可信任下一代互联网与真实IPv6源地址验证

毕 军
CERNET国家网络中心
清华大学信息网络工程研究中心
网络体系结构和IPv6研究室主任
2008年10月

主要内容

- 互联网面临的技术挑战和安全可信问题
- 以真实IPv6源地址验证为基础的可信任下一代互联网
- 真实IPv6源地址验证技术
- 可信任下一代互联网的研究内容
- 总结

互联网面临的主要技术挑战

- 互联网已经取得了巨大成功，当前IPv4互联网已经成为全球信息基础设施的主体(80%)，这是当初设计互联网没有想到的。
- 当前互联网存在的主要技术挑战：
  - 扩展性：更大
  - 安全性：更安全
  - 高性能：更快，更可靠
  - 实时性：更及时
  - 移动性：更方便
- 安全问题成为目前互联网发展的最主要障碍之一，建设新一代可信任互联网成为互联网发展的主要技术难题

新一代互联网发展的历史机遇

- 新一代互联网和IPv6主要解决目前互联网的可扩展性、安全性、高性能、移动性和实时性等重大技术难题，实际上是重新设计新的互联网体系结构
- 全世界的科技人员目前站在同一起跑线上
- 抓住互联网更新换代的历史机遇，针对目前互联网存在的主要问题，在国际合作的环境下，设计和构造新一代互联网体系结构，在基础研究、技术攻关和应用示范方面取得一批创新性成果，具有重大战略意义

互联网虚假地址和标识问题

- 真实的地址和标识是可信任的基础和前提
- 现有互联网对分组来源不做验证，导致拒绝服务攻击、网络欺诈、垃圾邮件泛滥
  - 有一些网络攻击在原理上依赖于源地址伪造（例如反射式DDoS攻击）
  - 有一些网络攻击在原理上不一定依赖于源地址伪造，但是如果伪造了源地址，则很难追溯
- 大量使用地址转换(NAT)，不仅使分组来源的检查更加困难，而且破坏了互联网端到端的特性，给网络管理和计费带来困难

Some Figures- 2007 Arbor Worldwide Infrastructure Security Report

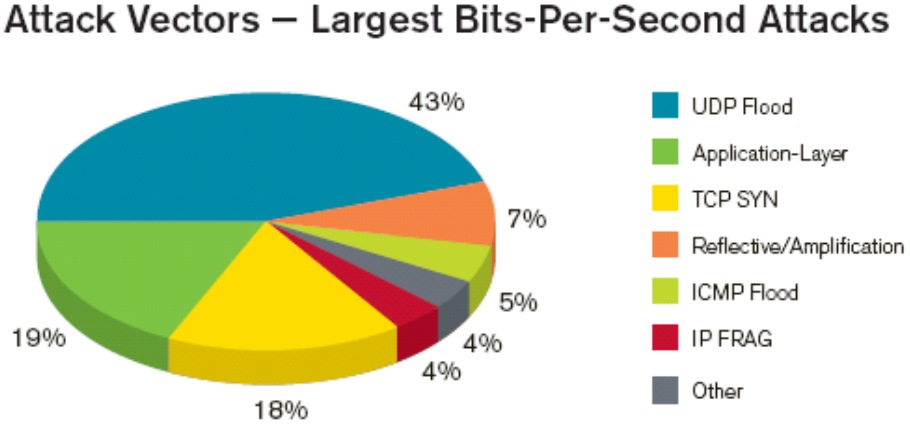


Figure 4: Attack Vectors – Largest Bits-Per-Second Attacks
Source: Arbor Networks, Inc.

