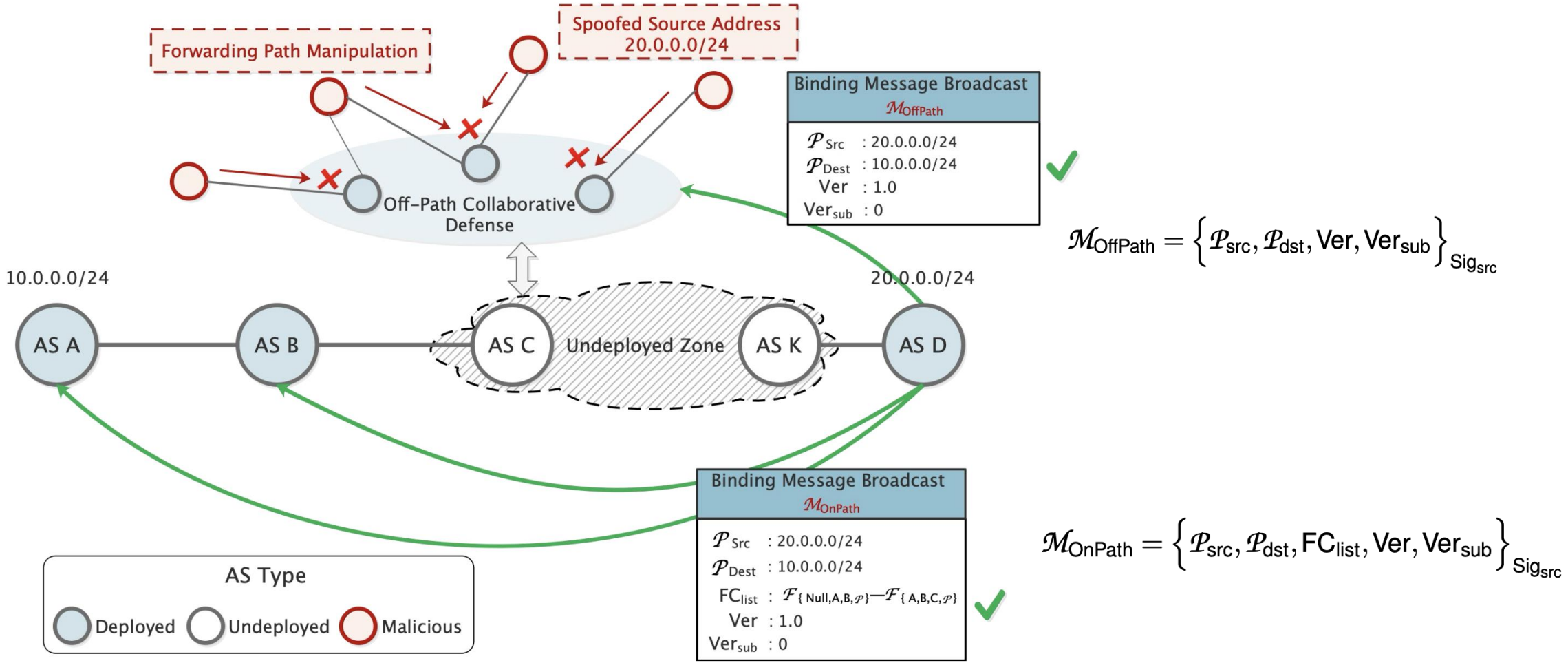
- **控制面：** AS A为控制面的源，发布前缀$Prefix_A$的路由并携带对应的FC，逐跳验证传播，实现路由宣告路径验证。
- **数据面：** AS D为数据面的源，选择D-C-B-A为转发路径，发送数据面绑定消息，On-Path节点建立相应过滤规则，实现数据面转发验证。

