互联网内生安全体系结构研究进展

徐 恪[1,2,3] 付松涛[1,2] 李 琦[2,4] 刘冰洋[5] 江伟玉[5] 吴 波[5] 冯学伟[1,2]

[1](清华大学计算机科学与技术系 北京 100084)

[2](北京信息科学与技术国家研究中心 北京 100084)

[3](鹏城实验室 深圳 518000)

[4](清华大学网络科学与网络空间研究院 北京 100084)

[5](华为技术有限公司 2012 实验室 北京 100085)

摘 要 随着互联网不断发展，网络功能逐步走向万物互联下自动交互与控制，大数据、云计算、边缘计算等技术不断深入应用，传统网络面临的源地址欺骗、DDoS 攻击、路由劫持等安全问题仍然存在，新的应用场景使用户面临更严重的安全问题，现有互联网体系结构面向性能的设计难以承担网络安全的需求. 互联网安全问题的根源在于体系结构设计时没有考虑安全需求，缺乏用户与网络的信任根基，由于体系结构设计缺失带来的问题应该从体系结构设计本身寻找解决方案. 设计自带安全属性和安全能力的体系结构，通过内生的方式提供网络安全，能够从根本上提升网络安全性能. 本文深入研究和总结了近年来针对互联网安全问题提出的各类解决方案，对方案的安全特性进行了分析，在此基础上提出了构建互联网内生安全体系结构的思路.

关键词 互联网；内生安全；互联网体系结构

中图法分类号 TP391 **DOI 号** 10.11897/SP.J.1016.2021.02149

The Research Progress on Intrinsic Internet Security Architecture

XU Ke[1,2,3] FU Song-Tao[1,2] LI Qi[2,4] LIU Bing-Yang[5] JIANG Wei-Yu[5]
WU Bo[5] FENG Xue-Wei[1,2]

[1](*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084)

[2](*Beijing National Research Center for Information Science and Technology, Beijing* 100084)

[3](*Peng Cheng Laboratory, Shenzhen* 518000)

[4](*Institute for Network Science and Cyberspace, Tsinghua University, Beijing* 100084)

[5](*2012 Labs, Huawei Technology Co. Ltd., Beijing* 100085)

Abstract With the development of the Internet, the functionality of the network extends to the automatic interaction and control under the interconnection of things. The security problems of the traditional network such as Source Spoofing, DDoS attack, and Route Hijacking still exist. At the same time, the technology of Big Data, Cloud Computing, as well as Edge Computing is applied to the Internet, brings new security problems. Therefore, the user in the network faced more security problems. The traditional Internet architecture, which is designed towards performance and lacks the foundation of trust between the users

收稿日期：2020-03-20；在线发布日期：2020-09-02. 本课题得到国家重点研发计划课题(2018YFB0803405)、国家杰出青年科学基金(61825204)、国家自然科学基金(61932016, 61802222)、北京高校卓越青年科学家计划项目(BJJWZYJH01201910003011)、国家研究中心项目(BNR2019RC01011)、鹏城实验室大湾区未来网络试验与应用环境项目(LZC0019)、华为技术有限公司委托项目(HF2019015003)资助. **徐 恪(通信作者)**，博士，教授，博士生导师，主要研究领域为新一代互联网、区块链系统、物联网和网络安全.E-mail: xuke@mail.tsinghua.edu.cn. **付松涛**，博士研究生，主要研究领域为网络体系结构、网络安全. **李 琦**，博士，副教授，主要研究方向为网络安全、隐私保护、大数据安全. **刘冰洋**，博士，主要研究方向为网络架构、网络安全及可信、路由和命名解析、确定性网络等. **江伟玉**，博士，主要研究方向为网络安全、可信身份管理、隐私与IoT安全. **吴 波**，博士，主要研究方向为网络体系结构、网络安全. **冯学伟**，博士研究生，主要研究方向为网络体系结构、网络安全.

and network, is not enough to meet the security requirements of the network. To improve network security performance, there have been many different ideas for constructing the future Internet architecture, which mainly including the following designs: (1) The way repaired the problems of the network for incremental deployment to the existing Internet architecture; (2)The clean-slate design which abandons the existing Internet architecture, redesigns the network in a revolutionary way; (3) The evolutionary way which aims to resolve the existing or emerging problems of the Internet, while keep the backward compatibility as well as the incremental deployment, and eventually towards a new Internet architecture. We believe that only through the repaired way can't solve the inherent problems of the existing Internet architecture, while the clean-slate design, which is difficult to achieve incremental deployment, at least so far, have not shown instances of new applications or services that can be directly or indirectly deployed in the current Internet. The evolutionary way, which change the Internet as an evolving ecosystem, could not only achieve a stable transition but also bring innovations to meet the evolving requirements. We maintain that the evolutionary way can be adopted by the current Internet architecture and bring positive impact on the ecosystem which many millions of people live, work, and communicate. To achieve the evolutionary way, we need to study and understand the current state of the Internet, predict where it is heading and the problems it might soon face, and eventually find the root cause of the existing Internet security problems. We insist that the root cause of the existing Internet security problems lies in the Internet architecture, and the security performance should be fundamentally improved by designing network architecture with intrinsic security attributes and capabilities. The intrinsic security architecture of the Internet embeds security functions as a basic element to the Internet, forming a “security gene”, which ensures that the basic communication units of the network and the users who access the network are trustworthy without the help of external forces (security software, firewalls, etc.). In general, the intrinsic security architecture should have the following two characteristics: (1) Autonomous immunity. The security function is embedded with the network protocol to form a “security gene”. It does not rely on external equipment to solve security problems and can dynamically improve security capabilities with changes in the network environment. (2) Reliable as well as controllable. The trustworthiness among the terminals, infrastructure and application services, achieve the control of network basic communication units, users, and the network application services. This paper deeply studies various kinds of designs against the Internet security problems in recent years, analyzes the intrinsic security characteristics of these designs, and proposes our design idea of building intrinsic Internet security architecture.

Keywords Internet; Intrinsic Security; Internet Architecture

1 引 言

传统互联网体系结构面向性能的设计导致其面临严重安全威胁，如互联网缺乏真实地址鉴别能力，无法验证数据来源，带来源地址欺骗（Source Spoofing）、拒绝服务（Denial-of-Service）、路由劫持（Route Hijacking）等攻击[1][2]，给互联网及相关经济、社会和军事系统带来极大破坏. 到目前为止，各类安全解决方案不能从根本上解决网络面对的各种威胁[3].

Zave 和 Rexford 认为互联网缺乏信任基础，网络组件和服务被攻击，甚至网络本身对用户非法监视或审查，这些安全问题应该在网络中解决[4]. 针对传统互联网完全不可信的假设，Google 设计了基于信任等级访问控制的零信任模型 BeyondCorp[5][6]，实现以身份为中心的动态访问控制，通过对用户行为和设备状态的分析管控构建新的安全互联网环境.

陈钟等人认为网络安全目标是使终端、网元、协议和应用具备先天防疫能力，摆脱网络安全被动跟随网络架构的束缚[7]. 于涵等人基于免疫网络理论，引入免疫系统监控和管理信息传输系统行为，建立动态的网络模型防止网络入侵[8]. 中国工程院

于全院士从生物免疫系统角度，通过借鉴生物免疫系统带来的启示，提出依靠群体协作与对抗学习的网络安全防御类免疫动态安全架构[9]. 中国工程院邬江兴院士认为，带来安全问题的漏洞或后门是未知的，通过生物拟态现象造成攻击者认知困境，形成内生的主动防御，从“构造决定安全”公理中寻求破解安全问题之路[10].

构建未来互联网体系结构，一直以来存在多种不同的思路，主要包括以下三种思路：（1）针对现有互联网体系结构不足进行增量式修补的改良式路线；（2）放弃现有互联网体系结构，重新设计的革命式路线；（3）寻求折中的演进式路线. 仅通过改良式路线不能解决现有互联网体系结构固有弊端，而革命式路线脱离当前互联网得以滋生、创新和发展的既有体系结构，难以实现增量式部署. 通过演进式路线，既能实现稳定过渡又能满足不断发展的应用需求[11]. 我们认为，演进式路线在继承互联网体系结构基本设计原则和保证增量部署前提下进行革新，通过内生安全的互联网体系结构，既保证体系结构稳定过渡，又具备解决网络安全问题的能力. 互联网内生安全体系结构将安全功能作为基本要素耦合到体系结构，形成“安全基因”，在不借助外力（安全软件、防火墙等）情况下，确保网络各通信基础单元及接入网络用户真实可信. 总体说来，内生安全应当具有以下两个特征：

（1）自主免疫. 安全功能与网络协议紧密耦合，形成“安全基因”，不借助外部设备解决安全问题，能够随网络环境变化动态提升安全能力.

（2）可信可控. 真实可信范围涵盖终端、基础设施到应用服务，实现网络各通信基础单元、接入网络用户及网络应用服务整体可信可控.

本文包括 5 个部分，第 2 部分分析了构建互联网内生安全体系结构面临的问题和挑战，第 3 部分对当前互联网具有一定内生安全能力的解决方案进行分析和比较，并对方案可部署性进行分析，第 4 部分提出了一个互联网内生安全体系结构框架，最后对本文进行了总结.

2　问题与挑战

互联网诞生之初，用户数量相对较少，且用户主要来自教育科研结构，用户与网络存在信任基础. 随着互联网不断发展，用户数量达到十亿规模并持续增长，数据中心、云计算、边缘计算等技术广泛应用于互联网[12][13][14]，用户与网络的交互更复杂，网络面临更严重的安全问题. 随着物联网的发展，互联网应用场景逐步走向人与万物互联[15]，伴随物联网发展的是巨大的安全隐患. 彻底解决网络安全问题，需要探究网络问题产生的根源，网络安全问题产生的根源在于互联网现有体系结构面向性能的设计导致网络空间与用户空间缺乏信任机制，这种信任机制缺乏主要表现在：

（1）地址标识不可信. 地址标识是互联网体系结构的基本载体，但没有成为真实可信的端设备标识. 互联网现有开放、易伪造的 IP 地址，严重破坏了通信真实性，由于没有源地址认证机制，导致 IP 地址可以被假冒、仿造、劫持，且难以溯源.

（2）路由体系不可信. 路由体系是互联网数据传输的核心，当前存在数据传输实际路径与宣告路径不一致，BGP 缺乏对宣告消息合法性的验证能力，导致路由被劫持和假冒，发送者无法得到数据包沿预定路径传输的保证. 此外，网络中时常发生大规模分布式拒绝服务（Distributed Denial of Service，DDoS）攻击等问题[16].

（3）应用服务和基础设施不可信. 为用户提供应用服务是互联网的目标，缺乏可信的用户身份认证机制造成数据访问隐私泄露，网络应用发布和运行监管缺失，大量针对应用漏洞的攻击带来严重安全问题. 现有中心化的公钥基础设施（Public Key Infrastructure，PKI）作为互联网的信任支撑，存在仿冒伪造及单点故障，易遭受攻击引起虚假身份等问题[17].

此外，互联网处于动态、开放的网络环境，安全问题解决方案还需要考虑部署成本问题. 因此，通过体系结构设计从根本上解决网络安全问题，需要将安全问题作为一个整体考虑，综合考虑方案的可部署性，将真实可信作为基本属性嵌入体系结构，建立网络和用户的信任机制. 我们认为，设计互联网内生安全体系结构面临如下挑战：

（1）建立多类型端设备接入条件下的终端设备地址标识管理机制. 如何综合权衡互通、成本、安全和兼容性，确保网络具备验证终端设备地址真实性的能力.

（2）大规模网络路径真实性和路由节点行为的有效管控. 如何基于分组的差异化需求，保证分组传输过程实际路径与宣告路径一致，在分布式场景下有效管控路由节点行为，确保网络传输与路由控制“可信、可靠、可验证”.

（3）跨域应用场景下数据访问和应用服务管

控与监测. 如何在复杂应用场景下实现全局身份认证，改变全球网络基础设施不可信现状，确保用户身份和网络行为，以及应用服务“可信、可审计、可追溯”.

3 现有解决方案分析

本节从端设备地址、传输路径、网络服务安全，以及新型体系结构设计等方面分析现有网络安全问题解决方案及其可部署性. 我们整理了当前具有一定代表性的网络安全问题解决方案，如表 1 所示，这些方案包括对现有互联网的改良或革命性设计，具备一定内生安全特性，对构建互联网内生安全体系结构具有借鉴和参考意义.

3.1 端设备地址安全

大量研究从源地址安全的角度改进互联网开放接入带来的各类安全问题，从提升 IP 地址真实可信能力和保护隐私等方面提升安全性. 此外，一些研究基于无线通信设备物理层特征提升设备接入的安全性，这些特征可以与端设备地址绑定，从而提供适应于更多应用场景的安全能力.

表 1 现有安全问题解决方案

类型	现有问题	解决方案	目标
端设备地址	缺乏端设备地址验证机制	SAVA[18]/SAVI[19]/ SPM [20]/ Passport[21]/ APPA [22]/ Hidasav[23]/DISCS[24]/RISP[25]/ IPsec[26]/ HIP[27]/APIP[28]/AIP[29]/ APNA[30]	实现源地址真实性鉴别，提供地址审计能力和用户隐私保护
		RFID 鉴别[31]/ ZigBee 鉴别[32]/802.11 网卡鉴别[33]	基于设备物理特征实现认证
传输路径	路由体系信任缺失	Pi[34]/ stackPi [35]/ ICING[36]/SNAPP[37]/ OPT[38]/OSP[39]/ PPV[40]/ ShortMAC[41]/ Faultprints[42]/RFL[43]/ TrueNet[44]/VeriDP[45]/ NetSight[46]/ DynaFL[47]/ DFL[48]//DYNAPFV[49]/ MINOS[50] SNP[51]/ SPP[52]/ Zeno[53]/ Confluo[54]	分组转发层面实现路径行为一致性验证、错误定位与网络诊断
		OA[55]/ Argus[56]/ DISCO[57]/SPV[58]/S-BGP[59]/ So-BGP[60]/ psBGP[61]/ IRV[62]/ BGPsec[63]/Path-End Validation[64]/ eOTC[65]/RLP[66]/ Listen and Whisper[67]/Consensus Routing[68]/NetReview[69]/ TBGP[70]/ Pathlet[71]/ SCION[72]/ Internet Blockchain[73]	解决 BGP 前缀劫持、路径劫持、路由泄露等问题
网络服务	数据访问、应用服务和基础设施不可信	Riverbed[74]/ Ghostor[75]/IotSan[76]/ IOTGUARD[77]	数据访问安全
		Hydra[78]/ SmartCrowd[79]/SmartRetro[80]	应用发布和运行阶段安全
		ARPKI[81]/IKP[82]/ CertChain[83]/ BlockPKI[84]	提升 PKI 等基础设施安全能力
新型体系结构设计		XIA[85]/ MobilityFirst[86]/ NDN[87]/ SAINT[88]/ Compositional Architecture[89]/ PINet[90]	建立解决互联网现有问题的新型体系结构

3.1.1 源地址安全

源地址安全包括源地址验证和源地址保护，源地址验证确保源地址真实可信，源地址保护在确保可审计性的前提下保护源地址不被伪造，且有效防止隐私泄露.

（1）源地址验证

源地址验证的目标是通过验证过滤含有非法源地址的数据包. 如图 1 所示，RFC 5210[18]中提出源地址验证体系结构（Source Address Validation Architecture，SAVA），将源地址验证划分为三层，在接入网、自治域（Autonomous System，AS）内、自治域间实现源地址验证及过滤三层框架. 在 CNGI- CERNET2（中国下一代互联网示范工程 CNGI 核心网之一）中对 SAVA 进行了部署实现[91].