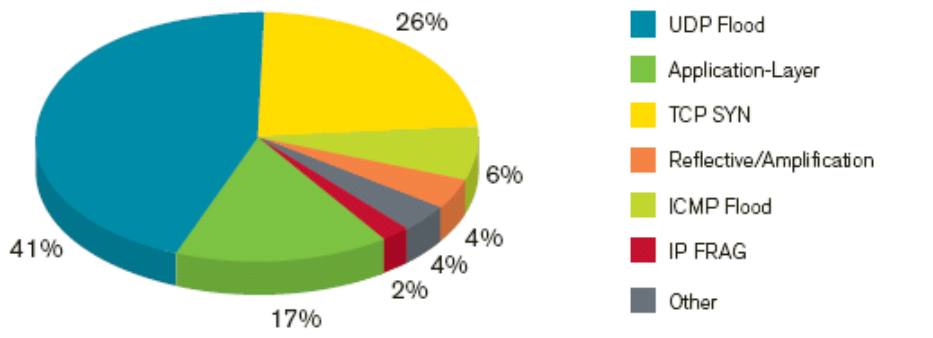


Figure 5: Attack Vectors – Largest Packets-Per-Second Attacks
Source: Arbor Networks, Inc.

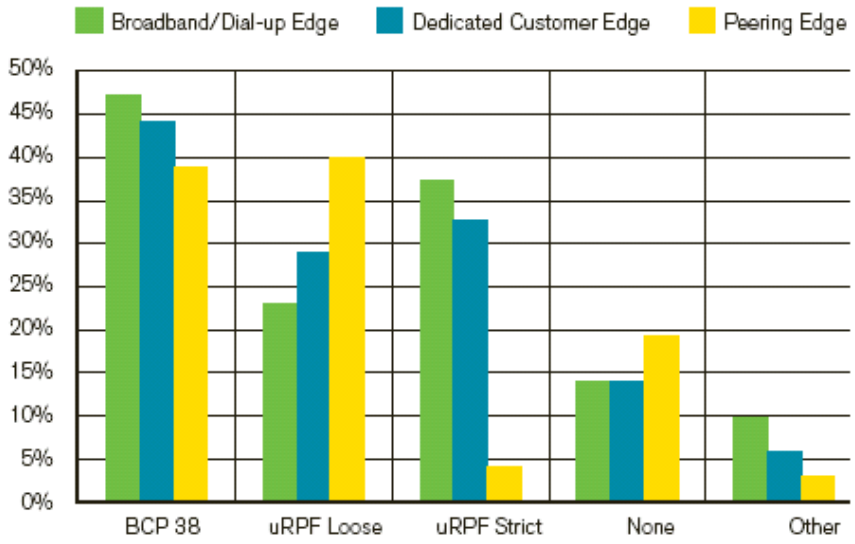


Figure 20: Application of Anti-Spoofing Techniques
Source: Arbor Networks, Inc.

以真实IPv6地址为基础的可信任一下代互联网

- Internet （R）evolution
  - 打补丁的解决方法 vs 体系结构的创新
  - Clean Slate Design vs Incremental Design
- 真实IPv6地址是可信任下一代互联网的基础
- “真实IPv6地址”是在新一代互联网中实现目的地址寻址和源地址认证相结合的新的互联网寻址体系结构，有望成为解决新一代互联网安全可信问题的创新性解决方案，同时还望解决其他问题
  - 网络管理（trace back）
  - 网络测量的准确
  - 基于源地址的计费
  - 提供高质量的端到端服务

涉及的国家项目和课题

基础理论： 国家973计划项目(2003CB314800)
“新一代互联网体系结构理论研究”

关键技术： 国家863重点课题“可信任下一代互联网关键技术及其应用示范研究”(2005AA121130)