举例：路由路径验证



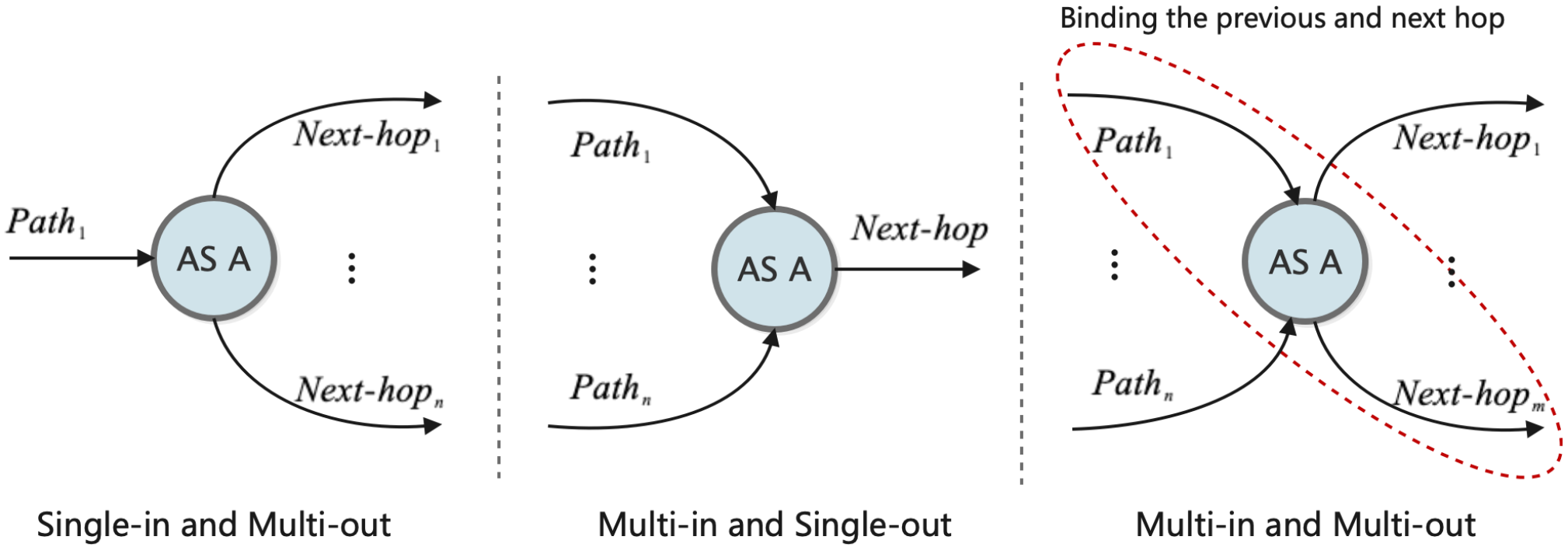
FC-BGP可以**穿越未部署区域**，不影响后续AS对已部署部分的验证。恶意节点（如AS E）因为**无法生成合法的FC片段**，伪造的短路径将被过滤。

举例：转发路径验证



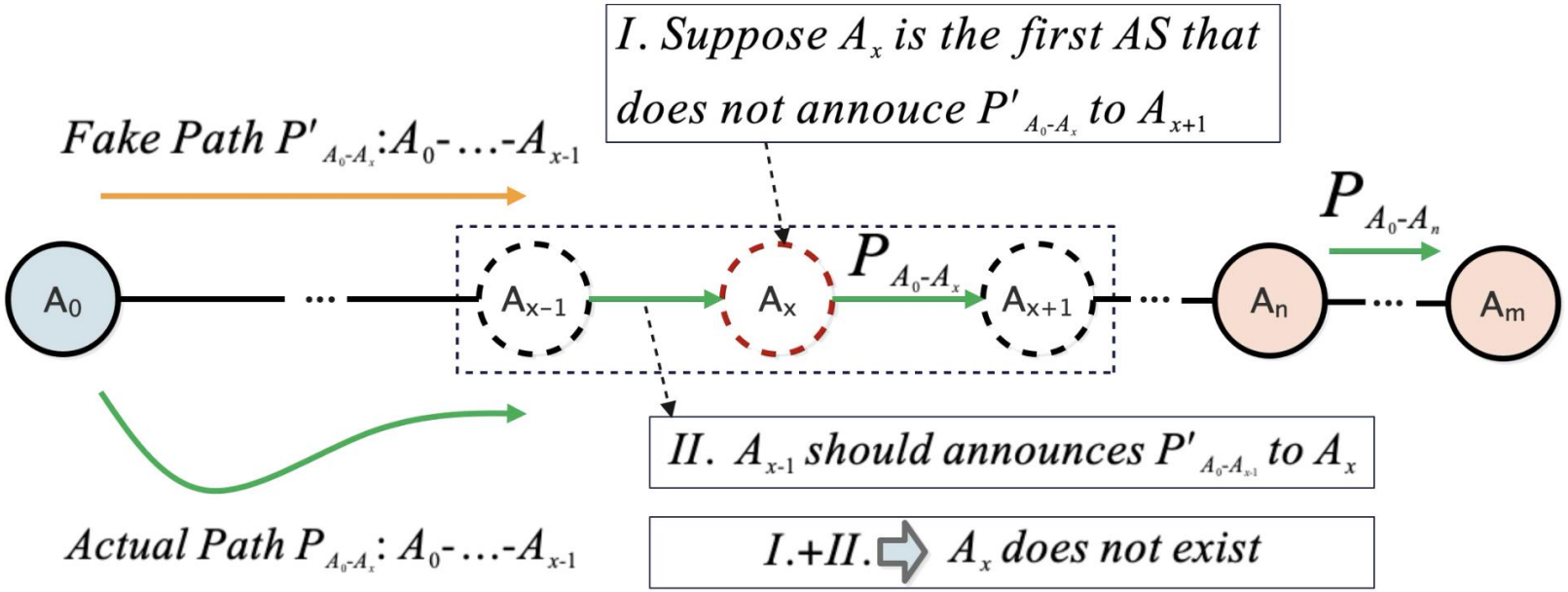
数据面的源端（AS D）可**发布转发路径绑定消息**，向On-Path和Off-Path节点宣告**合法流量和FC路径的绑定**关系，实现对伪造流量的识别和处理。