① 接入网验证

RFC7039[19]提出了接入网源地址验证增强技术（Source Address Validation Improvement，SAVI），能够在第一跳交换机实现主机粒度源地址验证. SAVI 中所有主机统一管理，采用方案符合本地接入子网地址分配和管理策略，通过交换机端口和真实源 IP 地址，或 MAC 地址、源 IP 地址和交换机端口动态绑定验证交换机端口的数据包合法性.

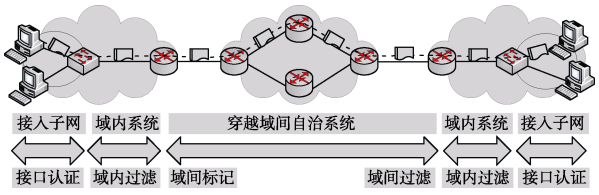


图 1 SAVA 架构图

② 域内验证

域内验证用于过滤域内用户发起的伪造报文，与接入网验证共同构建完整的域内防御体系. 与接入网验证一样，网络设备处于同一管理权限下，通过构建过滤表，将路由器每个传入接口与一组有效的地址前缀关联. 但域内验证只能约束域内用户行

为，无法对外域攻击建立防御基础. 实际部署后，域内源地址验证仅能约束域内用户不向外发送伪造报文使互联网受益，对“外部”数据包源地址验证能力不强，难以实现“谁部署谁受益”，导致缺乏部署激励[92].

③ 域间验证

相对域内验证而言，域间验证实现较为复杂. 自治域之间达成共识是实现域间验证的有效方式.

SPM（Spoofing Prevention Method）[20]建立自治域安全联盟，联盟内发送端与目的端事先协商好标签并添加于发送报文中，目的端验证源地址真实性. SPM 能够在接收端部署使部署者受益，以激励网络维护者部署，但 SPM 不能保护外部用户免受反射攻击，且密钥更新较慢降低了系统安全性. Passport[21]通过 AS 间分享对称密钥，源端边界路由器为出向流量增加消息认证码，经过每个自治域时依次对当前 AS 对应的消息认证码进行验证，直到到达目的端，Passport 的不足是传输路径改变时无法实现验证，对拓扑的依赖影响了可部署性.

APPA（Automatic Peer-to-Peer Anti-spoofing）[22]实现了自治域内和自治域间两级过滤，自治域内（intra-AS）签名在网关验证；自治域间（inter-AS）源边界路由器标记签名，目的边界路由器实现验证，通过自动状态机改变签名，基于状态机实现 AS 粒度前缀验证. 但扁平化的域间验证体系导致边界路由器维护状态机数量过大，增加了路由器开销和状态机同步难度. Hidasav（Hierarchical Inter-Domain Authenticated Source Address Validation）[23]提出一种分层级建立联盟的域间源地址验证体系，AS 联盟分为多个层级，每一层级联盟可作为成员参加更高层级联盟. 同一联盟内最低层级之间源地址验证通过联盟内状态机实现；跨联盟源地址验证时，源 AS 所在联盟各层级边界路由器作为跨联盟数据报文交互的“中继代理”自下而上替换标签，目的 AS 所在联盟各层级边界路由器自上而下替换标签，直到到达目的 AS. Hidasav 能够降低通信、存储及计算开销，建立自治域间的信任关系，并能在互联网增量部署，实现“先部署先受益”.

为提升域间源地址验证的灵活性，DISCS（DIStributed Collaboration System）[24]将互联网划分为多个防御联盟，联盟内提供与 SPM 类似的防御，仅在受到攻击时根据攻击类型按需调用联盟成员提供的防御函数. DISCS 提升了效率，其不足是可靠性依赖于 BGP 的安全性，这种依赖影响了方案的自主安全性. 同样依赖可信第三方的还有基于 RPKI（Resource Public Key Infrastructure）[93]提供源地址域间通信保护机制的 RISP[25]，通过 RISP 联盟中心、RISP 服务器和自治系统边界路由器共同完成出向和入向流量过滤. 该方法的不足是过于依赖 RPKI，RPKI 实际部署速度很慢，在 BGP 宣告的 IP 前缀中只有少量受到 RPKI 保护，限制了其性能.

此外，还有方案基于分组路由信息实现过滤，在路由器转发端口建立合法源地址绑定表，分组传输过程中过滤绑定表以外的源地址报文[94]. 但建立绑定表需要获取自治域合法地址前缀及源端路由选择信息，实际部署性较差.

总体说来，现有源地址真实性验证方案将验证功能与网络功能耦合，提供了一定的内生安全能力，但域内验证方案缺乏部署激励，域间验证方案存在带宽、计算资源开销过大等不足，影响数据传输性能，部分方案对第三方设施存在依赖. 建立互联网高效、可靠的地址验证体系，还需进一步探索.

（2）源地址保护

源地址保护在保证源地址可审计性基础上，保护源地址不被别的主机用于伪造身份，以及保护源地址隐私.

① 源地址伪造保护

IPsec[26]能够借助加密技术同时保护源地址和目的地址，但存在开销大、可扩展性低等不足. 为保护网络主机移动后 IP 地址不被其他主机用来伪造身份发送数据包，HIP（Host Identity Protocol）[27]在 L3.5 层设计主机标识，IP 地址只用于路由. 主机标识符 HI（Host Identity）标识用户身份，主机移动造成 IP 地址发生变化时对通信不存在影响，对端节点可以通过 HI 识别用户身份. HI 使用公钥哈希得到 128 位 HIT（Host Identity Tag）作为主机标识. HIP 通过增加标识，在不依赖对 IP 地址审计的前提下解决移动性问题，安全功能与正常功能紧密耦合，提供内生安全支持，但需要 IPsec 增强数据安全性，开销较大，且交换过程容易引入 DoS 攻击，同时只能用于身份识别，不能防御地址前缀欺骗.

② 源地址隐私保护

Naylor 等人认为增强 IP 地址可审计性的同时需要提供隐私保护，提出兼顾可审计性与隐私保护的 APIP（Accountable and Private Internet Protocol）[28]. APIP 将源 IP 分成两部分，对审计地址（Accountability Address）和回传地址（Return Address）分别管理. 作者在 AIP（Accountable Internet Protocol）协议[29]源地址审计机制基础上设计了保护用户隐私前提下可审计策略. 借鉴 AIP 中委托审计（Delegated Account

ability），将地址分为两部分，每个数据包携带多个地址，用于传输数据的目的地址（Destination Address），和用于识别的审计地址.

APIP 传输过程如图 2 所示，其传输过程包括：A：发送端携带审计地址发送；B：发送端向审计委托方发送数据包摘要；C：路由器或接收端向审计委托方确认数据包是否来自其委托的客户端；D：如果接收端确定数据包属于恶意流，则使用审计地址向委托审计方报告；E：接收方使用回传地址向发送方发出响应. APIP 能够确保只有委托审计方知道发送方发送了数据包，从而改进隐私保护问题，同时在处理恶意流的方式上有了更长效和明确的方案. 但安全功能并没有与正常协议功能紧密耦合，源端可以不报告或否认数据包.

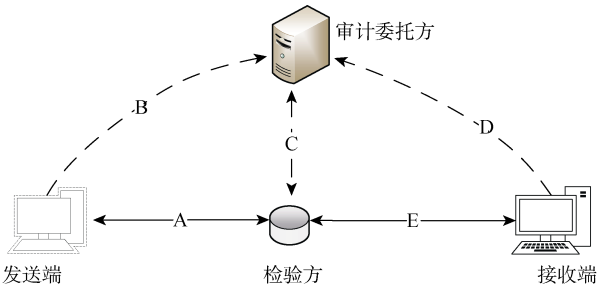


图 2 APIP 传输示意图

APNA（Accountable and Private Network Architecture）[30]在可审计性和隐私保护方面对 APIP 做了提升，AS 通过向所属范围内的主机分配临时 ID（Ephemeral Identifiers，EphIDs）用于通信，保护主机 IP 地址隐私，ISP 仅对认证后的主机发放 EphIDs，EphIDs 与主机公私钥对关联，通信时源端和目的端通过与 EphIDs 关联的证书和公私钥协商通信对称密钥，所有数据加密通信. 目的端可以向审计代理（Accountability Agent，AA）发送中断通信请求，AA 审计通过后终止源端流量. APNA 通过安全功能和协议功能的耦合提供了一定的内生安全性，但没有提供证书安全发放的手段，影响了整体安全性.

基于 IP 地址的命名与解析策略作为网络传输的核心承载机制，其设计对互联网影响至关重要，朱亮等人在文献[95]中提出了一种通用的地址框架，在文献[96]中提出了一种形式化的互联网地址机制通用框架，并进一步在文献[97]中创新命名机制，提出基于 xml 的通用命名服务，支持在体系结构中动态引入命名空间、协议实体以及对应解析机制，对应用透明的同时保证原有体系结构的兼容性及可理解性，可以作为构建具有内生安全能力互联网体系结构的参考和借鉴.

3.1.2 物理层鉴别

随着物联网的发展应用，大量设备/传感器通过网络互联，由于无线信道开放性引入的窃听、篡改或攻击，物理层鉴别（Physical-Layer Identification，PLI）作为传统基于密码的无线通信的补充，在阻止非授权用户截获、窃听数据方面具有一定优势. 大量关于物理层鉴别的研究表明，硬件设备在调制方式、瞬态转变等方面存在一定区别，由此可形成端节点“指纹”特征，具有自认证特点.

Danev 等人[31]提出射频识别设备（Radio Frequency Identification Devices，RFID）鉴别方式，基于 RFID 应答机响应信号的调制形状和频谱特征差别识别不同 RFID，为防止克隆设备伪造相同 RFID 指纹，通过在授权方使用数字签名将 RFID 指纹绑定到文档 ID，验证签名有效后，授权方将存储指纹与测量指纹进行比较，确保不受伪造设备影响. 此外，Danev 等人还通过 ZigBee 设备在数据包开始传送到实际数据传送短暂的瞬态特征不同对节点进行鉴别[32]. 但瞬态特征提取对设备要求极高，此外，攻击者可以通过爬山（Hill-climbing）算法试出被攻击者特征从而假冒被攻击者，也很容易制造噪声造成阻塞，影响了其实用性.

Polak 等人对 802.11 网卡的信号发射特征进行分析，认为这些信号差异即便可通过精确的制造工艺和质量控制来解决，但花费成本过高，可以通过无线网卡特征进行鉴别[33]. Henrik 等人分析了机器通信（Machine-type Communication，MTC） 网络中接入点与物联网节点的物理层认证（Physical Layer Authentication，PLA）协议，以及附近存在攻击者实施数据注入、解除关联、女巫攻击对 PLA 的影响，证明了 PLA 协议在 MTC 关键任务应用中面对三种攻击的可用性[98].

总体说来，如表 2 所示，在源地址真实可信方面，以 SAVA 为代表的源地址认证技术具备一定内生安全性，但域间验证存在开销大及对第三方设施依赖等不足. 源地址保护方面，现有解决方案还不具备同时保护用户隐私和实现可审计性的内生安全能力. 现有物联网设备安全解决方案基于设备自身特性，具有一定自主内生安全性. 但随着软件无线电技术的发展，伪造这些特性并不困难，解决方案能否随攻击能力提升安全能力尚不明确；同时方案只适合小规模用户场景，如网关对本域内节点验证. 这些方案可作为锚在接入网内与 IP 地址绑定，为构

建适用于异构网络节点接入的内生安全体系结构提供基础和参考.

表 2　端设备地址安全方案小结

类型	策略	优点	不足
源地址真实性	SAVA[18]/SAV[19]/ SPM[20]/ Passport[21]/ APPA[22]/ Hidasav[23]/ DISCS[24]/RISP[25]	提供域内自律验证、域间安全审计	域内缺乏部署激励, 域间开销大或依赖第三方设施
源地址保护	IPsec[26]/HIP[27]/ APIP[28]/ AIP[29]/APNA[30]	提供审计能力和用户隐私保护	开销大, 源端可避开审计或对第三方存在依赖
物理层鉴别	RFID 鉴别[31]/ ZigBee 鉴别[32]/ 802.11 网卡鉴别[33]	基于设备自身特性验证	适合小规模场景, 是否具备自我提升安全能力还需进一步验证

3.2　传输路径安全

确保数据传输链路从源地址到目的地址全链路生命周期安全是网络安全的重要组成部分. 我们从传输路径数据面和控制面分别分析相关解决方案.

3.2.1　传输路径数据面安全

传输路径数据面解决方案力求用最小的开销提供路径验证能力, 并通过错误定位方案检测传输链路上的错误位置, 甚至准确分析故障原因, 从而制定网络策略. 传输路径验证(Path Verification Mechanism, PVM) 主要关注路径一致和遵从性 (Path Consent and Path Compliance), 确保接收端和路径上的节点能够验证传输路径是否符合要求, 现有基于标识验证、可信硬件、集中式验证和设定路由规范等解决方案, 将安全功能与常规功能耦合, 具备一定的内生安全能力. 此外, 网络诊断系统能够针对网络故障提供诊断功能, 对构建互联网内生安全体系结构具有借鉴和参考意义.

(1) 基于标识验证

基于标识验证方面, 通过在 IP 分组头部添加标识判断恶意流量以保护接收端的方案有: Savage 等人[99]提出的基于随机标识辅助接收端判断恶意流量的机制; 确保接收端能够通过数据包转发路径确定错误位置的 Pi (Path Identifier) 机制 [34] ; 以及基于栈的概念, 中间节点将标识信息依次写入栈中, 接收端根据栈中信息判断转发路径是否安全的 stackPi 机制[35]. 这些方式可以通过标识追溯路由节点行为, 有效保护目的节点免遭 DDoS 攻击, 但由于没有从根本上解决中间节点受到恶意攻击时有效防范问题, 同时 IP 头部可以利用的标识符长度有限 (通常不超过 16 位), 假冒者可以学习标识添加方法, 难以实现精确定位.

SNAPP (Stateless Network-Authenticated Path Pinning) [37]的目标是通过路径一致在分组交换路由上实现电路交换性能, 发送端和路由器依次添加消息完整性验证码 (Message-Integrity Code, MIC), 下一跳路由器及目的端依次验证, 具备较高的验证效率, 但由于缺乏对数据包转发过程的防护, 导致其应对攻击能力较弱.

ICING 机制[36]在每个中间节点部署验证服务器, 对接收数据包进行安全验证, 提供了较高的安全保障. 但是其不足也十分明显, 首先其复杂的验证过程带来网络传输时延明显增加, 其次中间节点验证属于有状态操作, 大大增加了存储开销, 同时需要部署用于验证的专用服务器, 削弱了实际部署可能性. OPT (Origin and Path Trace) 方案[38]设计了一种轻量级的源地址和路径验证策略, 发送端在数据包头设置数据包转发路径上所有节点的标识, 中间节点 (路由器) 及接收端依次在路径上接收相应标识. OPT 的中间节点只执行两次消息认证码 (Message Authentication Code, MAC) 操作, 提升了效率, 但是需要所有节点都部署验证能力, 同时仍然无法解决中间节点受到攻击产生恶意丢包的行为. 此外, 由于 OPT、ICING 等认证码对加密方案的依赖, 在数据包较多时带来较大的加密和验证开销.