试验网络： 中国下一代互联网示范工程CNGI示范网络核心网
CNGI－CERNET2/6IX
（发改高技2003－2057号）

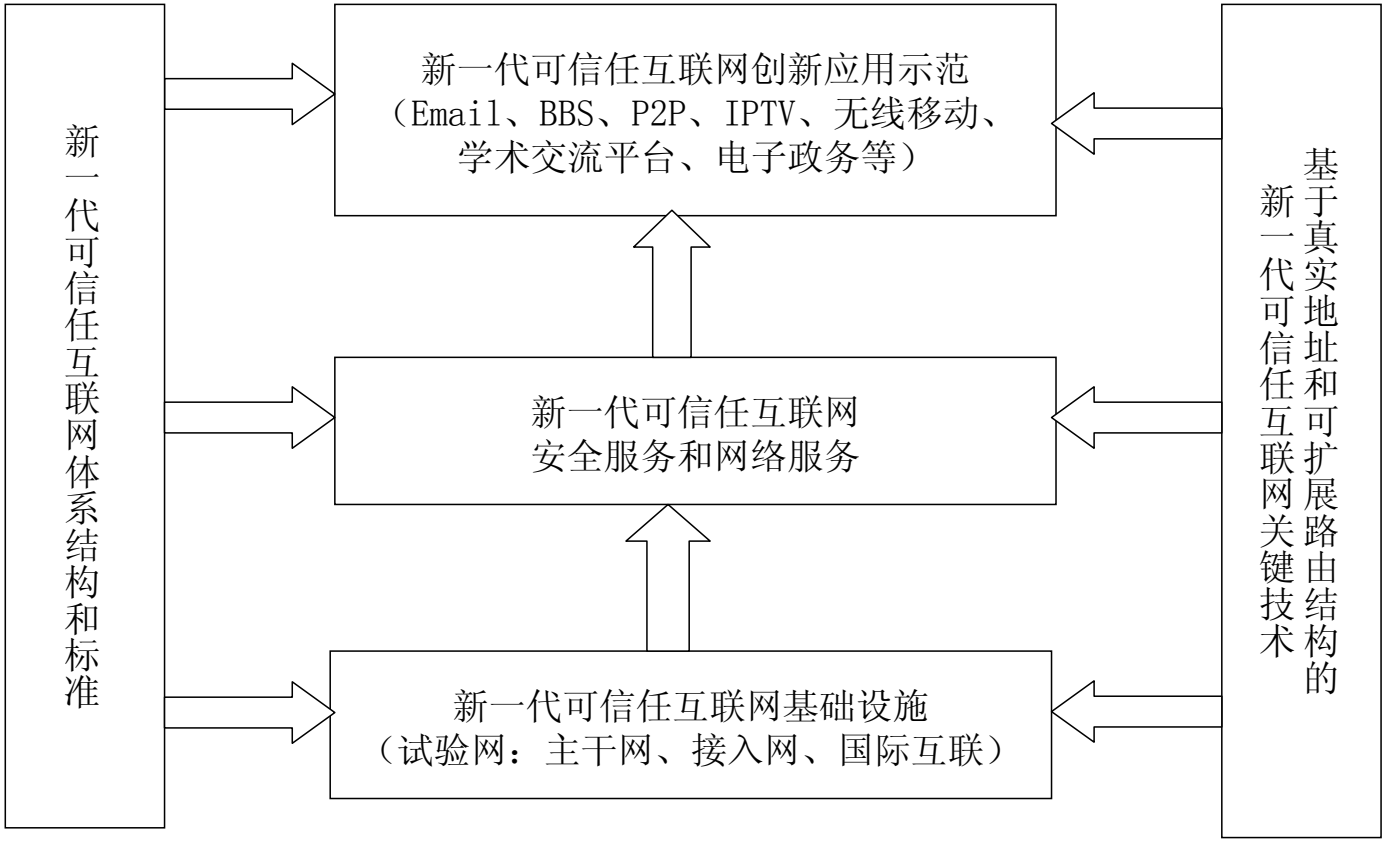
完善和推广部署：
国家科技支撑计划
“十一五”重大项目
“可信任互联网”

2003 2004 2005 2006 2007

总体目标

- 针对互联网的安全可信问题，研究新一代可信任互联网体系结构，突破基于真实地址和可扩展路由结构等新一代可信任互联网关键技术，提出相关标准
- 建设中国新一代可信任互联网试验网
  - 覆盖全国20个城市、25个核心节点的新一代可信任互联网试验网主干网
  - 分布在全国、接入主干网核心节点的50～100个新一代可信任互联网试验网接入网，接入用户规模达到100～200万人
  - 在建立国内新一代可信任互联网的技术试验与验证环境的基础上，在中欧之间实现2.5Gbps高速互联，建立新一代可信任互联网国际化研究试验环境
- 依托建成的中国新一代可信任互联网试验网，开展新一代可信任互联网安全服务和网络服务技术研究与试验
- 基于建成的中国新一代可信任互联网试验网，研究新一代可信任互联网创新应用示范