FC-BGP的安全性分析



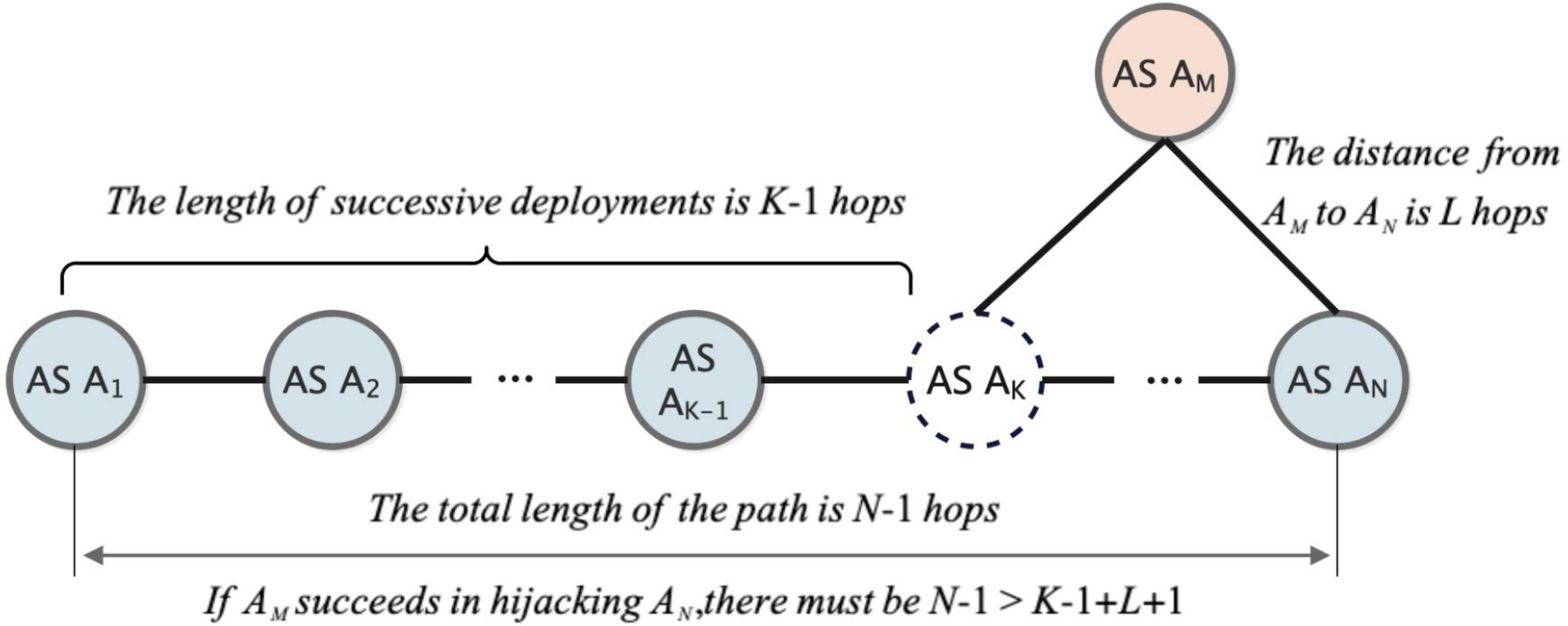
- 作为一种分段验证方案，保证FC-BGP安全性的核心在于**如何避免通过拼凑合法FC构造一条非法路径**。
- 节点私钥的安全性保证了**FC无法被伪造。**
- 拼凑合法FC仅可能出现在**多条路径的交汇点**，**“单进多出”**和**“多进单出”**均无法拼凑，仅有**“多入多出”**可能将前后两部分进行拼接。但**FC绑定前一跳和后一跳**的结构，使得“多入多出”也**无法将分别属于两条路径的FC进行拼接**。由此保证FC-BGP的安全性。