通过源端和路由器使用正交序列作为证书, OSP (Orthogonal Sequence based Protocol) [39] 传输数据时, 源端向提供商请求证书, 提供商向相应的路由器下发证书, 由于源端证书中包含与路由器证书正交的序列, 路由器节点能够验证包的源地址和路径. OSP 提高了路由器存储和验证效率, 其不足是每个节点都需要提供商下发验证信息, 增加了管理开销.

为进一步提高效率与可靠性, Wu 等人提出了中间路由节点以一定概率对数据包进行标识的 PPV 机制[40], 可以减少分组头部额外的通信开销和安全验证的延时开销, 从而提高源地址和路径验证的效率. 在 13 跳的情况下, PPV 将 OPT 所需的近 300 Bytes 通信开销降至 64 Bytes, 并在目的端提供错误定位功能, 同时基于随机标识方式更易在互联网增量部署.

通过在数据包头部新增标识字段, 使发送端能够根据回传信息实现错误定位的策略有 ShortMAC 机制[41]、Faultprints 机制[42]等. ShortMAC 在发送端增加标识字段, 传输路径上各节点识别标识字段并验证, 节点记录正确和错误的数据包数量, 并将记录回传到发送端. 发送端接收数据包传输记录后,

确定传输过程中异常发生的位置. ShortMAC 需要为每个源端存储对称密钥，对路由器存储资源消耗过大，无法用于域间通信. Faultprints 机制实现了域间路由转发错误定位. 其基本原理如下：发端发送数据时，按照一定规则设置数据包头，数据传输路径上各节点对数据包进行验证和采样，发送端接收来自传输路径的采样并定位异常节点. 由于设计了硬件加速方法，Faultprints 具有较高的验证效率. 它们共同的不足是如果路径上有节点受到干扰，传来错误采样信息，发送端无法判断真伪，降低了可靠性.

Wu 等人[100]提出了一种鲁棒性的轻量级错误节点定位机制，在此基础上，进一步在文献[43]中提出高鲁棒性错误定位机制（Robust Fault Localization，RFL）. 该机制中，每个路由节点随机采样数据包信息，源端接收这些回传信息. 通过高鲁棒性的密钥分发，轻量级的源地址和路径验证，实现高效可靠的错误定位. 如图 3 所示，ReqKey 和 AckKey 表示对称密钥分发的请求和反馈，ReqProb 和 AckProb 表示采样信息回传的请求与反馈. 经过对称密钥分发、源地址与路径验证到实现错误定位，由于采用了随机采样方式，降低了开销. 但 RFL 机制仍然不能保障回传信息不被篡改，基于传输路径不能假设为可靠信道这一前提，仍然没有策略能够解决恶意行为对中间节点的攻击，提供自主的内生安全性.

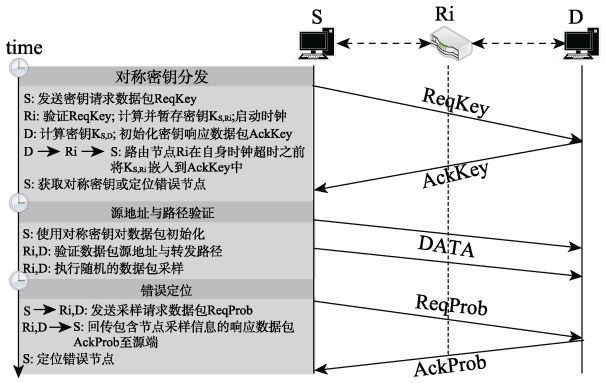


图 3 RFL 机制工作流程

（2）基于可信硬件

基于可信硬件方面，TrueNet 机制[44]引入了可信计算模块（Trusted Computing Base，TCB）收集网络状态，可信计算模块安装于发送端、传输路径节点、接收端，不同实体间的可信计算模块通过安全信息交互确定恶意链路位置. TrueNet 中可信计算模块的可信度直接影响了网络安全性，但可信模块本身并不是方案设计的一部分，方案的自主安全性受到可信模块的限制.

（3）集中式控制

集中式控制通过软件定义网络（Network Defined Software，SDN）技术，以集中方式对源地址真实性和路径一致性进行验证，能够提高验证效率和准确性. 如 VeriDP 机制[45]通过合理的控制层策略对数据传输进行验证，保证数据传输路径一致. NetSight[46]通过控制器收集传输路径上位于交换机的数据包相关信息，并通过这些信息恢复实际传输路径，从而判断网络行为，准确性更高. DynaFL（Dynamic Fault Localization）机制[47] 和 DFL（DFL: Secure and Practical Fault Localization for Datacenter Networks）机制[48]集中收集传输路径上的节点验证信息，通过节点间相互采样提供适应动态变化网络的能力，适用于数据中心网络 （Data Center Network，DCN），但容易带来单点故障问题，且在互联网中部署存在困难.

DYNAPFV（Dynamic Packet Forwarding Verification）[49]在 SDN 内实现了一种高鲁棒性轻量级数据包传输验证方案，通过检测数据包和流统计信息以验证数据包真实性和传输行为. DYNAPFV 采用 N-PFV（Novel Packet Forwarding Verification）验证机制，所有交换机出入口生成 packet_in 数据包向控制器传送，控制器基于随机间隔从交换机得到流统计信息，验证路径上传输数据包数目. 通过出入口交换机传送数据包对比，N-PFV 能够捕获包丢弃攻击，通过对比从相应交换机得到的信息，能够识别统计信息出现的错误，并能在出口和入口交换机包不匹配情况下捕获对包的篡改和一些复杂攻击. DYNAPFV 的特点是仅在 SDN 控制器部署，不需要对交换机做任何改动，具有较好的可部署性.

（4）路由器规范验证

路由器规范验证方面，Xu 等人提出 MINOS[50]，与以往通过加密认证等确保路由操作真实性不同，MINOS 从数据层面规范路由器，确保路由操作真实性. MINOS 通过中央管理器（Centralized Manager）验证路由器数据层面操作，在运行环境下动态规范路由器行为. 通过设定 8bit 的路由器组件识别符（Component Identifier，CID）和由组件识别符序列组成的操作识别符（Action Identifier，AID），采用中央管理器的控制，识别数据包克隆、非法读取、丢弃等行为，从而规范路由行为. 作者基于 Click 路由器证实了 MINOS 的有效性和可靠性. MINOS 在数据层面实现了实时的路由规范，安全功能和路由功能紧密耦合，提供了内生安全性，但需要中央管理器管理正常行为，与集中式控制方式一样难以直

接应用于互联网.

（5）网络诊断系统

基于网络诊断系统分析网络行为实现网络故障诊断，能够提供更符合用户需求的安全性能. 文献[51]中建立了一种网络安全溯源机制（Secure Network Provenance，SNP），在发现恶意行为时找出产生该问题的根本原因. 基于记录数据相关性的数据起源图和记录节点行为证据的防伪日志，作者设计了 SNooPy 系统，将图的变化放在日志中，使用哈希保证其防篡改特性，利用对日志的微查询检验路由信息.

文献[52]中设计了一种新的网络诊断架构，作者认为现有网络故障检测，无论是借用 ICMP 等机制实现，还是增加协议字段、开发新协议等，都存在弊端，且与现有安全机制不兼容. 作者在 IP 层获取数据，通过网络记录包传输等事件及原因，为故障诊断提供帮助. 为了实现这种安全原语，作者定义了起源图模型，并基于该模型开发了安全数据包起源（Secure Packet Provenance，SPP）协议. 起源图中顶点代表事件，边代表事件之间的因果关系，每个节点记录与维护部分起源图，相邻节点交叉验证. SPP 协议在不改变现有协议条件下提供诊断功能，引入的额外通信流量也很小，同时考虑了不改变现有协议的增量部署方式，但目前并没有大规模实验验证.

Wu 等人认为常规方法通过分布式日志记录并分析故障位置，不能得到故障产生的本质原因，无法从根本上解决故障. 为了找到网络故障的真实原因，作者提出了 Zeno[53]，引入了临时起源（Temporal Provenance）概念，找到故障产生的本质，从而解决故障. Zeno 能够发现故障产生原因，甚至能分析一些离线原因，提升了网络故障诊断能力.

为提升高速网络（速度高于 10Gbps）的数据包分析能力，Confluo[54]着眼于高速网络中尽可能减少 CPU 使用前提下，对所有数据包进行监测，改善了现有情况下支持速率低、一致性差等问题. Confluo 设计了原子多重日志（Atomic MultiLogs）数据结构，通过保持处理过的头部信息不变以及采用定长记录捕获数据包头的方法，提升了高并发条件下读写操作能力，可通过 Hypervisor 对部署在端主机上的多台 VM 进行监控管理，但整个系统端主机之间无法分享监控资源.

综上所述，当前路径验证方案通过安全功能与正常协议功能耦合，提供了一定的内生安全性能，其不足是无法保证不可信传输路径上遇到攻击时的防范能力. 故障诊断系统提供了一定的故障诊断能力，但仍然无法提供较高的离线故障分析能力，且安全功能没有与正常功能耦合，不具备内生安全特性，但可以作为解决路径传输安全问题的参考和借鉴.

3.2.2　传输路径控制面安全

传输路径控制面安全主要解决 BGP 前缀劫持、路径劫持和路由泄露方面存在的安全问题. 其安全解决方案采用的策略与路径验证存在相似之处，如可通过添加标签或签名实现验证，但其解决的问题有所不同，BGP 安全更关注路由计算. 现有解决方案包括部分或全部解决 BGP 前缀劫持、路径劫持和路由泄露问题方案，以及新型方案设计.

（1）部分解决方案

解决前缀劫持的方案有 OA（Origin Authentication）[55]，新增 OAT（Origin Authentication Tags）标识，OAT 在路径上传递，直至到达目的端，该机制无法保证 OAT 字段在传递过程中不受篡改. Argus[56]通过检测系统检测控制面和数据面相关系数实现快速检测前缀劫持异常，并在互联网实际部署验证其低时延，高可靠的前缀劫持检测能力. RPKI 基于数字签名和证书实现路由起源认证，有效防范前缀劫持，但由于缺乏部署激励导致其在互联网部署进度缓慢. DISCO[57]是基于 RPKI 基础设施部署进展慢这一实际情况设计的基于分布式信任的路由起源认证系统，系统通过分布于各 AS 的代理（Agent）发布前缀和公钥绑定信息，分布式登记服务器（Registrar）收集 BGP 宣告信息，在一定时间间隔（Certification Interval）收到的绑定信息超过阈值时，则认为该 AS 与公钥之间绑定关系真实可信，登记服务器签名认证后向公共数据库（Repository）发布. 公共数据库收集到一定数量登记服务器对相同绑定关系的认证后，发布真实可信的前缀及公钥绑定关系，可供全局查询. DISCO 通过分布式检测机制降低了源认证的部署难度，但检测方案如何嵌入体系结构内部，以及如何与路径劫持、路由泄露等安全问题结合，形成内生的安全机制，还需进一步探索.

解决路径劫持的方案有 SPV（Security Path Vector）[58]，SPV 在提高效率、减少密钥管理复杂度方面性能较好，其不足是无法抵御前缀劫持. 同样只关注路径劫持的还有 Signature Amortization[101]和 Reference Locality[102]，由于只针对路径劫持，算法应用场景有限.

同时针对前缀和路径劫持的方案中，S-BGP（Secure BGP）[59]首次基于 BGP 安全问题建立了体

系化解决策略，利用洋葱路由特性，签名采用洋葱格式，加强地址前缀及传输路径保护. S-BGP 的不足是提升了对路由器能力的需求，通过集中方式实现认证，采用非对称加密验证签名，计算开销和时延较大，存在扩展性问题. 为解决 S-BGP 的扩展性问题，So-BGP[60]设计了一种分布式认证解决方案，提高实际环境中部署能力. 但 So-BGP 的路径验证功能不足，尤其对 BGP 中 AS_PATH 不能提供保护，限制了实用性. 另一种借助邻居 AS 协同证明的方案，psBGP（Pretty Secure BGP）[61]提升了路径验证能力，但仍然无法抵抗合谋攻击，且由于 AS 可能从不同的 ISP 获取 IP 地址，使得方案难以在实际中部署.

IRV（Interdomain Route Validation）机制[62]在每个 AS 部署一个 IRV 服务器，服务器在域间交互信息验证各 AS 宣告信息，提升地址前缀和路径劫持防护能力. IRV 能够提升验证效率和可靠性，但需要部署新设备，增加了维护管理难度.

在 RPKI 基础上，通过相邻 AS 授权的 BGPsec[63]在每个 AS 收到宣告路由后，验证每个 BGPsec 签名，确保宣告路径的可靠性，但开销较大，且在部分部署时难以提升整体安全性能. 基于 RPKI 设计的路径-终端验证（Path-End Validation） 协议[64]提供了一种部分部署下实现安全性能整体提升的方案，AS 使用 RPKI 授权私钥签名“路径-终端”记录，包括支持的邻接 AS 列表等. 这些记录来自不同的 AS，可基于记录提供离线过滤，同时保护其后面没有部署的 AS 免受恶意路由传播影响，在部分部署情况下提供较强的防护能力. 当然，BGPsec 全面部署后的安全性仍然需要进一步验证，文献[103]分析了即便 BGPsec 完全部署后仍然存在漏洞，如合谋 AS 可以构造虫洞攻击，假路由更新也能得到有效签名.

针对路由泄露问题，RFC 7908[104]中对路由泄露产生原因及分类进行了分析，阐明 BGP 协议路由器配置错误是产生泄露的主因. 基于此，一些方案通过降低路由器错误配置提高安全性. 其中，相邻 AS 间的关系通过 eOTC（external Only To Customer）[65]属性记录并传递，eOTC 属性设置的规则包括：对没有设置 eOTC 属性的发送方，如果其角色是提供商（Provider）或对等方（Peer），则必须添加发送方编号为 eOTC 属性；对设置了 eOTC 属性的接收方，如果其角色是提供商或对等方，若 eOTC 值不是相邻 AS 的编号，则存在路由泄漏，给予较低的本地优先级或被丢弃. 通过 eOTC 属性传递能够提供域内和域间防护，如图 4 所示. 另一种实现策略 RLP （Route Leak Protection）[66]在 BGP 中增加了 DO（Down Only）、L（Leak detected）两种属性判断是否发生泄露，与 eOTC 相较，RLP 可达能力更强. eOTC 和 RLP 的不足之处在于可能泄露自治域间的商业关系，有的关系显然属于隐私范畴.

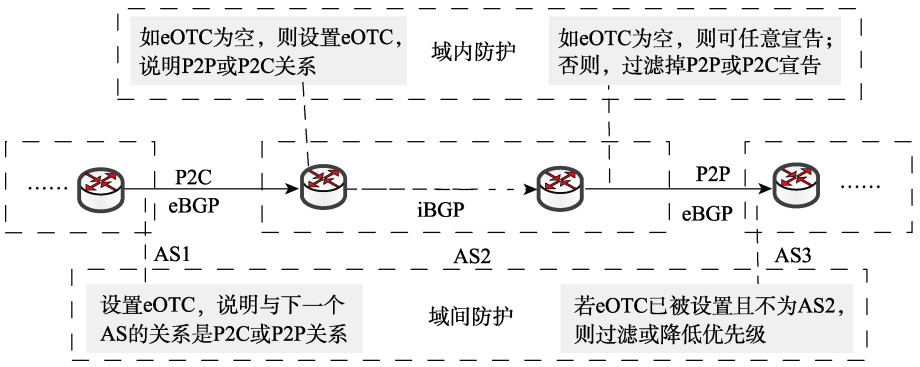


图 4 eOTC 路由泄露防护机制原理图

以上 BGP 安全方案将安全功能与正常协议功能整合，具备一定的内生安全能力，部分方案需 RPKI 支持，需要整合 RPKI 才能实现自主的内生安全能力，其不足是方案在实际部署中抗攻击能力有限，同时部分方案牺牲了 AS 间的隐私关系.