研究内容的总体结构


新一代可信任互联网体系结构和标准
新一代可信任互联网创新应用示范
（Email、BBS、P2P、IPTV、无线移动、
学术交流平台、电子政务等）
新一代可信任互联网
安全服务和网络服务
新一代可信任互联网基础设施
（试验网：主干网、接入网、国际互联）
基于真实地址和可扩展路由结构的
新一代可信任互联网关键技术

主要研究内容

- 新一代可信任互联网体系结构和相关标准
- 新一代可信任互联网关键技术
- 新一代可信任互联网服务技术
- 新一代可信任互联网试验网
- 新一代可信任互联网创新应用示范

新一代可信任互联网体系结构和相关标准总体研究—研究内容

- 新一代可信任互联网的总体设计
- 新一代可信任互联网的设计原则和目标，面向不同的应用设计可信任互联网功能框架和体系结构
- 新一代可信任互联网体系结构相关标准
- 项目的总体组织、协调和管理
- 项目测试，对各课题的测试和项目范围的集成测试

新一代可信任互联网
真实地址关键技术—研究内容

- 基于真实地址的核心主干网关键技术
  - 研究真实IPv6地址访问体系结构，支持增量部署并具有激励机制，体现谁部署、谁受益的特点
  - 研究域间信任关系建立和维护方法以及域间真实地址验证方法和真实源地址前缀的映射方法，包括算法和协议、网络设备的支持技术等
  - 研究域内子网间信任关系建立和维护方法以及域内真实地址验证方法，包括算法和协议、网络设备的支持技术等
- 基于真实地址的接入网关键技术
- 目前互联网向新一代可信任互联网过渡或互通的关键技术
- 提交相关标准、申请发明专利
- 方法和系统在新一代可信任互联网试验网内通过验证