FC-BGP的安全性分析



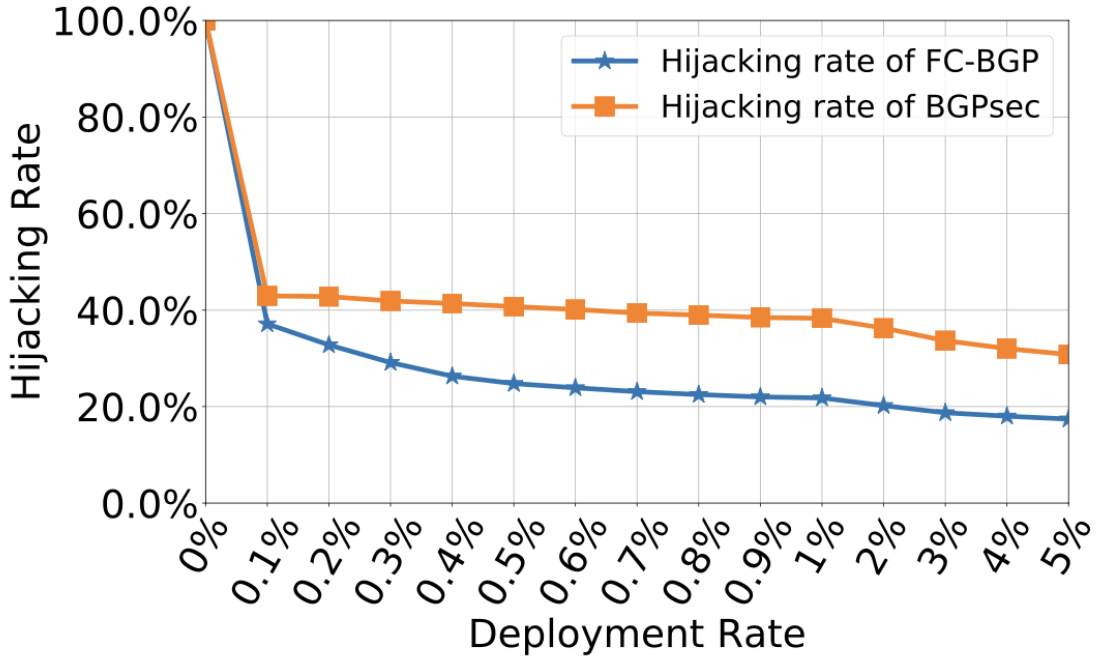
- 严格的安全性证明，详见FC-BGP的preprint链接： https://arxiv.org/abs/2309.13271
- 概括来讲，FC-BGP的机制设计，可以保障攻击者通过策略性的拼凑FC可以得到的任意最短AS-Path，均为实际宣告过的真实路径。换言之，**攻击者无法伪造出一条比实际路径更短的AS-Path。**

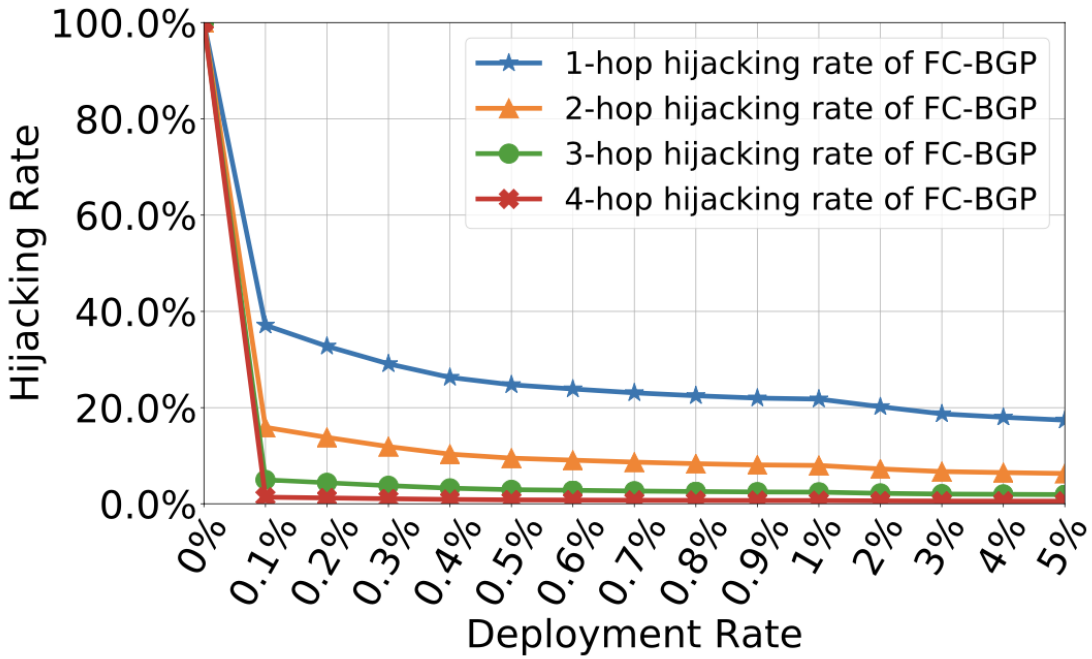
部分部署的安全收益



- 从源端开始连续部署的FC-BGP，**连续部署的跳数越多，攻击者必须距离被攻击者越近**。当部署跳数足够多时，攻击者将不再可能劫持目标流量。
- 例如A_1-A_2-A_3-A_4-A_5-A_6组成的5跳路径（互联网路由路径平均4.6跳），当A_1至A_3均部署后，攻击者仅能伪装为A_4的邻居。此时即便攻击者距离A6仅1跳，也无法伪造出比实际路径更短的路径来完成劫持，即**部分部署即可保障路径完全安全**。