（2）整体解决方案

基于整体解决 BGP 安全问题的方案中，文献[67]提出了 Listen and Whisper 协议. 通过 Listen 在数据面探测并检查到不同目的网络的潜在路径，Whisper 在控制面检查伪造的路由宣告，二者结合消除路由器配置错误，降低恶意攻击的危害. 作者认为 PKI 基础设施花费巨大且不可信，因此采用了不需要 PKI 支持的策略. Listen 在数据面完成路由可达性验证，Whisper 对传播无效路由的路由器发出警告，并检查宣告多条无效路由的恶意路由器，降低无效路由带来的危害. Whisper 包括弱分岔（Weak

Split）和强分岔（Strong Split）两个等级验证路由一致性，其中弱分岔采用哈希链方式验证，强分岔采用非对称加密机制验证，并通过改进策略大幅度降低合谋攻击的危害. 在可部署性上，Listen 可以在现有 BGP 上实现增量部署，Whisper 虽然能够在不改变数据包格式的前提下与现有 BGP 整合，检测所有交换路由宣告潜在的异常，但其检测能力较弱，影响了其实用性.

John 等人认为 BGP 协议注重响应度而忽视一致性，不仅牺牲了网络可用性，使路由环路、黑洞、丢包等现象大量出现，更造成了协议行为复杂与不可预测性. 针对这一问题提出了路由共识（Consensus Routing）[68]，实现路由一致性与网络高可用性. Consensus Routing 使用稳态与瞬态模式分别保证路由一致性与可用性. 稳态模式下，所有路由器参与到一个分布式合作算法中，计算稳态转发表（SFTs）. 算法要求一个路由更新只有在被所有路由器知晓后才应用到 SFTs 中，保证了 SFTs 的一致性. 稳态路由未达到共识时转向瞬态模式，瞬态模式主要整合 3 种已有方案：路由偏转、路由绕道与备用路由. 保证在链路故障、协议更改等情况下，所有 AS 依然可达，实现了比 R-BGP[105]更通用和有效的链路故障适应能力，提供了网络高可用性. 但该机制实验评估不全面，难以保证真实场景下实际效果.

Haeberlen 等人提出了 NetReview[69]，作者通过 BGP 错误检测系统检测路由问题，并定位造成该问题的 AS. NetReview 设计了防篡改日志和规范语言，边界路由器在防篡改日志中记录所有 BGP 消息，邻居间周期性地互相审计日志. 防篡改日志保证对条目的修改、删除或伪造等行为可被检测，日志组织为哈希链形式，记录所有发送与接收的路由消息，每个消息包含签名信息，接收者对每个消息发送确认. 采用规范语言描述每个 AS 的 BGP 期望行为，通过几个简单规则检测路由问题，包括源配置错误、引入路由扩展错误、路由重分发攻击、路径长度不一致等. 在实现上，NetReview 不需要 PKI 支持，支持增量部署，但作者并没有针对检测故障提出解决策略.

TBGP（Trusted BGP）[70]通过建立可传递的信任关系降低计算开销和网络资源. 可传递信任关系的核心依赖于前缀所有者使用私钥对路由进行的签名. 在路由器入口和出口过滤器上引入路由验证服务保证路由没有被错误配置或恶意修改. 路由器出口过滤器成功验证路由通告后签名，邻居路由器在入口过滤器验证该路由签名并更新自己的路由表，并将路由信息通告给它的邻居，通过可传递信任关系防止虚假路由扩散. 但是，TBGP 不解决配置冲突，同时基于可信计算模块提升安全性，可信计算模块的安全性是 TBGP 安全的基础.

以上方案通过增量式部署提升 BGP 安全性能，安全功能与正常功能耦合，具备一定的内生安全能力，但方案没有大规模部署，实际可部署性还需要进一步验证.

（3）新型解决方案

新型解决方案基于现有安全问题重新建立路由与转发认证策略，提供更高的安全性能.

Pathlet[71]可以实现粒度更细的路由与转发. Pathlet 包含不同的 AS，每个 AS 内由众多节点组成多条转发路径（Pathlet），AS 将这些 Pathlet 对外宣告，发送方在发送消息的时候，基于发送要求灵活选择 Pathlet. 这样，从发送端到接收端由多条 Pathlet 组成了一条转发路径，通过该路径可以实现端到端传输. 这种方式能提高转发效率，同时提高传输可靠性. 其不足是各 AS 对 Pathlet 的宣告，以及发送端对 Pathlet 的选择，不但引入额外通信开销，也带来控制层面复杂度提升.

SCION（Scalability，Control，and Isolation On Next-Generation Network）[72]在网络中建立隔离域（Isolation Domain，ISD），每个隔离域由多个 AS 构成. 每个隔离域设置一个核（ISD Core），用于管理本隔离域. 不同的隔离域之间通过核交换信息，同时通过可信根配置（Trust Root Configuration）实现全网安全管理. 数据传输时，SCION 各隔离域通过核交互传输路径. SCION 在交互过程中及时发现不可靠 AS，并避开这些 AS. 其不足是核之间的信息交互带来大量额外开销，影响转发效率. Pathlet 和 SCION 等新型设计提供了自主安全能力，具有较高的内生安全特性，但是对互联网改动较大，难以实现增量式部署.

由于区块链能够在分布式环境下建立信任机制，一些域间路由安全协议通过区块链实现对 IP 地址前缀及路径信息的认证. Internet Blockchain[73]首次利用区块链建立分布式信任框架，将 IP 前缀认证和路由通告认证交易通过区块链发布，形成防篡改的交易记录. 作者提出了互联网增量部署方案，逐步扩大资源和地域保护范围. 资源保护范围方面，按照 IP 前缀认证，BGP 交易认证等逐步扩大资源保护范围；地域范围方面，首先通过企业内部或数据中心内部区块链发布路由交易，如基于 BGP 的 SDN

控制器之间，逐步扩大应用范围至互联网. 后续工作如 BGPcoin[106]等在此基础上进行了 IP 前缀认证的验证测试工作. 尽管区块链可作为解决分布式信任问题的有效手段，但目前相关研究仍然处于初步测试和可行性验证阶段.

此外，一些独特的 BGP 解决方案通过巧妙设计为解决安全问题提供了新思路，如针对 DDoS 攻击，文献[107]中提出了一种 DDoS 缓解系统 Nyx，在拥塞点附近选择备用路由，不借助合作或网络重设计情况下缓解 DDoS 攻击，将 DDoS 攻击缓解转化为简单的路由问题，不依赖外部设备提供安全性能. 转化攻击的思想作为疏导攻击的有效策略，可以作为构建互联网内生安全体系结构的参考.

如表 3 所示，传输路径数据面，现有方案在路径验证、错误定位等方面难以抵御中间节点合谋攻击. 传输路径控制面安全方案存在安全能力不足和缺乏可部署性等问题.

表 3 传输路径安全方案小结

类型	策略	优点	不足
传输路径数据面安全	Pi[34]/ stackPi[35]/ ICING[36]/ SNAPP[37]/ OPT[38]/ OSP[39]/ PPV[40]/ ShortMAC[41]/ Faultprints[42]/ RFL[43]	增加一定开销实现源地址和路径验证	难以抵御中间节点合谋或回传信息被篡改等攻击
	TrueNet[44]	定位精度高	依赖可信计算模块
	VeriDP[45]/ NetSight[46]/ DynaFL[47]/ DFL[48]/ DYNAPFV[49]	集中制方式定位故障	易出现单点故障
	MINOS[50]	规范或检测路由行为	需中央管理器管理
	SNP[51]/ SPP[52]/ Zeno[53]/ Confluo[54]	具备一定故障诊断能力	难以发现离线故障
传输路径控制面安全	OA[55]/ Argus[56]/ DISCO[57]/ SPV[58]/ S-BGP[59]/ So-BGP[60]/ psBGP[61]/IRV[62]/ BGPsec[63]/ Path-End Validation[64]/ eOTC[65]/RLP[66]	部分解决前缀劫持、路径劫持、路由泄露问题	抗攻击能力有限、部分方案需第三方支持或开销较大、泄露 AS 间商业关系
	Listen and Whisper[67]/Consensus Routing[68]/ NetReview[69]/ TBGP[70]	提供较全面的解决方案	方案实际部署性未得到验证
	Pathlet[71]/ SCION[72]/ Internet Blockchain[73]	提供更彻底的解决方案	需进一步探索互联网增量部署机制

3.3 网络服务安全

网络服务安全主要包括数据访问和网络应用安全，以及支撑大量互联网应用的 PKI 等基础设施安全. 由于数据和应用直接面向用户，这类安全威胁可能会直接关系到用户财产甚至生命安全.

3.3.1 数据访问安全

实现云计算等场景下用户数据的保护，确保用户对数据的控制权. 文献[108]通过信息流控制（Information Flow Control，IFC）为进程或管道分配标签实现敏感数据安全保护. 由于传统 IFC 太过繁重，无法在大型云端直接使用，文献[74]中提出了 Riverbed，为用户提供验证服务器端代码运行在隐私保护环境的机制. Riverbed 架构如图 5 所示，其中白色部分为原来的组件，灰色部分为新增组件. 用户可以使用预定义模板文件定义信息流策略. 当用户产生一个 HTTP 请求，web 代理在用户端增加相应的数据流策略并发送. 在数据中心，Riverbed 使用关联的用户策略标记，仅在用户策略允许情况下执行. 相同数据流策略在 Riverbed 中称为一个集合（Universe），同一集合允许相同类型的数据操作. 作者对 Riverbed 性能进行了实验验证，在最坏情况下一些实际应用的速度仅仅降低了 10%. 但 Riverbed 需要用户端安装代理，实际用户体验和安全性需要进一步验证，且 Riverbed 的安全性依赖于可信硬件设施，如果要具备自主内生安全性，需与可信硬件进一步整合.

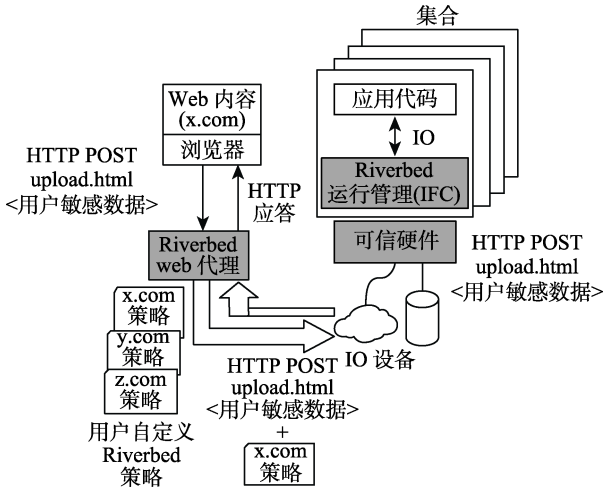


图 5 Riverbed 架构

Ghostor（Ghosts accessing the storage）[75]基于区块链实现用户匿名访问共享数据，确保数据操作的一致性，对敏感数据（如健康档案）访问提供保护. Ghostor 包括服务端和客户端，服务端处理客户端请求并在时间片结束后向区块链发布存储对象最新摘要及时间片信息，客户端接收应用访问请求，通过密钥获得相应的数据访问权并在每个时间片结

束时验证区块链上发布的信息. Ghostor 提供了更全面的用户隐私保护，但区块链性能是否满足实际应用访问效率还需进一步验证，同时系统对 IP 地址的隐私保护采用匿名网络，影响了自主内生安全性.

物联网应用场景对数据访问提出更高安全要求. He 等人提出一种智慧家庭访问控制和认证策略，提高 IoT 设备认证能力[109]. IotSan[76]通过对 IoT 系统“传感器—应用—执行”链检测信息泄露、错误配置等隐患. IOTGUARD[77]通过收集应用运行信息，动态存储运行行为，确保设备运行安全. 但这些方案主要解决物联网域内访问安全问题，不能应用于大规模网络跨域访问.

3.3.2　网络应用安全

由于网络攻击或自身故障引发的应用安全问题，可采用一些技术手段和策略提升应用安全性，如运行时随机化（RUNTIMEASLR）[110]技术通过地址空间布局随机化提高程序运行安全性. 同时大量应用漏洞研究和修补提升了应用安全性，如文献[111]中对浏览器扩展漏洞进行调研并提出建议. 文献[112]中提出检测高级持续性威胁（Advanced persistent threat，APT）的系统，为构建可信网络应用服务提供了辅助手段. 但构建可信网络应用服务环境需要建立及时发现并修补漏洞的机制. 现行漏洞发现方式主要是技术人员发现漏洞后上报，应用提供商检测通过后支付赏金，不仅存在滞后性，应用提供商的违约问题也无法得到监管，应用提供商与检测者难以建立信任. 一些方案通过去中心化机制建立应用提供商和检测者之间的信任关系.

Hydra[78]是一种具有标准化赏金机制和抗漏洞利用的智能合约. 作者提出了传统 N 版本编程的变种 NNVP（N-of-N-Version Programming），通过独立编写一种功能的多种实现版本同时运行，只有所有版本输出结果相同时才正常运行. 当出现一个版本的运行结果不一致时，可以判定出现了漏洞，自动产生赏金，黑客通过上报漏洞领取. 作者建立了一套赏金体系标准，激励漏洞发现者选择上报漏洞，避免漏洞利用攻击.

物联网作为一种大型分布式系统，去中心化网络特征和设备能力受限导致物联网面临更严重的安全威胁. 增强物联网生态中应用服务安全成为急需解决的难题[113]. 为提供安全物联网应用服务，Wu 等人[79]引入智能合约，设计了基于区块链的物联网系统漏洞检测平台 SmartCrowd. 物联网提供商提供保证金作为漏洞检测奖励，约束其提供更安全的应用，激励分布式检测者积极参与，构建可靠的物联网应用环境. 如图 6 所示，SmartCrowd 通过物联网服务提供商、物联网检测者、物联网设备与用户组成. 提供商发布应用时提供保证金，检测者检索区块链并下载应用，发现漏洞后向平台发送检测报告，提供商之间建立区块链，达成共识后触发智能合约，奖励检测者一定金额作为激励. 物联网用户通过检索区块链，根据报告选择更安全的应用. SmartCrowd 通过智能合约自动触发交易，在激励检测者参与的同时约束物联网应用提供商的行为，促使其发布更安全的应用. 在应用执行阶段，SmartRetro[80]针对物联网安全采用去中心化激励，用于回顾性检测，吸引分布式检测者参加安全检测，提供安全的网络应用.