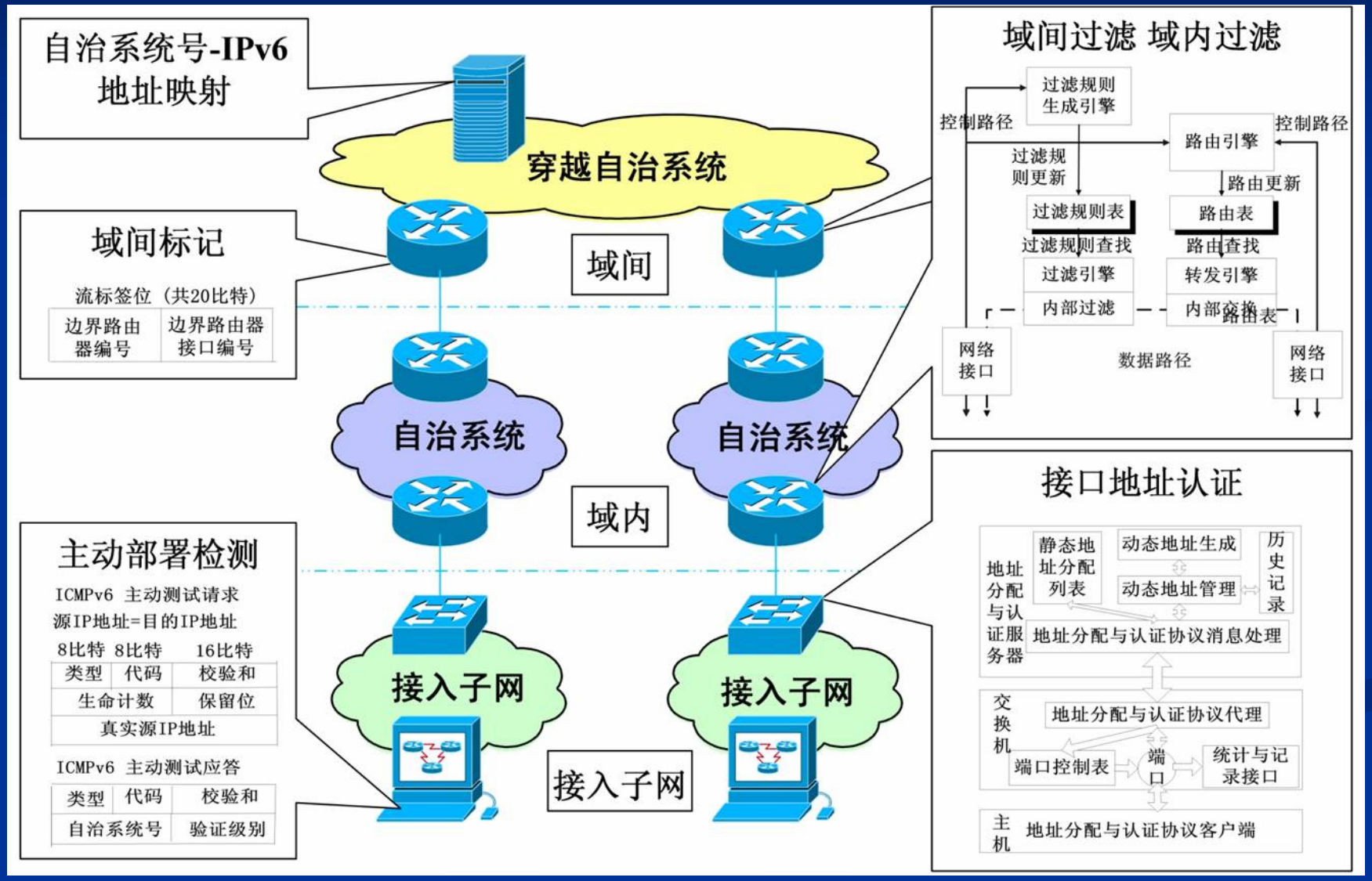
已经取得的一些阶段性成果

- 初步提出了真实地址体系结构和域间、域内、接入网三个层次的源地址验证方法,发表一批学术论文，申请发明专利若干
- 在CNGI-CERNET2进行了一定规模的部署
- 2008年5月，在国际互联网标准化组织IETF推动成立SAVI工作组(Technical Advisor:吴建平，Secretary:毕军）
- 2008年6月，RFC 5210（吴建平、毕军、李星等)获得IETF通过，是我国第一个非informational类的RFC

SAVA Design Principles

1. Hierarchical Architecture (Multi-fence solutions)
2. Solutions for IPv6 first (feasible way to deploy)
3. Proactive protection
4. Incrementally Deployable (Incomplete deployment still be beneficial)
5. Provide incentive for deployment (The source address space of a network that deployed SAVA can not be spoofed by others)
6. Performance, Cost and Scalability

真实IPv6源地址验证体系结构



SAVA Solutions

- Inter-AS
  - Early stage: APPA (lightweight end-to-end signature between the source AS and the destination AS)
  - Neighboring ASes: ARBIF (AS relationship based method deployed in the neighboring AS boarder routers)
- Intra-AS: DVF
- Access Network：来自IPv6的要求和接入网的复杂性