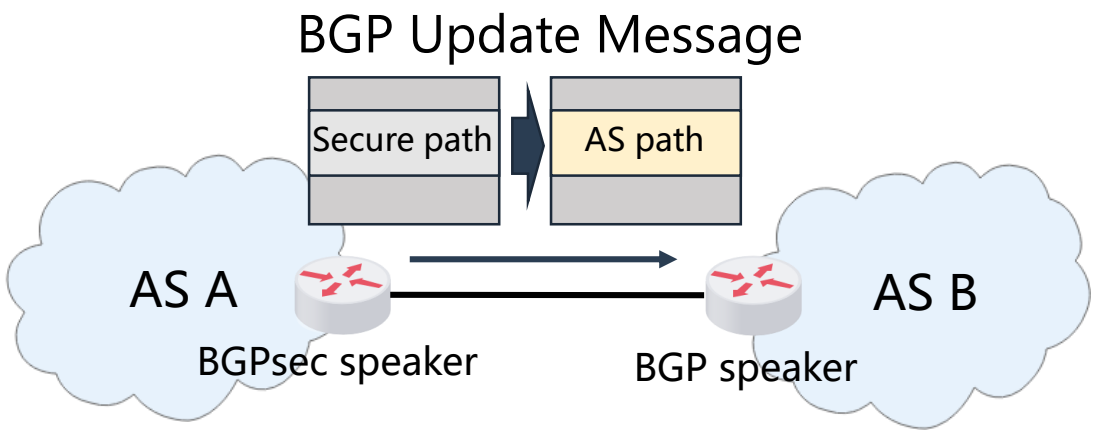
部分部署的安全收益

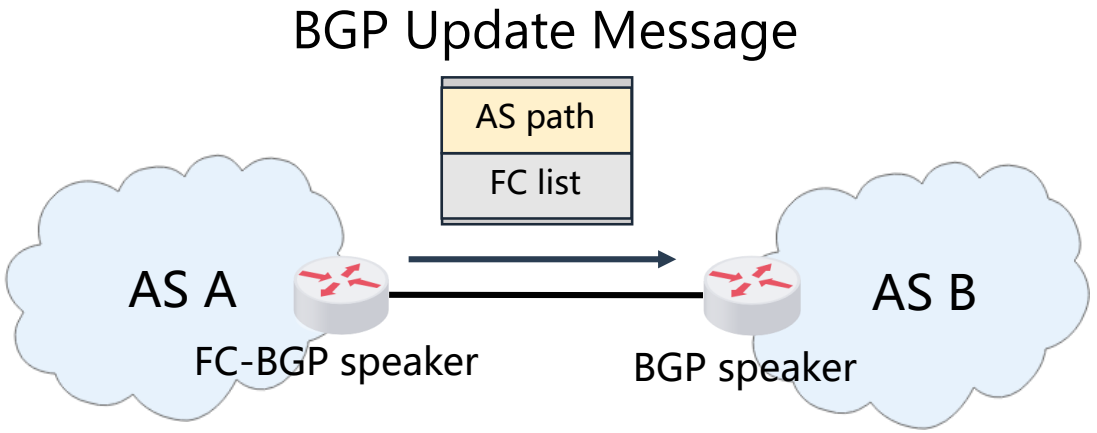




- 利用CAIDA 2023年9月路由数据库，将所有AS按照邻居数量降序排列，将前r%的AS部署FC-BGP后，计算所有已知路由路径的可被劫持比例，分析结果如图所示。
- 实验结果显示，相比要求全路径部署的BGPsec，**FC-BGP可以明确提供更多的安全收益，额外保障最多18%的路径的安全性。**