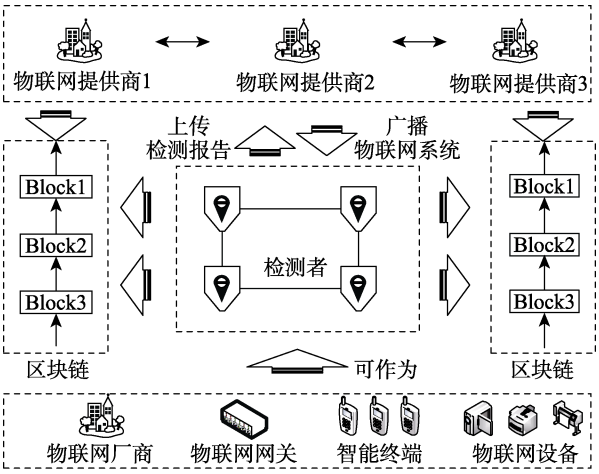


图 6　SmartCrowd 机制示意图

去中心化方案在建立用户与网络应用信任关系上具有一定优势，但方案实际安全性还需要进一步验证. 此外，如何将检测功能内生于互联网体系结构，仍然需要进一步探索.

3.3.3　PKI 安全

PKI 通过证书颁发机构（Certificate Authority，CA）实现证书管理等功能，为用户提供安全保护. CA 受到攻击后会带来非法撤销或颁发假证书等问题，大量研究致力于缓解和避免针对 CA 的攻击，主要包括多重验证方案和去中心化方案两大类.

（1）多重验证方案

Henry 等人[114]对现有 PKI 及 CA 漏洞攻击进行分析，认为 CA 证书颁发机制易受到攻击，并通过实验证实了攻击者可利用 BGP 漏洞成功实施攻击，通过劫持发往受害者的流量骗取 CA 颁发虚假证书. 作者提出 CA 通过多个节点（Vantage Point）验证，或采用 BGP 监控系统检测可疑路由等方式避免攻击者成功劫持验证过程流量，提升 PKI 安全性. 但

现有 CA 的脆弱性不仅表现在验证机制被攻击，CA 本身的可信性也需要得到验证. 为更大程度提升证书颁发过程可靠性，多重验证方案通过多个实体监督验证提升安全性.

Basin 等人[81]通过多重实体互相监督的方式，在可审计密钥设施（Accountable Key Infrastructure，AKI）基础上设计了抗攻击 PKI（Attack-Resilient Public-Key Infrastructure，ARPKI）. 通过 n 个实体互相监督保证当 n-1 个实体被攻击时安全运行. n 个实体包括 n-1 个 CA 和 1 个可信日志服务器（Integrity Log Server，ILS）. 实际运行中，域名 A 首先向 CAs 和 ILSs 注册证书（ARCert），CAs 不但在域名拥有者注册证书时检查拥有者的身份，更重要的是检查 ARCert 中来自不同 CAs 的证书，以及从 ILSs 下载所有接受申请并验证 ILSs 行为. 通过 CAs 和 ILSs 的监督，提供了较强的安全性能，但由于 CAs 之间依次传递消息，n 个实体都需要处理注册、确认和更新操作，当 n 的数量较大时，系统效率会降低，n 较小时系统抗攻击能力较弱.

（2）去中心化方案

去中心化方案通过激励各方参与恶意行为检举促进 CA 主动重视自身安全. IKP（Instant Karma PKI）[82]利用区块链共识和智能合约，从以下两个方面建立激励机制：一是通过分布式检测者参与 CA 证书发放检测过程，激励检测者提高检测可靠性；二是通过惩罚激励 CA 正确执行证书发放. 实际运行中，CA 在系统缴纳注册费完成注册，费用放入 CA 余额，余额越多，说明 CA 赔偿能力越高，用户可选择余额较多的 CA 颁发证书. 域名持有者选择自己信任的 CA 申请证书，并在注册域名时指定信任 CA. 检测者上报恶意证书后，自动从 CA 赔付余额中得到一定金额. CA 违约信息作为后续用户选择的参考，使 CA 更谨慎的投入安全维护. IKP 的不足是没有考虑 CA 私钥被盗时，攻击者发布恶意证书，巨大的赔付额给 CA 带来严重损失. 同时，作为保管金钱的平台，IKP 本身的安全性也值得商榷.

CertChain[83]通过去中心化方式对 CA 进行监督. 作者分析指出，现阶段引入日志服务器来记录证书的发布及操作信息容易受到单点攻击. 为了确保日志服务器的一致性和安全性，作者提出一种基于可靠性排名的共识机制，设计了支持可追溯证书转发的数据结构，及基于双计数布隆过滤器（Dual Counting Bloom Filter，DCBF）消除假阳性的方法，实现对证书状态高效查询. CertChain 包括数据层、网络层、扩展层以及应用层. 数据层基于区块链设计高效检索机制，通过数据结构解决效率问题. 网络层设计了基于 P2P 和洪范的策略，提高可靠性. 扩展层设计了可靠性排名基础上的共识和激励，根据 CA 发布证书量和执行过的恶意行为对其历史行为排名，排名越高，区块产生概率就越高，这种激励方式有利于 CA 持续保证行为正常性；应用层设计了证书的注册、更新、撤销和验证，直接为用户提供服务.

BlockPKI[84]通过智能合约构建了一种去中心化 PKI，提出了自动对多个 CA 支付的框架，通过多个 CA 执行提供更高安全性. 作者在以太坊上进行了测试验证，在 CA 数量达到 20 时，客户端验证签名的时间约为 0.102ms，密钥绑定的时间约为 0.052ms，这个增加对用户带来的影响几乎可以忽略不计，一定程度上证实了去中心化 PKI 的可行性.

IKP、CertChain、BlockPKI 等去中心化方案具备了一定内生安全性能，但方案本身存在一定不足，如证书历史查询对用户隐私保护不足，CA 私钥或平台被攻击可能引发资金风险. 此外，去中心化方案的实际运行效率能否满足用户体验是方案能否实际部署的关键.

如表 4 所示，数据访问和应用服务安全方面，还没有内生的安全机制建立应用和用户的信任. 解决 PKI 出现的安全问题，去中心化基础设施在提供安全性上具有优势，但现有方案存在一定风险，且尚未验证效率是否满足用户实际需求. 因此，实现用户与应用间的信任机理，形成真实可信的网络应用环境，还需要更深入的研究.

表 4 网络服务安全方案小结

类型	策略	优点	不足
数据访问安全	Riverbed[74]/ Ghostor[75]	云场景下安全访问	存在第三方依赖
	IotSan[76]/ IOTGUARD[77]	物联网应用场景下安全访问	仅支持域内小范围访问
网络应用安全	Hydra[78]/ SmartCrowd[79] /SmartRetro[80]	通过去中心化方式激励用户参与营造安全网络环境	安全性还需进一步验证，检测功能没有内生于应用
PKI 安全	ARPKI[81]	多重实体验证提供容错能力	实体数量不足时安全性较低，过大时效率不足
	IKP[82]/ CertChain[83]/ BlockPKI[84]	去中心化方式提升 PKI 安全能力	隐私保护不足，CA 私钥或平台被攻击可能引发资金风险，尚未验证实际运行效率

3.4　新型网络体系结构设计

新型网络体系结构方案采用全新设计解决互联网现有或可能遇到的各类问题，如通过自认证特性提供内生安全功能，从根本上解决网络安全问题.

XIA（eXpressive Internet Architecture）[85]核心是将内生的安全标识用于通信. XIA 使用标识和地址分离设计， NID（Network ID）代表网络域或子网，用来定位网络地址，HID（Host ID）代表主机标识. 路由器通过 NID 标识找到网络，然后由 HID 标识转发数据到主机. XIA 支持主机和域鉴别源地址真实性，在第一跳路由器验证主机源地址真实性，各网络自治域边界路由器依次检查上一跳是否合法. 网络标识符（NID 和 HID）能够与公钥绑定提供自认证方式，但作为通信主体的用户（主机名称、域名）需要通过 PKI 实现用户标识符与公钥绑定，影响了其自主内生安全性能.

为支持网络移动性和可信性，MobilityFirst [86]使用标识与位置分离的机制，认为逻辑上集中的全局名称服务可增强移动性和安全性. MobilityFirst 标识包括用户标识符（Name）、全局唯一标识（Globally Unique Identifier，GUID）和网络地址（Network Address，NA）. Name 用于标识用户、内容或群组等名称. GUID 采用通信实体的公钥哈希值，提供自认证能力，具备一定的内生安全性. NA 作为路由，与 GUID 动态绑定. 每个通信实体拥有一个 Name 和对应 GUID，但每个 Name/GUID 可设置多个网络地址 NA. MobilityFirst 通过用户标识证书解析服务（Name Certificate & Resolution Service，NCRS）绑定 Name 和 GUID. 全局用户标识解析服务（Global Name Resolution Service，GNRS）存储并更新 GUID 和 NA 的映射关系，并利用 GUID 公钥对更新进行鉴别. 由于 GUID 的自认证特性，MobilityFirst 可以摆脱 IP 地址缺乏源地址认证带来的劫持、假冒等现有互联网问题. 其不足是大量节点频繁移动时，需要两次查询“Name- GUID- NA”得到对端网络地址，对系统能力提出了较高要求；通过 PKI 分发公钥证书，用户量过大时可能存在证书管理能力不足问题. 此外，与 XIA 一样，MobilityFirst 同样存在对 PKI 的依赖.

NDN（Named Data Networking）[87]是由 Zhang Lixia 等人提出的一种新型网络体系结构. NDN 摒弃了以 IP 为中心的路由设计，以内容名称（Name）为基础设计路由. 使用者交换两种类型数据包：兴趣包和数据包（Interest and Data）. 两种类型的数据包都带有一个名称，使用者将所需数据段名称放入兴趣包中，发送到网络. 兴趣包到达具有请求数据的节点，节点将返回一个包含名称和内容的数据包，以及绑定两者的提供商密钥签名. 和 URL 相似，NDN 命名采用的结构如/ucla/videos/demo.mpg 所示，这个命名可以和/ucla/videos/demo.mpg/1/3 共同聚合于/ucla，通过层次化保证路由快速收敛. NDN 由数据本身加密保证安全，与互联网通过端节点保证安全相比，可以防范欺骗和篡改；通过名称实现路由，避免了地址空间耗尽、NAT 穿透、地址管理等问题；在用户鉴别方面，NDN 将用户标识符和网络标识符合并，通过内容命名与公钥绑定实现用户鉴别，提高安全性，但 NDN 对用户的鉴别需要第三方（如 PKI）提供证书验证.

可扩展的下一代认证基础设施（Scalable Authentication Infrastructure for Next-generation Trust，SAINT）[88]将现有信任机制分为三个方面：用于路由认证的 BGPsec，用于域名认证的 DNSSEC[115]，以及用于端到端认证的 TLS[116]，并进一步将这种信任关系划分为路由信任和服务信任（包括域名和端到端信任）. 作者认为现有三种信任机制并没有形成一个整体，同时存在如过于中心化的域名服务、BGPsec 效率低下，CA 权力难以有效监督等问题，无法为用户提供充分的信任机制. 作者基于 SCION 实现全局认证、域内授权，设计了兼具灵活性、高效率和透明性的认证机制，其核心为每个 ISD 配置一个信任根，通过信任根配置文件（Trust Root Configuration Files，TRC Files）为用户提供快速查询和更新信息，通过跨 ISD 签名机制建立全局信任. 用户选择自己的 ISD 作为信任锚，在不同 ISD 移动时为用户提供灵活的全局信任机制. 实际使用中，SAINT 建议以国家作为信任机制的分界，每个国家配置一个 ISD，AS 和服务器均采用公私钥认证，确保用户通过 TRC Files 得到全局可信任服务. 作者通过模拟测试和基于 SCION 的实际部署验证了 SAINT 比现有信任机制更具有效性和可靠性，但同时也存在如以国家建立 ISD 是否可行，TRC Files 的初始发布如何保证安全性等问题.

总体说来，XIA、MobilityFirst、NDN 将安全功能与协议功能耦合，提供了一定的内生安全能力，但仍然无法实现用户标识符、网络标识符和公钥的天然绑定，需要通过 PKI 提供公私钥对，从而不能提供自主的内生安全能力. 陈钟等人通过基于组合公钥密码体制的自认证标识命名方案[3]，用于标识安全绑定，为 XIA、MobilityFirst 和 NDN 中支持身份或地址鉴别的方法提供了更强的自主安全性.

SAINT 建立了全局的信任机制,但与现有机制相比,其建立和验证过程过于繁琐,同时其 ISD 机制能否适用于互联网还需进一步验证.

Zave 和 Rexford 在文献[89]中提出,互联网面临安全问题急剧增长,以及应用场景不断变化(如终端移动性、云计算大量发展、电信和娱乐基础设施向互联网迁移),如 MobilityFirst、NDN 等新架构既无法彼此统一,在解决互联网问题时所采取的方式也过于复杂. 作者认为 Internet 由大量自治网络组成,基于组合架构(Compositional Architecture)模型的研究可能是建立兼具灵活性和可管理性网络体系结构的关键. 新模型中,互联网由可组合网络灵活组合,每个可组合网络都具有名称空间、路由、转发协议、会话协议和目录等机制. 由于网络用途、地理范围、成员资格不同,这些机制可能各不相同,但同一类型网络可以实现模式重用. 同时,组合网络模型可以验证可信赖服务,因为可信赖服务在网络间接口处定义,通常取决于多个网络的交互. 组合网络基于互联网实际应用在更高的抽象层次上对互联网现有结构进行研究,希望找到真正满足可预见需求,甚至可以适应不可预见需求的体系结构,提供了基于互联网现状通过分析工具和推理技术进行形式化验证的手段.

全维可定义多模态智慧网络(PINet)[90]从网络构造的角度,自底向上定义,通过细粒度组织方式动态重构网络,扩展网络功能和效用. 全维可定义技术对开放架构下基础网络软硬件、协议、接口、芯片等进行定义,支持 IP、内容标识、身份标识、地理空间标识等多模态标识共存与协同,突破传统网络 IP“窄腰”结构制约,通过基于动态异构冗余的内生安全结构扰乱攻击链,获得网络内生安全效应.

另一方面,大量研究致力于新型网络体系结构在互联网增量部署,以在实际应用中验证新型网络体系结构的能力,Trotsky[117]是其中一种具备可行性的方案. Trotsky 的前提是现有互联网存在固有缺点,同时却又根深蒂固,需要一种既能从根本上解决问题,又能在现有网络增量部署的方案. 作者认为网络安全问题包括通信双方的可用性(Availability)和身份可认证性(Identity)、数据的来源(Provenance)和真实性(Authenticity)、隐私性(Privacy),除了 Availability 外,都可以通过加密等方法在端节点进行处理,而 Availability 需要在网络层解决,以抵御 DDoS 等攻击. Trotsky 本身并不解决安全问题,而是为更安全的网络层协议提供框架. 同时,立足 SDN/NFV 技术及边缘计算技术的应用,以及基于自治域架构组成互联网这一现实,在 L3 层上设计了 L3.5 层,并在域的边缘(Domain Edges)设置处理器(Trotsky-Processors,TPs),通过 TPs 为端到端的连接建立逻辑管道(Logical Pipe). 基于 Trotsky 框架作者整合了 NDN、XIA 等协议,验证了 Trotsky 框架在现有互联网基础上提供“革命性”设计的能力,也为诸如 Pathlet、AIP、SCION 等设计实现提供了平台(由于代码库等原因作者并没有移植这些协议到 Trotsky 框架). 可部署性方面,实验环境下通过软件处理 10Tbps 数据,需要投入约 200,000 美元. 随着应用的拓展和深入,如采用硬件支持,能够进一步提高效率. Trotsky 框架在现有互联网上提供了高效且向后兼容的 L3.5 层处理方式,降低了新架构实现的门槛,但其部署还需要运营商的支持. 总体说来,Trotsky 为现有互联网架构演进提供了新的思路和实践,使得不断改变互联网直至实现内生安全体系结构成为可能.

