未来网络可信通信技术

Trusted Communication Technologies for Future Networks

闫新成 /YAN Xincheng[1,2]
周娜 /ZHOU Na[1,2]
蒋志红 /JIANG Zhihong[2]

（1. 移动网络和移动多媒体技术国家重点实验室，中国 深圳 518057；
2. 中兴通讯股份有限公司，中国 深圳 518057）
(1. State Key Laboratory of Mobile Network and Mobile Multimedia Technology, Shenzhen 518057, China;
2. ZTE Corporation, Shenzhen 518057, China)

DOI：10.12142/ZTETJ.202105011
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20211009.1646.002.html

网络出版日期：2021–10–11
收稿日期：2021–08–26

摘要：可信通信技术是网络 5.0、6G 等未来网络的核心技术方向，也是长期困扰学术界和产业界的关键安全问题。系统分析了未来网络新架构下的可信通信需求和现有技术方案的缺陷，构造了一套可信通信技术体系，并阐述了可信通信的基本原则。在此基础上明确了两种技术防御思路，并在技术研究和产业化应用方面提出了相关建议。

关键词：未来网络；可信通信；身份假冒

Abstract: Trusted communication technology is the core technology direction of future networks such as network 5.0 and 6G. It is also a key security problem that has plagued academia and industry for a long time. The requirements of trusted communication under the new network architecture in the future and the defects of existing technical schemes are systematically analyzed. A trusted communication technology system is constructed. The basic principles of trusted communication are introduced. On this basis, two technical defense ideas are defined, and relevant suggestions are put forward in technical research and industrial application.

Keywords: future network; trusted communication; identity spoofing

互联网协议（IP）地址是当前 IP 网络体系结构的核心，拥有网络身份和路由位置两种属性 [1]。其中，网络身份属性用来标识通信对象，而路由位置属性则代表拓扑位置，是路由寻址的基础。地址欺骗可能会造成非法访问服务、分布式拒绝服务（DDoS）攻击、事件难以追溯等一系列安全问题，因而 IP 地址的安全性是构建可信任网络的基础 [2–3]。攻击者通过伪造 IP 地址来隐藏自己的真实身份，有时也会将报文引向非法位置。RFC 6959[4]（互联网工程任务组发布的征求意见稿）列举的 10 类攻击都与 IP 地址真实性相关。麻省理工学院的研究表明，互联网中至少有半数以上的网络可以产生一种类型的 IP 地址伪造攻击 [5]。据 CAIDA 的统计，互联网中平均每天有 3 万起伪造源地址的攻击事件发生 [6]。

IP 地址真实性是未来网络可信通信的核心要素，而当前传统的 IP 网络体系并不具备对 IP 地址真实性验证的内在机制。解决 IP 地址的欺骗问题，保障地址网络身份的唯一性以及路由位置的真实性，并确保 IP 地址所标识的身份和位置信息在通信过程中不被篡改和伪造，是未来网络可信通信所要解决的关键问题。

学术界对可信通信的研究相对较早。早在 2003 年，以麻省理工学院为代表的学术团体就推出了下一代互联网的新架构 NewArch[7]，明确了 IP 地址具有位置和身份的双重属性，同时强调了对 IP 地址进行安全保障的必要性。清华大学吴建平院士针对新一代互联网体系提出需要保障互联网地址身份及其位置属性真实可信的观点 [8]。

产业界近年也掀起了可信通信的热潮。国际移动通信（IMT）–2030（6G）、中国通信标准化协会（CCSA）等均开展了大量对未来网络安全方面的研究工作。中国网络 5.0 产业和技术创新联盟 [9] 更是将 IP 网络的安全体系，尤其是 IP 地址真实性保障，作为未来网络内生安全的重要目标。

当前产业界缘何要兴起可信通信的热潮？可信通信要解决什么问题？当前方案存在哪些不足，又该如何改进？针对这些问题，本文结合学术研究和产业应用，阐述和分析了可信通信的产业驱动力，提出了可信通信的必要条件和基本策略，对可信通信的主要技术方向进行了对比分析，并给出了技术应用建议。

1 未来网络可信通信需求和挑战

未来网络具备泛连接、广覆盖和

高可靠的网络能力，深度融合了 5G、云计算、边缘计算、大数据、人工智能、卫星通信等一系列新兴技术，现阶段正飞速发展，将深入经济社会各个领域，为社会带来全方位、深层次的影响，并将引领我们步入一个高度互联、内生智能、万物感知的世界。然而，未来网络在提升业务应用价值、使能社会高度信息化的同时，也为利益驱动的攻击者创造了有利条件，为其实施更大规模、更高强度的攻击提供了可能。