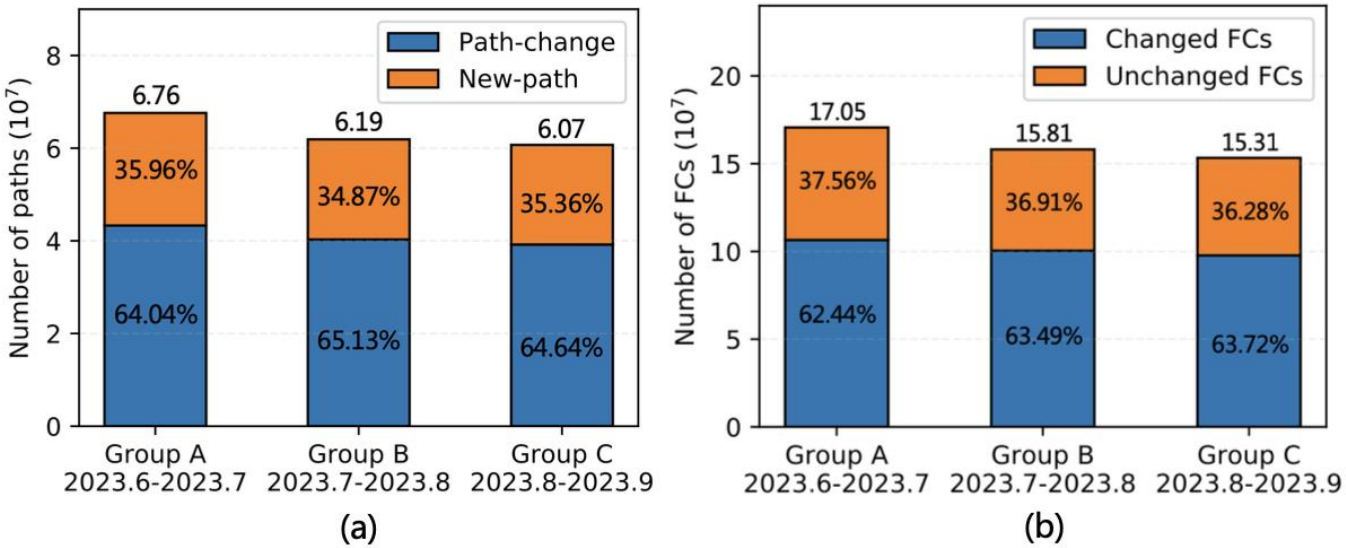
部分部署的兼容性



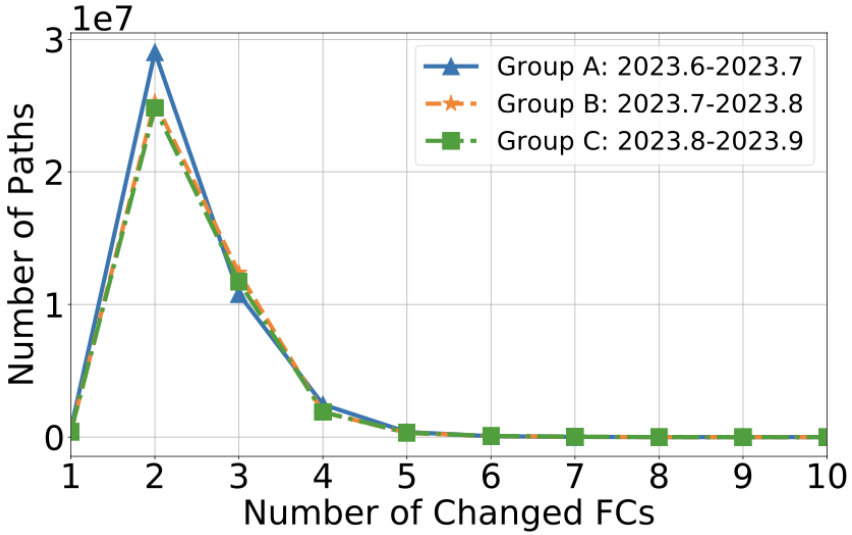


- 与BGPsec不同，FC-BGP并**不修改**标准BGP Update报文中的**AS Path字段**，而是增加一个新的可传递路径属性，用来携带路径对应的FC列表。
- 因此，FC-BGP具备对标准BGP协议的原生兼容性，**避免了**AS Path字段替换为Secure Path的额外操作和协商。