当然,解决方案在互联网具有可部署性仅仅是能够部署的前提,实际部署还受多种因素影响. 首先是方案解决安全问题的能力,如在针对入侵检测系统(Intrusion Detection System,IDS)性能提升上,IDS 标准化器[118]能否具备满足用户需求的能力将直接影响部署者积极性. 同时还需考虑用户接受能力和体验,如 HTTPS 加入了安全性能较高的传输层安全协议 TLS,然而其部署并不令人满意,文献[119]中分析了由于客户端时钟不正确、中间件能力不足影响用户体验,导致用户真正遭受攻击时对警告无动于衷. 文献[120]中对 HTTPS 终端用户和管理者分别进行调研,发现两者对信息加密及 HTTPS 都存在误解. 终端用户低估了 HTTPS 的益处,经常忽略安全提醒,管理者不理解功能协议组件的相互作用. 因此,解决方案在互联网中的可部署性,不仅是一个技术问题,也关系到用户能力和心态等多种因素,构建互联网内生安全体系结构,需要分析并考虑这些影响因素.

4 构建互联网内生安全体系结构

互联网体系结构需要兼顾网络可服务性、可扩展性、可部署性、可演化性和可信性,选取最适合的协议或机制[121]. 在不改变 TCP/IP 基础架构前提下,为构建互联网内生安全体系结构,同时满足“自主免疫”和“可信可控”要求,解决大规模网络实体和网络行为各关联要素可验证、可管控、可追溯等真实可信核心问题,我们从以下三个方面建立网络和用户之间的信任关系:

（1）建立支持多类型端设备接入的真实可信地址命名机制及验证体系，解决端设备地址信任问题.

（2）建立支持路径验证及错误定位的路由行为检测体系，解决转发路径和转发行为不可信问题.

（3）建立支持真实可信应用的基础设施，解决单一节点安全脆弱性与信任失效等问题，构建真实可信的网络应用生态.

如图 7 所示，我们引入了区块链作为建立信任关系的基础[122]，体系结构具备分层分级（接入网、域内、域间）的源地址验证能力，分组转发过程的可信验证和错误定位能力，网络用户行为的可信追溯能力，以及应用服务安全增强能力，建立用户与网络的信任机制.

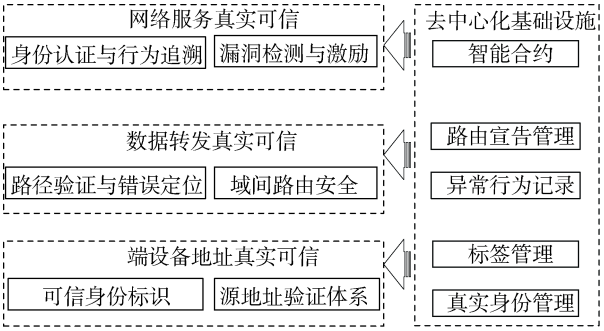


图 7　真实可信新一代互联网体系结构

4.1 端设备地址真实可信

为实现端设备地址真实可信，我们综合权衡地址标识体系的互通、成本、安全和兼容性，将设备真实地址与身份相互融合，基于真实可信地址标识，建立接入网、域内和域间真实可信地址验证体系.

（1）设计真实可信的地址标识. 考虑地址的安全性与可验证性，标识的类别和形式，通过分离 IP 地址定位符空间与标识符空间，我们将设备真实身份与真实地址相互融合，实现地址格式的平滑革新. 地址标识遵循 IPv6 地址格式，在 IPv6 地址后 64 位嵌入身份标识，增加标识符语义. 身份标识由用户组织、编号、时间戳等构成，通过哈希截短、加密等方式编码，带有自认证特性，并随时间动态变化，实现终端设备身份动态标识和隐私保护.

（2）建立真实可信地址验证体系. 如图 8 所示，基于 SAVA 体系架构，结合真实身份机制，实现接入网、自治域内、自治域间分层级的真实源地址验证，确保端设备地址真实可信. 接入网验证功能由地址生成服务器、身份管理服务器、身份追溯服务器及接入验证交换机共同实现. 身份管理服务器通过 802.1x 协议查证申请接入的端节点身份，并将验证结果告知地址生成服务器，由其为端设备生成携带真实身份标识的合法 IPv6 地址. 具备 SAVI 功能的接入交换机监听地址生成过程并建立地址与端口绑定关系，IP 地址发送分组时，接入交换机查证绑定关系实现主机粒度的源地址验证. 对于物联网等异构网络，接入网关基于设备指纹等特征完成节点设备认证. 自治域内管理服务器管理域内地址前缀，将域内路由器的每个入口与一组有效的源地址前缀关联，实现 IP 前缀粒度源地址验证及过滤. 自治域间由 AS 组建信任联盟，实现自治域粒度的源地址验证. 信任联盟成员边界路由器为通过 AS 级别源地址前缀检查的本域发往其它联盟成员的报文添加带有可验证标签的扩展报文头，保证源自本 AS 的报文源地址真实可信，目的端边界路由器对收到的报文进行标签验证，确保 AS 地址前缀未被篡改. AS 信任联盟的成员通过动态更新的状态机保持一致，AS 前缀及标签初始状态通过去中心化方式将信息摘要及链接存储于区块链，确保 AS 地址前缀及状态可追溯、可验证.

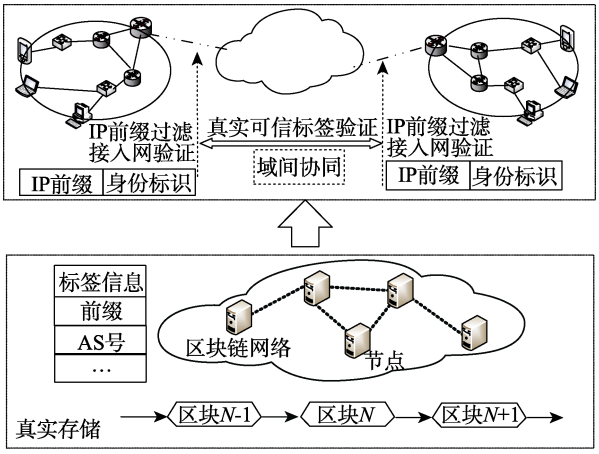


图 8　真实可信地址验证体系

4.2 传输路径真实可信

为实现数据分组传输路径真实可信，在数据传输全生命周期，数据面通过路径验证实现路由节点过滤恶意流量，端节点验证数据真实传输路径；控制面基于分布式共识和信任度建立域间路由安全策略，实现通信服务“可信、可靠、可验证”.

（1）传输路径数据面真实可信方面，我们重点从效率和鲁棒性上设计解决问题的思路，既提供路由节点过滤能力，又提供端节点真实路径验证能力. 采用基于信任联盟的标签解决共享密钥问题，采用随机标识方式减少数据包头部标识长度，改变逐跳

逐包的验证方式，卸载验证能力至端节点，以降低计算及通信开销. 路径验证过程如图 9 所示，发送分组前，源端发送请求数据包，路由器节点与目的端同步各路由器节点针对本次会话的共享密钥（标签），源端发送请求数据包，路由节点依次添加信任联盟标签，目的端验证后存储对应标签，作为与路由节点的共享密钥. 目的端向源端发送应答数据包，源端验证后存储对应标签. 数据传输过程中，路由节点通过随机方式完成恶意流量过滤及路由节点标识添加，标识包括路由器链路信息、剩余跳数，以及由共享密钥和以上信息经哈希计算生成的验证码；源端采用随机标识的方式，等概率为路由节点计算标识，对应路由节点验证标识，过滤标识不一致的恶意流量；同时，路由节点也通过随机方式等概率添加标识. 目的端收到数据包后，首先验证源端及路由节点验证码的正确性，随后根据标识中路由器连接关系，恢复数据流实际转发路径，与目的端拥有的本次会话期望路径比较，实现路径验证和错误定位，并将异常结果告知源端. 此外，对网络异常行为采用去中心化方式形成共识，提供可追溯能力. 方案尽可能降低路由节点处理能力，路由节点仅需少量哈希计算，适应互联网“核心简单，边缘复杂”的实际情况，提供可增量部署的互联网传输路径验证能力.

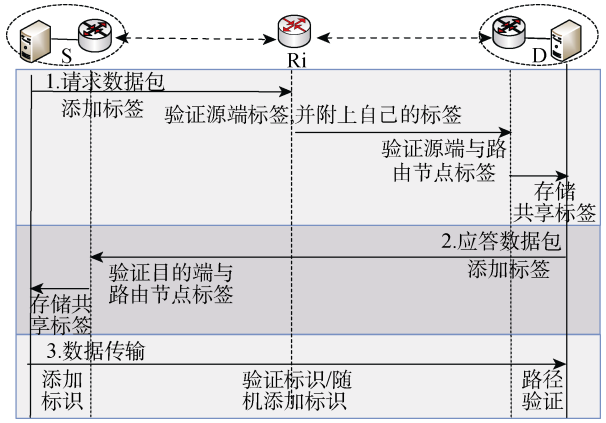


图 9 数据面路径验证流程

（2）传输路径控制面真实可信方面，如图 10 所示，通过区块链记录 AS 号、前缀、AS 邻居关系及路由器公共参数等信息，通过真实存储建立分布式共识，提供全局可验证能力. 路由决策前，通过形成分布式共识的真实 AS 号与前缀绑定关系识别前缀劫持；通过真实邻居关系识别 AS 虚假路径宣告. 为提供可信路由决策，基于路由器节点交互行为及攻击特征，建立分级可信的节点行为信任度，在路由通告路径上，基于信任度建立可传递的信任关系，提升路由决策安全性.

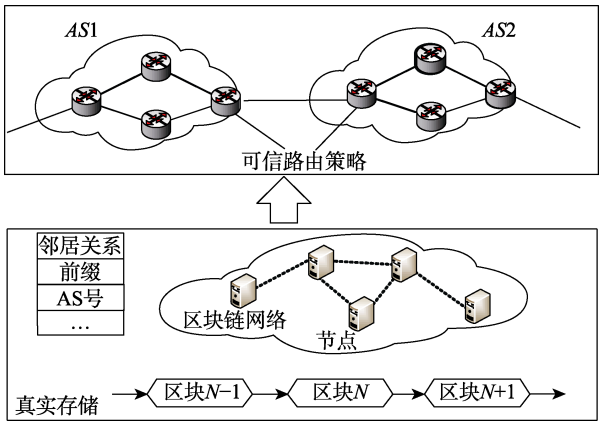


图 10 真实可信路由计算

4.3 网络服务真实可信

建立互联网数据访问与应用服务信任机理，提供真实可信的云/边缘计算数据访问，以及应用发布和运行阶段的有效管控和监测. 我们将区块链作为解决复杂跨域应用下信任问题的有效手段，通过去中心化基础设施，解决中心节点安全脆弱性与信任失效等问题.

（1）数据访问真实可信方面，以真实身份为信任锚点，去中心化基础设施为信任支撑，实现基于去中心化密钥管理架构的身份认证与行为追溯. 去中心化密钥管理架构由网关、CA、主链和局域网子链组成. 内部端设备证书由网关进行签发，生成局域网子链，控制访问权限. 重要设备（如网关）证书通过主链达成共识，如图 11 所示，拥有真实地址的终端根据身份 ID 由终端生成公私钥，向 CA 提交身份证明、IP 地址、公钥和签名，CA 对申请真实

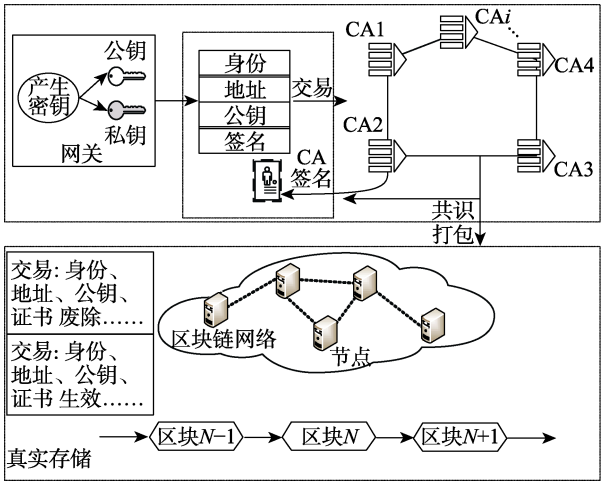


图 11 去中心化密钥管理设施

性进行验证后，生成包含 CA 签名的数字证书，将终端地址、公钥、证书等信息发送到区块链主链，通过共识机制形成在用公钥数据库. 对敏感服务请求，访问端进行数据访问时通过私钥附带签名，目的端接收访问端数据签名，通过区块链查询到访问端公钥，对数据包签名进行认证，认证通过后响应终端访问请求，实现跨域协同的身份认证. 此外，用户访问行为通过去中心化方式形成分布式共识，实现全局可查证可追溯，确保数据访问真实可信.

（2）应用服务真实可信方面，基于应用提供商、用户、检测者真实身份，引入智能合约，形成对应用漏洞兼具效率和可靠性的检测. 如图 12 所示，以真实身份为基础，应用提供商和需要提供漏洞报告的用户提供保证金，作为对漏洞检测者的奖励. 用户通过智能合约发布需要检测的应用，检测者检测到漏洞后触发智能合约，经过应用提供商检测通过后写入区块链. 智能合约建立内置问责机制，从应用提供商保证金自动为漏洞检测者提供相应的奖励，约束应用提供商发布更安全的应用，同时，智能合约能够根据区块链记录对用户进行反馈，自动将用户的部分保证金用于激励检测者，激励检测者积极参与应用运行阶段监测. 应用提供商、用户和检测者通过智能合约建立应用漏洞检测机制，实现全局“可协同、可验证、可追溯”，推动形成安全、可信的应用服务生态系统.

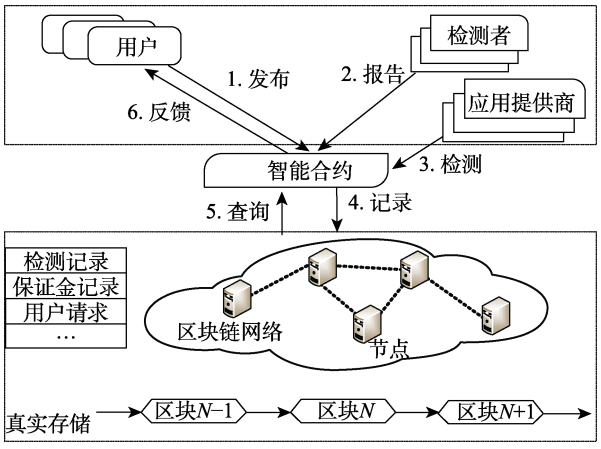


图 12　去中心化应用漏洞检测机制

综上，我们提出的互联网内生安全体系结构通过可信身份标识和源地址验证体系实现端设备地址真实可信，通过路径验证与错误定位、域间路由安全实现数据转发过程真实可信，并通过身份验证与行为追溯实现数据安全访问，提供应用发布与运行阶段安全监管能力，建立彼此信任的用户空间及网络空间，实现内生于网络的安全保障.

5　结　论

本文从端设备地址、传输路径和网络服务安全，以及新型体系结构设计等方面分析了现有互联网安全问题解决方案及其内生安全特性，并对各类安全方案的可部署性进行了分析. 总体说来，现有互联网安全问题解决方案，无论是针对安全问题的修补，还是全新架构设计，已有大量具备一定内生安全特性的解决方案，但目前缺乏将这些解决方案整合起来的体系结构，即没有设计从硬件、软件到协议完整的内生安全解决方案，很难从根本上解决安全问题.