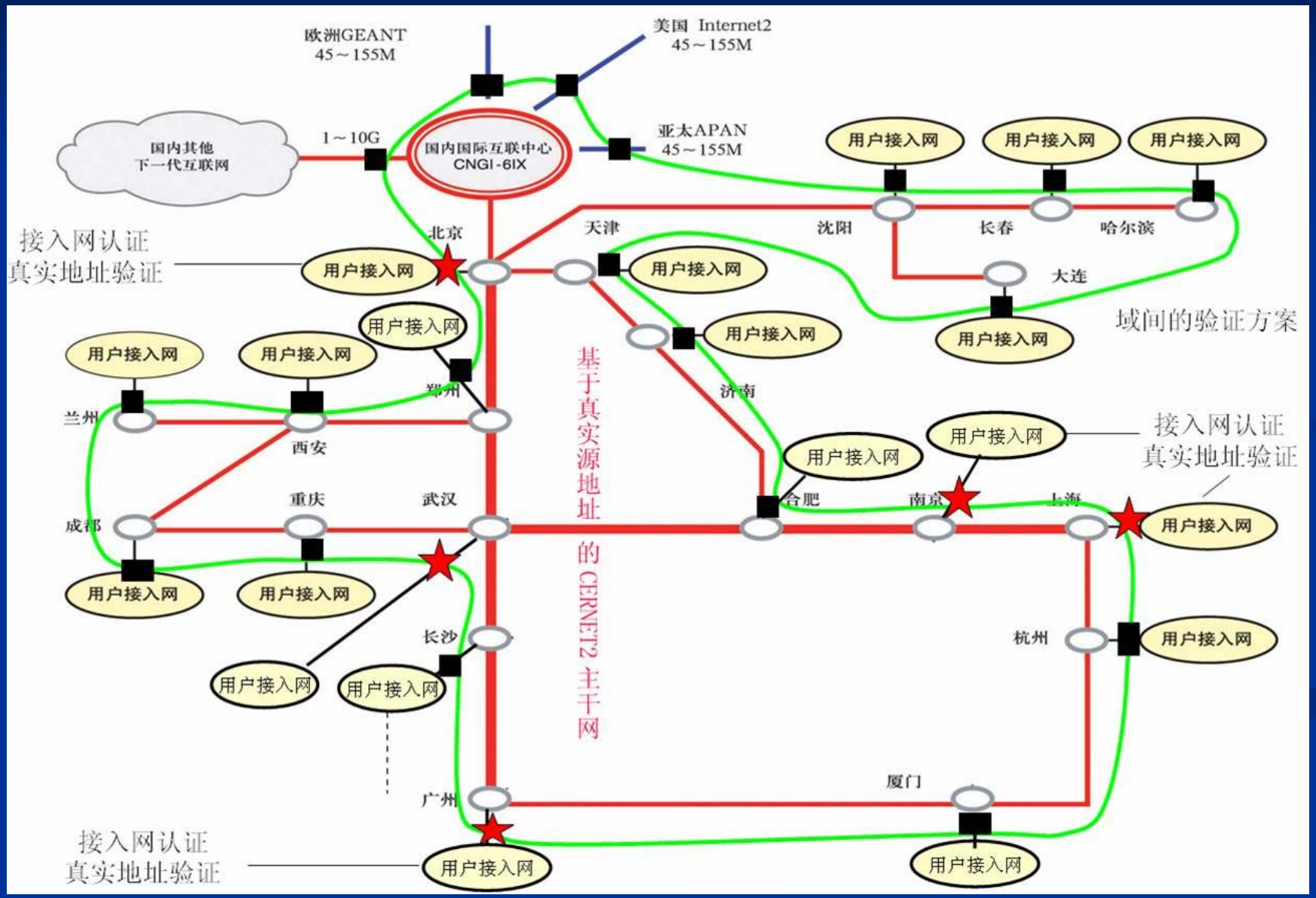
SAVA Solutions

- Access Network：来自IPv6的要求和接入网的复杂性
  - 多种地址分配方式
    - Stateless, DHCPv6, 静态，CGA, Privacy
  - 如何确定Location信息
    - Routers and hosts with multiple interfaces
    - Nodes that use multiple IP addresses are assigned to an interface
    - Nodes that have multiple link-layer addresses on the same interface
    - Nodes that have multiple interfaces to the same link
    - Nodes that move to another port on the same link
    - Hosts with anycast addresses
    - Hosts connected with WiFi
    - Host Layer2 mobility

Current SAVA Solutions

- Access Network
  - First Layer 2 Hop
    - 新的IPv6地址分配方式
    - IP地址与低层Trust Anchor的绑定
  - First Layer3 Hop: CSA
    - 适应于目前已有IPv6地址分配方式Stateless, DHCPv6, 静态， CGA, Privacy
    - IP地址与高层Trust Anchor的绑定，基于CGA地址做ID
    - 具有一定移动性

在CNGI-CERENT2主干网上的部署



IETF的工作

- IETF 66 (Montreal, July 2006), SAVA Side Meeting with IAB/IESG
- IETF 67 (San Diego, Nov 2006), Internet Area Open Meeting
- IETF 68 (Prague, March 2007), first BoF Discussion
- IETF 69 (Chicago, July 2007), RFC drafts proposed, Internet Area Open Meeting and SAVA Side Meeting with IESG to prepare the 2nd BoF
- IETF 70 (Vancouver, Dec. 2007), BoF for SAVI Working Group (Source Address Validation Improvements)
- IETF 71 (Philadelphia, March 2008), discuss/revise WG charter
- RFC 5210 and SAVI WG were approved by IESG in May 2008
- IETF 72 (Dublin, July 2008), the first SAVI WG meeting
- To Subscribe: https://www.ietf.org/mailman/listinfo/savi