FC-BGP计算开销



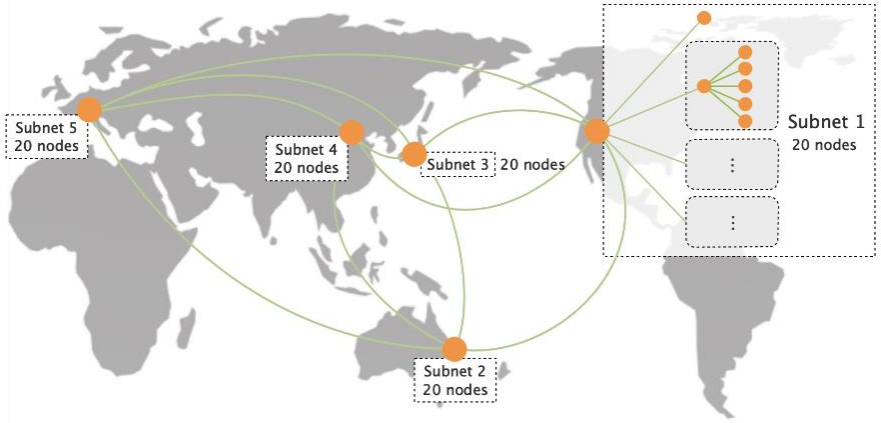
BGP更新的静态分析统计



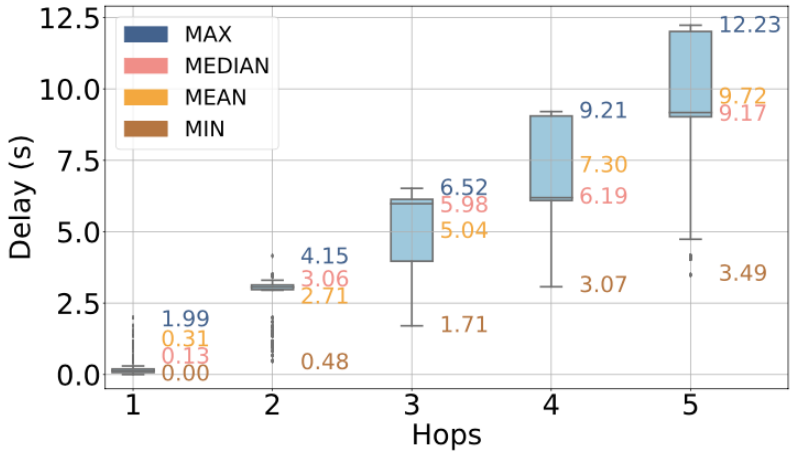
按照FC变化量细分后的路径数量分布

- 利用2023年6月至2023年9月的CAIDA互联网BGP宣告数据，分析并统计了互联网BGP路由的更新情况。
- **超过60%**的BGP路由更新，均**为路径部分变动**（Path-change），其中，**超过36%的FC保持不变的**，无需再次生成验证。
- **超过64%**的部分变动路径，其**变动的部分不超过2跳**，分段验证的**FC-BGP可以有效降低验证次数。**

FC-BGP计算开销



跨大洲的实验拓扑示意



FC-BGP的处理延迟

Table 1: Delay Comparison

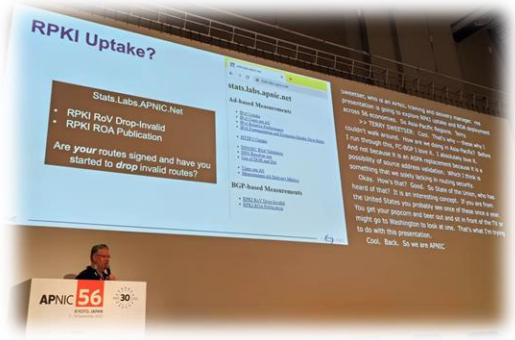
	Average	Max	Min
Intra-region delay	14.85ms	35.3ms	35.3ms
Inter-region delay	430.33ms	1099.74ms	80.34ms
RoadMap processing delay	0.025ms	0.23ms	0.013ms

FC-BGP处理延迟与传输延迟对比

- 基于FRRouting和VPP在x86平台实现了FC-BGP的原型，并在全球范围组建了100个节点的跨大洲实验床进行FC-BGP的性能实验。
- 实验结果显示，**单次FC生成大约为0.025毫秒**，与传输延迟相比，FC-BGP的处理延迟几乎可以忽略不计。2023年9月BGP宣告最多的AS6939，9月完成了138,286,813条宣告，其对应的全部FC可在71分钟内完成（虚拟机，3.7Ghz CPU，4G内存）。

标准化工作

APNIC 56



"...FC-BGP I love it, I absolutely love it. And not because it is an ASPA replacement because it is a possibility of source address validation. Which I think is something that we solely lacking in routing security...."

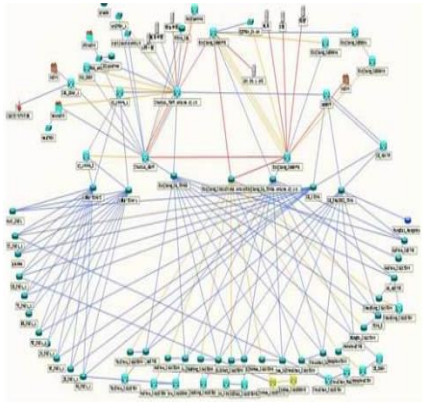
- 目前，研究组正在积极推动FC-BGP的标准化工作
- 2023年9月参加APNIC 56会议，FC-BGP得到了广泛关注和好评
- 2023年11月参加IETF 118会议，idr组内讨论了FC-BGP，受到广泛关注，得到BGPsec作者Sriram、idr主席Jeff和Keyur等的积极评价与建议