网络安全与个人乃至国家安全息息相关，构建互联网内生安全体系结构，需要在借鉴互联网发展经验和教训的基础上，准确分析网络面对的安全威胁，综合运用最新技术成果，科学设计网络协议和实现，同时考虑系统的可部署性，为用户构建安全、高效的网络环境. 本文提出了构建互联网内生安全体系结构的思路和方向，希望能够为后续研究者提供建议和参考.

参　考　文　献

[1] Wu Jianping, Liu Ying, Wu Qian. Advances in new generation internet architecture theory. Science in China (Series E: Information Sciences), 2008, 38(10): 1540-1564 (in Chinese)
(吴建平, 刘莹, 吴茜.新一代互联网体系结构理论研究进展. 中国科学(E 辑: 信息科学), 2008, 38(10): 1540-1564)

[2] Xu Ke, Zhu Liang, Zhu Min. Architecture and key technologies of internet address security. Journal of Software, 2014, 25(1): 78-97 (in Chinese)
(徐恪, 朱亮, 朱敏.互联网地址安全体系与关键技术.软件学报, 2014, 25(1): 78-97)

[3] Chen Zhong, Meng Hongwei, Guan Zhi. Research on intrinsic security in future internet architecture. Journal of Cyber Security, 2016, 1(2): 36-45 (in Chinese)
(陈钟, 孟宏伟, 关志. 未来互联网体系结构中的内生安全研究. 信息安全学报, 2016, 1(2): 36-45)

[4] Zave Pamela, Rexford Jennifer. Patterns and interactions in network security. ACM Computing Surveys, 2021, 53(6): 1-37

[5] Ward Rory, Beyer Betsy. BeyondCorp: a new approach to enterprise security. Login Usenix Magazine, 2014, 39(6): 6-11

[6] Osborn Barclay, McWilliams Justin, Beyer Betsy, et al. BeyondCorp: design to deployment at google. Login Usenix Magazine, 2016, 41(1): 28-35

[7] Chen Zhong, Guan Zhi, Meng Hongwei, and Meng Ziqian. A survey of future internet architecture and security design. Journal of Information Security Research, 2015, 1(01): 9-18 (in Chinese)
(陈钟, 关志, 孟宏伟, 孟子骞. 未来网络体系结构及安全设计综述.信息安全研究, 2015, 1(01): 9-18)

[8] Yu Han, Wang Yi, Shen Chang-xiang. A new model of information security system based on immune system. Acta Electronica Sinica, 2006, 34(12A): 2455-2457(in Chinese)
(于涵, 王毅, 沈昌祥. 一种基于免疫系统原理的信息安全系统新模型. 电子学报, 2006, 34(12A): 2455-2457)

[9] Yu Quan, Ren Jing, Zhang Jiyan, et al. An immunology-inspired network security architecture. IEEE Wireless Communications, 2020, 27(5):168-173

[10] Wu Jiangxing. Cyberspace Mimic Defense: Generalized Robust Control and Endogenous Security. Springer, 2019

[11] Wu Jianping, Lin Song, Xu Ke, et al. Advances in evolvable new generation internet architecture. Chinese Journal of Computers, 2012, 35(6): 1094-1108 (in Chinese)
(吴建平, 林嵩, 徐恪等. 可演进的新一代互联网体系结构研究进展. 计算机学报, 2012, 35(6): 1094-1108)

[12] Lv Liang, Zhang Yuchao, Li Yusen, et al. Communication-aware container placement and reassignment in large-scale internet data centers. IEEE Journal on Selected Areas in Communications, 2019, 37(3): 540-555

[13] Chen Fei, Li Haitao, Liu Jiangchuan, et al. Migrating big video data to cloud: a peer-assisted approach for vod. Peer-to-Peer Networking and Applications, 2018, 11(5): 1060-1074

[14] Li Tong, Wang Kezhi, Xu Ke, et al. Communication and computation cooperation in cloud radio access network with mobile edge computing. CCF Transactions on Networking, 2019, 2: 43-56

[15] Xu Ke, Qu Yi, Yang Kun. A tutorial on internet of things: from a heterogeneous network integration perspective. IEEE Network, 2015, 30(2): 102-108

[16] Peng Tao, Leckie Christopher, Ramamohanarao Kotagiri. Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys, 2007, 39(1): 1-42

[17] Kim Tiffany Hyun-Jin, Huang Lin-Shung, Perrig Adrian, et al. Accountable key infrastructure (AKI): a proposal for a public- key validation infrastructure//Proceedings of the 22nd International World Wide Web Conference. Rio de Janeiro, Brazil, 2013: 679-690

[18] Wu Jianping, Bi Jun, Li Xing, et al. A source address validation architecture (SAVA) testbed and deployment experience. RFC 5210, 2008, https://doi.org/10.17487/RFC5210

[19] Wu Jianping, Bi Jun, Bagnulo M., et al. Source address validation improvement (SAVI) framework. RFC 7039, 2013. https://doi.org/10.17487/RFC7039

[20] Anat Bremler-Barr, Hanoch Levy. Spoofing prevention method// Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Miami, USA, 2005: 536-547

[21] Liu Xin, Li Ang, Yang Xiaowei, et al. Passport: secure and adoptable source authentication//Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation. San Francisco, USA, 2008: 365-376

[22] Bi Jun, Liu Bingyang, Wu Jianping, et al. Preventing IP source address spoofing: a two-level, state machine-based method. Tsinghua Science and Technology, 2009, 14(4): 413-422

[23] Li Jie, Wu Jianping, Xu Ke, et al. An hierarchical inter-domain authenticated source address validation solution. Chinese Journal of Computers, 2012, 35(1): 85-100 (in Chinese)
(李杰, 吴建平, 徐恪, 等. Hidasav: 一种层次化的域间真实源地址验证方法. 计算机学报, 2012, 35(1): 85-100)

[24] Liu Bingyang, Bi Jun. DISCS: a distributed collaboration system for inter-as spoofing defense//Proceedings of the 44th IEEE International Conference on Parallel Processing. Beijing, China, 2015: 160-169

[25] Jia Yihao, Liu Ying, Ren Gang, et al. RISP: An rpki-based inter-as source protection mechanism. Tsinghua Science and Technology, 2018, 23(1): 1-12

[26] Kent S., Seo K. Security architecture for the internet protocol. RFC 4301, 2005. https://doi.org/10.17487/RFC4301

[27] Moskowitz R., Nikander P., Jokela P., et al. Host identity protocol. RFC 5201, 2008. https://doi.org/10.17487/RFC5201

[28] Naylor David, Mukerjee Matthew K., Steenkiste Peter. Balancing accountability and privacy in the network//Proceedings of ACM SIGCOMM 2014 Conference. Chicago, USA, 2014: 75-86

[29] Andersen David G., Balakrishnan Hari, Feamster Nick, et al. Accountable internet protocol (AIP)//Proceedings of ACM SIGCOMM 2014 Conference. Seattle, USA, 2008: 339-350

[30] Taeho Lee, Christos Pappas, David Barrera, et al. Source accountability with domain-brokered privacy//Proceedings of the 12th International on Conference on Emerging Networking Experiments and Technologies. Irvine, USA, 2016: 345-358

[31] Boris Danev, Thomas S. Heydt-Benjamin, Srdjan Capkun. Physical-layer identification of RFID devices//Proceedings of the 18th USENIX Security Symposium. Montreal, Canada, 2009: 199-214

[32] Danev Boris, Capkun Srdjan. Transient-based identification of wireless sensor nodes//Proceedings of the 8th International Conference on Information Processing in Sensor Networks. San Francisco, USA, 2009: 25-36

[33] Adam C. Polak, Dennis L. Goeckel. Identification of wireless devices of users who actively fake their RF fingerprints with artificial data distortion. IEEE Transactions on Wireless Communications, 2015, 14(11): 5889-5899

[34] Yaar Abraham, Perrig Adrian, Song Dawn. Pi: a path identification mechanism to defend against DDoS attacks// Proceedings of the 2003 IEEE Symposium on Security and Privacy. Oakland, USA, 2003: 93-107

[35] Yaar Abraham, Perrig Adrian, Song Dawn. StackPi: new packet marking and filtering mechanisms for DDoS and IP spoofing defense. IEEE Journal on Selected Areas in Communications, 2006, 24(10): 1853-1863

[36] Naous Jad, Walfish Michael, Nicolosi Antonio, et al. Verifying and enforcing network paths with icing//Proceedings of the 2011 Conference on Emerging Networking Experiments and Technologies. Tokyo, Japan, 2011: 1-12

[37] Parno Bryan, Perrig Adrian, Andersen Dave. SNAPP: stateless network-authenticated path pinning//Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security. Tokyo, Japan, 2008: 168-178

[38] Kim Tiffany Hyun-Jin, Basescu Cristina, Jia Limin, et al. Lightweight source authentication and path validation// Proceedings of the ACM SIGCOMM 2014 Conference. Chicago, USA, 2014: 271-282

[39] Cai Hao, Wolf Tilman. Source authentication and path validation with orthogonal network capabilities//Proceedings of the 2015 IEEE Conference on Computer Communications Workshops. Hong Kong, China, 2015: 111-112

[40] Wu Bo, Xu Ke, Li Qi, et al. Enabling efficient source and path verification via probabilistic packet marking//Proceedings of the IEEE/ACM International Symposium on Quality of Service. Banff, Canada, 2018: 1-10

[41] Zhang Xin, Zhou Zongwei, Hsiao Hsu-Chun, et al. ShortMAC: efficient data-plane fault localization//Proceedings of the 19th Annual Network and Distributed System Security Symposium. San Diego, USA, 2012: 1-14

[42] Basescu Cristina, Lin Yue-Hsun, Zhang Haoming, et al. High-speed inter-domain fault localization//Proceedings of the IEEE Symposium on Security and Privacy. San Jose, USA, 2016: 859-877

[43] Wu Bo, Xu Ke, Li Qi, et al. RFL: robust fault localization on unreliable communication channels. Journal of Computer Networks, 2019(158): 158-174

[44] Zhang Xin, Zhou Zongwei, Hasker Geoffrey, et al. Network fault localization with small TCB//Proceedings of the 19th annual IEEE International Conference on Network Protocols. Vancouver, Canada, 2011: 143-154

[45] Zhang Peng, Li Hao, Hu Chengchen, et al. Mind the gap: monitoring the control-data plane consistency in software defined networks//Proceedings of the 2th International Conference on Emerging Networking Experiments and Technologies. Irvine, USA, 2016: 19-33

[46] Handigol Nikhil, Heller Brandon, Jeyakumar Vimalkumar, et al. I know what your packet did last hop: using packet histories to troubleshoot networks//Proceedings of the 11th USENIX Symposium on Networked Systems Design and Implementation. Seattle, USA, 2014: 71-85

[47] Zhang Xin, Lan Chang, Perrig Adrian. Secure and scalable fault localization under dynamic traffic patterns//Proceedings of the IEEE Symposium on Security and Privacy. San Francisco, USA, 2012: 317-331

[48] Zhang Xin, Zhou Fanfu, Zhu Xinyu, et al. DFL: secure and practical fault localization for datacenter networks. IEEE/ACM Transactions on Networking, 2014, 22(4): 1218-1231

[49] Li Qi, Zou Xiaoyue, Huang Qun, et al. Dynamic packet forwarding verification in SDN. IEEE Transactions on Dependable and Secure Computing, 2019, 16(6): 915-929

[50] Xu Lei, Xu Ke, Shen Meng, et al. MINOS: regulating router dataplane actions in dynamic runtime environments//Proceedings of the ACM Turing 50th Celebration Conference-China. Shanghai, China, 2017: 1-10

[51] Zhou Wenchao, Fei Qiong, Narayan Arjun, et al. Secure network provenance//Proceedings of the 23rd ACM Symposium on Operating Systems Principles. Cascais, Portugal, 2011: 295-310

[52] Chen Ang, Haeberlen Andreas, Zhou Wenchao, et al. One primitive to diagnose them all: architectural support for internet diagnostics//Proceedings of the Twelfth European Conference on Computer Systems. Belgrade, Serbia, 2017: 374-388

[53] Wu Yang, Chen Ang, Phan Linh Thi Xuan. Zeno: diagnosing performance problems with temporal provenance//Proceedings of the 16th USENIX Symposium on Networked Systems Design and Implementation. Boston, USA. 2019: 395-420

[54] Khandelwal Anurag, Agarwal Rachit, Stoica Ion. Confluo: distributed monitoring and diagnosis stack for high-speed networks//Proceedings of the 16th USENIX Symposium on Networked Systems Design and Implementation. Boston, USA, 2019: 421-436

[55] William Aiello, John Ioannidis, Patrick D. McDaniel. Origin authentication in interdomain routing//Proceedings of the 10th ACM Conference on Computer and Communications Security. Washington, USA, 2003: 165-178

[56] Shi Xingang, Xiang Yang, Wang Zhiliang, et al. Detecting prefix hijackings in the internet with argus//Proceedings of the Internet Measurement Conference 2012. Boston, USA, 2012: 15-28

[57] Hlavaceky Tomas, Cunhaz Italo, Gilad Yossi, et al. DISCO: sidestepping RPKI's deployment barriers//Proceedings of the Network and Distributed Systems Security Symposium. San Diego, USA, 2020: 1-17

[58] Hu Yih-Chun, Perrig Adrian, Marvin A. Sirbu. SPV: secure path vector routing for securing BGP//Proceedings of the ACM SIGCOMM 2004 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication. Portland, USA, 2004: 179-192

[59] Stephen T. Kent, Charles Lynn, Karen Seo. Secure border gateway protocol (S-BGP). IEEE Journal on Selected Areas in Communications, 2000, 18(4): 582-592

[60] White Russ. Securing BGP through secure origin BGP. Business Communications Review, 2003, 33(5): 15-22

[61] Wan Tao, Kranakis Evangelos, Oorschot Paul C. van. Pretty secure BGP (psBGP)//Proceedings of the Network and Distributed System Security Symposium. San Diego, USA, 2005: 1-16

[62] Goodell Geoffrey, Aiello William, Griffin Timothy, et al. Working around BGP: an incremental approach to improving security and accuracy of interdomain routing//Proceedings of the Network and Distributed System Security Symposium. San Diego, USA, 2003: 1-11

[63] Lepinski M, Sriram K. BGPsec protocol specification. RFC 8205, 2017. https://doi.org/10.17487/RFC8205

[64] Cohen Avichai, Gilad Yossi, Herzberg Amir, et al. Jumpstarting BGP security with path-end validation//Proceedings of the ACM SIGCOMM 2016 Conference. Florianopolis, Brazil, 2016: 342-355

[65] Azimov A, Bogomazov E, Bush R, et al. Route leak detection and filtering using roles in update and open messages, 2018. https://tools.ietf.org/id/draft-ymbk-idr-bgp-eotr-policy-02.html

[66] Sriram K, Montgomery D, Dickson B, et al. Methods for Detection and Mitigation of BGP Route Leaks, 2018. https://sandbox.ietf.org/doc/draft-ietf-idr-route-leak-detection-mitigation

[67] Lakshminarayanan Subramanian, Volker Roth, Ion Stoica, et al. Listen and whisper: security mechanisms for BGP//Proceedings of the 1st Symposium on Networked Systems Design and Implementation. San Francisco, USA, 2004: 127-140