新一代可信任互联网可扩展路由关键技术

- 路由的可扩展性问题研究
  - 研究可信任的、支持真实IPv6地址访问的域间路由体系结构
  - 支持未来可信任互联网的大规模部署，支持目的地址信息和真实IPv6源地址信息的安全可信分发，支持多路径路由和面向突发流量的路由优化
- IP地址语义重载问题研究
  - 区分路由标识和主机标识，保证在路由不变的情况下上层应用的灵活性
  - 为分布式计算、移动、multi-homing等应用提供底层支持
- 可信任路由和保证服务质量路由问题研究
  - 研究跨域路由的服务质量问题。在可信任互联网的体系结构下根据需求、资源情况和互联协议提供保证服务质量的算法、协议和标准
- 跨域组播问题问题研究
  - 在可信任互联网的体系结构下研究跨域组播的算法和协议

新一代可信任互联网安全和网络服务

- 安全服务
  - 实体标识和身份认证
  - 基于信任的资源管理和访问控制服务
- 网络服务
  - 大规模可扩展组播服务
  - 可信任互联网中的服务质量控制技术
  - 可信任互联网的流量工程和协议测试技术
  - 可信任互联网的网络管理和安全监控技术

新一代可信任互联网试验网

- 新一代可信任互联网试验网的规划和设计，构造新一代可信任互联网试验网
- 基于新一代可信任互联网试验网，对可信任关键技术进行试验和验证
- 为开展关于安全服务、网络服务等新一代可信任互联网服务技术研发提供网络基础设施
- 为部署和试验新一代可信任互联网创新应用提供网络基础设施，支持具有一定用户规模的创新应用
- 与国际下一代互联网互联，支持国际化的技术合作与试验；与国内运营商的下一代互联网试验网互联，探索新一代可信任互联网试验网向商业网的扩展；配合开展重大行业应用试验，探索新一代可信任互联网的应用推广

新一代可信任互联网创新应用示范

- 新一代可信任互联网基础应用
- 新一代互联网视频应用
- 新一代无线移动互联网应用
- 新一代可信任的电子政务应用

新一代可信任互联网基础应用

- 研究内容
  - 基于真实地址的可信任电子邮件系统
  - 基于真实地址的可信任电子公告牌系统BBS
  - 基于真实地址的P2P应用

新一代互联网视频应用

- IPTV和互动电视
  - 建设IPTV和互动电视iTV应用示范点，实现可控、可管和可信的要求
  - 在IPTV基础业务之上开发增值业务
  - 研制支撑各类IPTV增值业务的运营管理系统

新一代无线移动互联网应用

- 研究内容
  - 大规模分布式无线多媒体通信应用支撑平台
  - 大规模分布式无线移动多媒体通信应用示范系统
  - 宽带无线移动多媒体通信运行管理系统

新一代可信任的电子政务应用

- 研究内容
  - 为电子政务构建可信任的互联网基础设施
  - 为电子政务的各种应用提供统一的安全服务平台
  - 建立可信任的电子政务关键应用系统

总 结

- 以真实地址为基础，突破互联网的可信任性难题，提高我国自主创新能力，提升我国相关产业核心竞争力，提升我国国际学术地位和影响力
- 建立一定规模的新一代可信任互联网试验网，成为我国科技创新基础平台，有利于新一代可信任互联网的应用推广
- 基于与国际下一代互联网高速互联建立的国际合作研究试验平台，有助于形成由我国主导的国际标准
- 可信任互联网技术的推广应用，将在新一代互联网领域创造新的经济增长点，对经济和社会发展产生巨大的推动作用
- 建立新一代可信任互联网，可以强化互联网网络和信息安全管理，从信息基础设施的层面为保障国家安全、促进社会发展和人民生活水平的提高提供了良好的基础和有力的保证