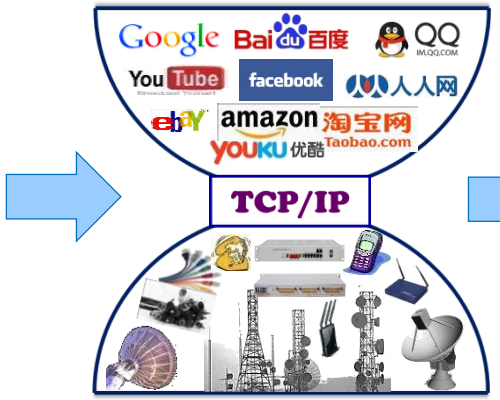
总结

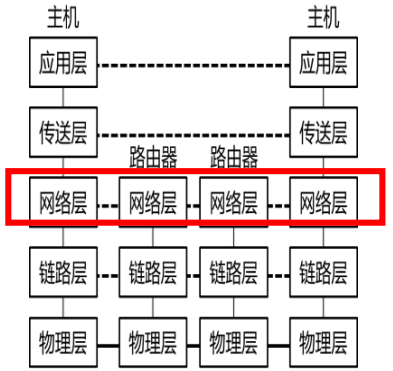
域间路由系统是互联网安全的基石

互联网路由系统是互联网连接各个网络的基础

承上启下，保证全网通达，是互联网的核心







- **路由学习**
- **数据转发**

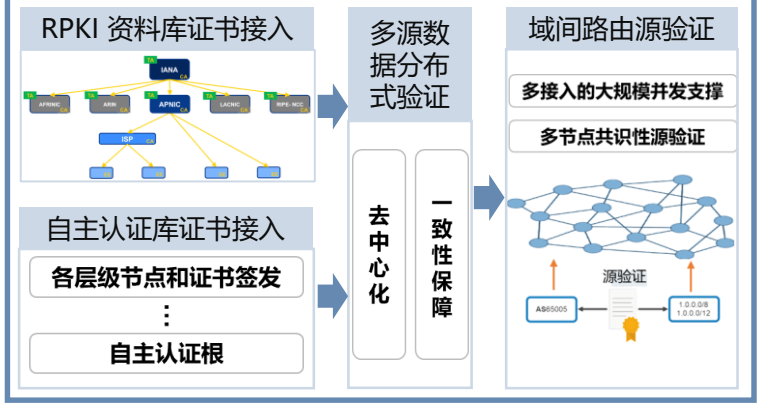
环境开放，行为复杂，信任缺失，攻击多样，
验证开销大，部署收益不明确，分布式验证困难

域间路由信任建立和高效传递
是互联网安全的关键难题

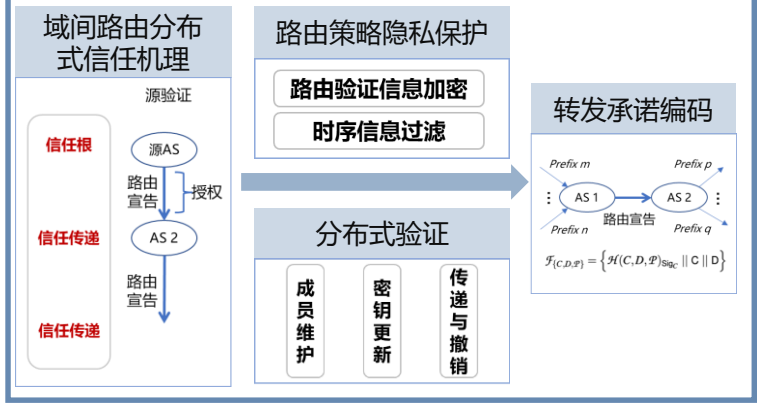
VRO和FC-BGP 新型域间路由安全体系

建立支持分布式验证和部分部署的新型路由系统安全技术体系，利用统一的核心机制，实现对路由起源、路由宣告和数据转发的完整保护，有效强化互联网路由系统安全防御能力，提升互联网治理水平。

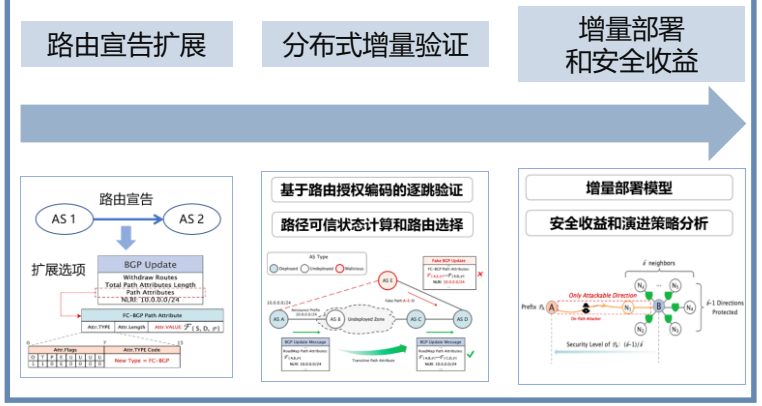
去中心化的域间路由可信源验证



域间路由分布式信任构建与路由授权



域间路由路径的分布式增量验证



突破 域间路由信任建立和高效传递关键问题

创新设计

提出 域间路由信息的去中心化安全源验证机制及域间路由通告的信任建立与传递

通过可验证的转发承诺实现域间安全路由与数据转发

谢 谢！