[68] John P. John, Ethan Katz-Bassett, Arvind Krishnamurthy, et al. Consensus routing: the internet as a distributed system// Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation. San Francisco, USA, 2008: 351-364

[69] Haeberlen Andreas, Avramopoulos Ioannis C., Rexford Jennifer, et al. NetReview: detecting when interdomain routing goes wrong//Proceedings of the 6th USENIX Symposium on Networked Systems Design and Implementation. Boston, USA. 2009: 437-452

[70] Li Qi, Xu Mingwei, Wu Jianping, et al. Enhancing the trust of

internet routing with lightweight route attestation//Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. Hong Kong, China, 2011: 1-10

[71] Godfrey Brighten, Ganichev Igor, Shenker Scott, at al. Pathlet routing//Proceedings of the ACM SIGCOMM 2009 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications. Barcelona, Spain, 2009: 111-122

[72] Zhang Xin, Hsiao Hsu-Chun, Hasker Geoffrey, et al. SCION: scalability, control, and isolation on next-generation network// Proceedings of the 32nd IEEE Symposium on Security and Privacy. Berkeley, USA, 2011: 212-227

[73] Hari A, Lakshman TV. The internet blockchain: a distributed, tamper-resistant transaction framework for the internet//Proceedings of the 15th ACM Workshop on Hot Topics in Networks. Atlanta, USA, 2016: 204-210

[74] Wang Frank, Ko Ronny, Mickens James. Riverbed: enforcing user-defined privacy constraints in distributed web services// Proceedings of the 16th USENIX Symposium on Networked Systems Design and Implementation. Boston, USA, 2019: 615-629

[75] Hu Yuncong, Kumar Sam, Popa Raluca Ada. Ghostor: toward a secure data-sharing system from decentralized trust//Proceedings of the 17th USENIX Symposium on Networked Systems Design and Implementation. Santa Clara, USA, 2020: 851-877

[76] Nguyen Dang Tu, Song Chengyu, Qian Zhiyun, et al. IotSan: fortifying the safety of IoT systems//Proceedings of the 14th International Conference on emerging Networking Experiments and Technologies. Heraklion, Greece, 2018: 191-203

[77] Celik Z. Berkay, Tan Gang, McDaniel Patrick. IOTGUARD: dynamic enforcement of security and safety policy in commodity IoT//Proceedings of the Network and Distributed Systems Security Symposium 2019. San Diego, USA, 2019: 61-66

[78] Lorenz Breidenbach, Philip Daian, Florian Tramèr, et al. Towards principled bug bounties and exploit-resistant smart contracts//Proceedings of the 27th USENIX Security Symposium. Baltimore, USA, 2018: 1335-1352

[79] Wu Bo, Xu Ke, Li Qi, et al. SmartCrowd: decentralized and automated incentives for distributed IoT system detection// Proceedings of the 39th IEEE International Conference on Distributed Computing Systems. Texas, USA, 2019: 387-398

[80] Wu Bo, Li Qi, Xu Ke, at al. SmartRetro: blockchain-based incentives for distributed IoT retrospective detection// Proceedings of the 15th IEEE International Conference on Mobile Ad Hoc and Sensor Systems. Chengdu, China, 2018: 308-316

[81] Basin David A., Cremers Cas, Kim Tiffany Hyun-Jin, et al. Design, analysis, and implementation of arpki: An attack-resilient public-key infrastructure. IEEE Transactions on Dependable and Secure Computing, 2018, 15(3): 393-408

[82] Matsumoto Stephanos, Reischuk Raphael M.. IKP: turning a PKI around with decentralized automated incentives//Proceedings of the 2017 IEEE Symposium on Security and Privacy. San Jose, USA, 2017: 410-426

[83] Chen Jing, Yao Shixiong, Yuan Quan, et al. Certchain: public and efficient certificate audit based on blockchain for TLS connections//Proceedings of the 2018 IEEE Conference on Computer Communications. Honolulu, USA, 2018: 2060-2068

[84] Dykcik Lukasz, Chuat Laurent, Szalachowski Pawel, et al. BlockPKI: an automated, resilient, and transparent public-key infrastructure//Proceedings of the 2018 IEEE International Conference on Data Mining Workshops. Singapore, 2018: 105-114

[85] Han Dongsu, Anand Ashok, Dogar Fahad R., et al. XIA: efficient support for evolvable internetworking//Proceedings of the 9th USENIX Symposium on Networked Systems Design and Implementation. San Jose, USA, 2012: 309-322

[86] Raychaudhuri Dipankar, Nagaraja Kiran, Arun Venkataramani. MobilityFirst: a robust and trustworthy mobility-centric architecture for the future internet. Mobile Computing and Communications Review, 2012, 16(3): 2-13

[87] Zhang Lixia, Afanasyev Alexander, Burke Jeff, et al. Named data networking. ACM SIGCOMM Computer Communication Review, 2014, 44(3): 66-73

[88] Matsumoto Stephanos, Reischuk Raphael M., Szalachowski Pawel, et al. Authentication challenges in a global environment. ACM Transactions on Privacy and Security, 2017, 20(1): 1-34

[89] Zave Pamela, Rexford Jennifer. The compositional architecture of the internet. Communications of the ACM, 2019, 62(3): 78-87

[90] Hu Yuxiang, Yi Peng, Sun Penghao, Wu Jiangxing. Research on the full-dimensional defined polymorphic smart network. Journal on Communications, 2019, 40(8): 1-12 (in Chinese)
(胡宇翔, 伊鹏, 孙鹏浩, 邬江兴.全维可定义的多模态智慧网络体系研究. 通信学报, 2019, 40(8): 1-12)

[91] Wu Jianping, Ren Gang, Li Xing. Source address validation: architecture and protocol design//Proceedings of the IEEE International Conference on Network Protocols. Beijing, China. 2007: 276-283

[92] Jia Yihao, Ren Gang, Liu Ying. Review of internet inter-domain IP source address validation technology. Journal of Software, 2018, 29(01): 176-195 (in Chinese)
(贾溢豪, 任罡, 刘莹.互联网自治域间 IP 源地址验证技术综述.软件学报, 2018, 29(01): 176-195)

[93] Lepinski M., Kent S.. An infrastructure to support secure internet routing. RFC 6480, 2012. https://doi.org/10.17487/RFC6480

[94] Kihong Park, Heejo Lee. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets//Proceedings of the ACM SIGCOMM 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication. San Diego, USA. 2001: 15-26

[95] Zhu Liang, Xu Ke. A general framework of internet address mechanisms．Journal of Xi'an Jiaotong University, 2017, 51(2): 8-16 (in Chinese)
(朱亮, 徐恪.互联网通用地址体系框架.西安交通大学学报, 2017, 51(2): 8-16)

[96] Zhu Liang, Xu Ke, Xu Lei. A formal general framework of internet address mechanisms. Journal of Computer Research and Development, 2017, 54(05): 940-951 (in Chinese)
(朱亮, 徐恪, 徐磊.一种形式化的互联网地址机制通用框架. 计算机研究与发展, 2017, 54(05): 940-951)

[97] Zhu Liang，Xu Ke，Feng Mei. A dynamic service of internet naming and resolving. Acta Electronica Sinica. 2018, 46(05): 1089-1094 (in Chinese)
(朱亮, 徐恪, 冯梅.互联网动态地址命名与解析服务.电子学报, 2018, 46(05): 1089-1094)

[98] Forssell Henrik, Thobaben Ragnar, Al-Zubaidy Hussein, et al. Physical layer authentication in mission-critical mtc networks: a security and delay performance analysis. IEEE Journal on Selected Areas in Communications, 2019, 37(4): 795-808

[99] Savage Stefan, Wetherall David, Karlin Anna R., et al. Network support for IP traceback. IEEE/ACM Transactions on Networking, 2001, 9(3): 226–237

[100] Wu Bo, Xu Ke, Li Qi, et al. Robust and lightweight fault localization//Proceedings of the IEEE International Performance Computing and Communications Conference. San Diego, USA, 2017: 1-8

[101] Zhao Meiyuan, Smith Sean W., Nicol David M. Aggregated path authentication for efficient BGP security//Proceedings of the 12th ACM Conference on Computer and Communications Security. Alexandria, USA, 2005: 128-138

[102] Butler Kevin R. B., McDaniel Patrick D., Aiello William. Optimizing BGP security by exploiting path stability// Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria, USA, 2006: 298-310

[103] Li Qi, Liu Jiajia, Hu Yih-Chun, et al. BGP with BGPsec: attacks and countermeasures. IEEE Network, 2019, 33(4): 194-200

[104] Sriram K, Montgomery D, McPherson D, et al. Problem definition and classification of BGP route leaks. RFC 7908, 2016. https://doi.org/10.17487/RFC7908

[105] Kushman Nate, Kandula Srikanth, Katabi Dina, et al. R-BGP: staying connected in a connected world//Proceedings of the 4th USENIX Symposium on Networked Systems Design and Implementation. Cambridge, USA, 2007: 341-354

[106] Xing Qianqian, Wang Baosheng, Wang Xiaofeng. BGPCoin: A trustworthy blockchain-based resource management solution for BGP security//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Dallas, USA, 2017: 2591-2593

[107] Smith Jared M., Schuchard Max. Routing around congestion: defeating DDoS attacks and adverse network conditions via reactive BGP routing//Proceedings of the 2018 IEEE Symposium on Security and Privacy. San Francisco, USA, 2018: 599-617

[108] Hedin Daniel, Sabelfeld Andrei. A perspective on information-flow control. Software Safety and Security, 2012, 33: 319-347

[109] He Weijia, Golla Maximilian, Padhi Roshni, et al. Rethinking access control and authentication for the home internet of things//Proceedings of the 27th USENIX Security Symposium. Baltimore, USA, 2018: 255-272

[110] Lu Kangjie, Nurnberger Stefan, Backes Michael, et al. How to make aslr win the clone wars: runtime re-randomization// Network and Distributed Systems Security Symposium 2016. San Diego, USA, 2016: 1-15

[111] Somé Dolière Francis. EmPoWeb: empowering web applications with browser extensions//Proceedings of the 40th IEEE Symposium on Security and Privacy. San Francisco, USA, 2019: 227-245

[112] Zhao Guodong, Xu Ke, Xu Lei, et al. Detecting apt malware infections based on malicious dns and traffic analysis. IEEE Access, 2015, 3: 1132-1142

[113] Xu Ke, Wu Bo, Shen Meng. Blockchain: a new vision for iot security. ZTE Technology Journal, 2018, 24(6): 52-55 (in Chinese)
(徐恪, 吴波, 沈蒙. 区块链：描绘物联网安全新愿景. 中兴通讯, 2018, 24(6): 52-55)

[114] Henry Birge-Lee, Sun Yixin, Edmundson Anne, et al. Bamboozling certificate authorities with BGP//Proceedings of the 27th USENIX Security Symposium. Baltimore, USA. 2018: 833-849

[115] Arends R., Austein R., Larson M., at al. DNS security introduction and requirements. RFC 4033, 2005. https://doi.org /10.17487/RFC4033

[116] Rescorla E.. The transport layer security (TLS) protocol version 1.3. RFC 8446, 2018. https://doi.org/10.17487/RFC8446

[117] McCauley James, Harchol Yotam, Panda Aurojit, et al. Enabling a permanent revolution in internet architecture//Proceedings of the ACM Special Interest Group on Data Communication. Beijing, China, 2019: 1-14

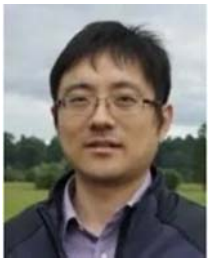
[118] Handley Mark, Paxson Vern, Kreibich Christian. Network intrusion detection: evasion, traffic normalization, and end-to-end protocol semantics//Proceedings of the 10th USENIX Security Symposium. Washington, USA, 2001: 1-17

[119] Acer Mustafa Emre, Stark Emily, Felt Adrienne Porter, et al. Where the wild warnings are: root causes of chrome https certificate errors//Proceedings of the 2017 Conference on Computer and Communications Security. Dallas, USA, 2017: 1407-1420

[120] Krombholz Katharina, Busse Karoline, Pfeffer Katharina, et al. If https were secure, I wouldn’t need 2fa-end user and administrator mental models of https//Proceedings of the 40th IEEE Symposium on Security and Privacy. San Francisco, USA, 2019: 246-263

[121] Xu Ke, Zhu Min, Lin Chuang. Internet architecture evaluation models, mechanisms and methods. Chinese Journal of Computers, 2012, 35(10): 1985-2006 (in Chinese)
(徐恪, 朱敏, 林闯.互联网体系结构评估模型、机制及方法研究综述.计算机学报, 2012, 35(10): 1985-2006)

[122] Xu Ke, Xu Song-Song, Li Qi. Decentralized trusted internet infrastructure based on blockchain. Communications of the CCF. 2020, 16(2): 29-34 (in Chinese)
(徐恪, 徐松松, 李琦. 基于区块链的去中心化可信互联网基础设施. 中国计算机学会通讯. 2020, 16(2): 29-34)



XU Ke, Ph.D., professor, Ph.D. supervisor. His research interests include next-generation Internet, Blockchain systems, Internet of Things, and network security.

FU Song-Tao, Ph.D. candidate. His research interests include Internet architecture, network security.

LI Qi, Ph.D. associate professor. His research interests include network security, privacy preserving, big data security.

LIU Bing-Yang, Ph.D. His research interests include Internet architecture, network security and trust, routing and naming resolution, deterministic network.

JIANG Wei-Yu, Ph.D. Her research interests include network security, trusted identity management, privacy and IoT security.

WU Bo, Ph.D. His research interests include Internet architecture, network security.

FENG Xue-Wei, Ph.D. candidate. His research interests include Internet architecture, network security.

Background

The traditional Internet architecture designed towards performance lacks the foundation of trust between the users and network, results serious security issues, such as Source Spoofing, DDoS attack, and Route Hijacking. With the development of the Internet, the functionality of the network extends to the automatic interaction and control under the interconnection of things, a higher requirement of network security has been brought forward. Designing architecture with intrinsic security attributes and capabilities could fundamentally improve the network security performance. The evolutionary way which aims to resolve the existing or emerging problems of the Internet, while keep the backward compatibility as well as the incremental deployment, and eventually towards a new Internet architecture, could not only achieve a stable transition but also bring innovations to meet the evolving requirements of building the Internet intrinsic security architecture.

This paper deeply studies various kinds of designs against the Internet security problems in recent years, analyzes the intrinsic security characteristics of these designs, and proposes the design idea of building intrinsic Internet security architecture. The Internet intrinsic security architecture has the “security gene”, which solves security problems without external force (security software, firewall, etc.), ensure the security of the network communication as well as the authenticity of the users. In general, the intrinsic security architecture has the two characteristics, autonomous immunity, reliable as well as controllable. It could build the trustworthiness among the terminals, infrastructure and application services, achieve the control of network basic communication units, users, and the network application services.

This work was in part supported by the National Key R&D Program of China with No. 2018YFB0803405, National Science Foundation for Distinguished Young Scholars of China with No. 61825204, National Natural Science Foundation of China with No. 61932016, No. 61802222, Beijing Outstanding Young Scientist Program with No. BJJWZYJH01201910003011 and Beijing National Research Center for Information Science and Technology (BNRist) with No. BNR2019RC01011, PCL Future Greater-Bay Area Network Facilities for Largescale Experiments and Applications (LZC0019), the project of Huawei Technology Co. Ltd. with No. HF2019015003.