1.1 网络可信通信需要适应新的业务模式

新技术驱动智慧医疗、工业互联网、能源互联网、车联网、算网融合、天地一体化等多个场景持续发展与创新，并带来诸多新的业务特征。本节将重点分析这些业务特征给网络可信通信带来的需求和挑战。

• 泛在连接。网络连接模式从“人 – 人”互联向“物 – 物”互联以及“人 – 物”互联发展。泛在连接不仅包括连接数量的指数级增长和空天地海的广域覆盖，更重要的是，还包括无处不在的连接、算力的下沉和通信节点间的自主连接。车联网、传感器网络等新型业务模式，促使通信从单一客户端 / 服务器的请求服务模式向多元化的对等通信模式演变。当前服务器认证终端用户的方式不再普遍适用，可信通信架构需要进行重构。

• 网络开放。云计算、边缘计算、天地一体化都使得网络更加开放，需要在开放的物理环境下构建一个相对安全可信的逻辑网络。更重要的是，企业信息化和数字化转型打破了原有生产领域的封闭性。生产网络 IP 化、终端的智能化均使得生产领域面临域内、域间的双重威胁，因此不能仅仅关注来自办公领域的横向渗透。如何保障数字化生产领域的域内安全，构建安全可信的内部通信网络，是企业数字化转型时需要重点考虑的安全问题。

• 海量终端。未来网络不仅要提升网络覆盖的广度，还要提升覆盖的连接密度。类型多样、数量庞大的终端将使得网络的攻击面进一步扩大。尤其是低功耗、低成本的弱终端，缺乏自我防护能力，存在漏洞修复困难问题，更易于被攻击者利用或假冒。因而网络需要增强对通信终端的控制力，尤其要增强对通信节点真实性的保障。

• 算力增强。伴随着算力提升，单位时间内的数据量也将持续增长，攻击者更容易获取攻击所需的算力。网络资产（尤其是一些高价值的资产）将更容易遭受到攻击，例如卫星节点遭受 DDoS 攻击。避免算力因素对通信节点假冒攻击的放大效应，提升对通信节点真实性的保障。

未来网络的安全挑战包括两个方面：一方面，随着网络承载的资产价值增大，攻击程度在加深，风险也随之变大；另一方面，业务模型的多样化使得通信模式发生改变，通信安全架构需要进行再设计。未来网络需要进行安全设计，以便在新业务应用场景中为新型网络体系架构赋予最基础而又有效的可信通信能力，为未来业务的持续创新和广泛应用提供必要条件。

1.2 未来网络需要在网络层构建可信通信技术

在传统网络中，由于网络缺乏安全设计，通信安全问题需要由应用层来解决。例如，在对身份的真实性进行验证时，由于网络身份缺乏唯一性和确定性表达，通常由应用层对用户身份进行验证。长此以往，人们甚至会认为，安全问题应该仅由应用层来解决。然而，应用层的“补丁式”防护，不但效能低下，而且难以在未来网络的诸多新兴场景中应用。本节围绕身份真实性问题，对比分析了网络层 IP 地址真实性与应用层用户身份真实性的防护能力与效果，同时论述了在网络层构建可信通信技术的必要性。

（1）网络层的身份真实性防护机制比用户层具有更高的系统效能。

图 1 展示了一个用户访问网络的典型模型，其中图的上半部分展示的是只进行应用身份真实性防护的情况。当前，大部分应用都会在向用户提供服务之前对用户身份进行验证，因而非法用户（黑色用户图标）如果不能通过身份验证，则无法访问该应用服务。但是，对用户身份进行验证是一项很复杂的工作，中间件和操作系统层通常不具备这项能力。例如，“永恒之蓝”[10] 之所以可以广泛传播，就是因为借助了 Windows 的 445 开放端口服务。同时，应用层虽然可以阻止非法用户的访问，却难以有效防范 DDoS 攻击。

图 1 的下半部分展示的是同时进行网络层身份真实性防护的情况。如果加入基本的网络准入机制，网络就会首先拒绝非法用户（黑色用户图标）的接入，可以有效减少非法用户对应用节点和其他网络节点的攻击。虽然网络准入不能替代应用层的身份验证，却可以极大地降低应用层遭受攻击的风险。

基于应用层的用户身份真实性防护机制，只能为单个服务提供保护，无法保障整个系统的安全；而基于网络层的身份真实性防护机制，却可以提供更低风险、更“干净”的通信环境。同时，网络身份的唯一性具有不可否认属性。不论是非法用户还是合法用户，在网络攻击发生后，均可以被溯源和审计，而应用层身份不具备普遍追溯的能力。因此，网络层的身份真

实性防护至少具备两个优势：为封闭网络提供准入机制，为开放网络提供溯源能力。

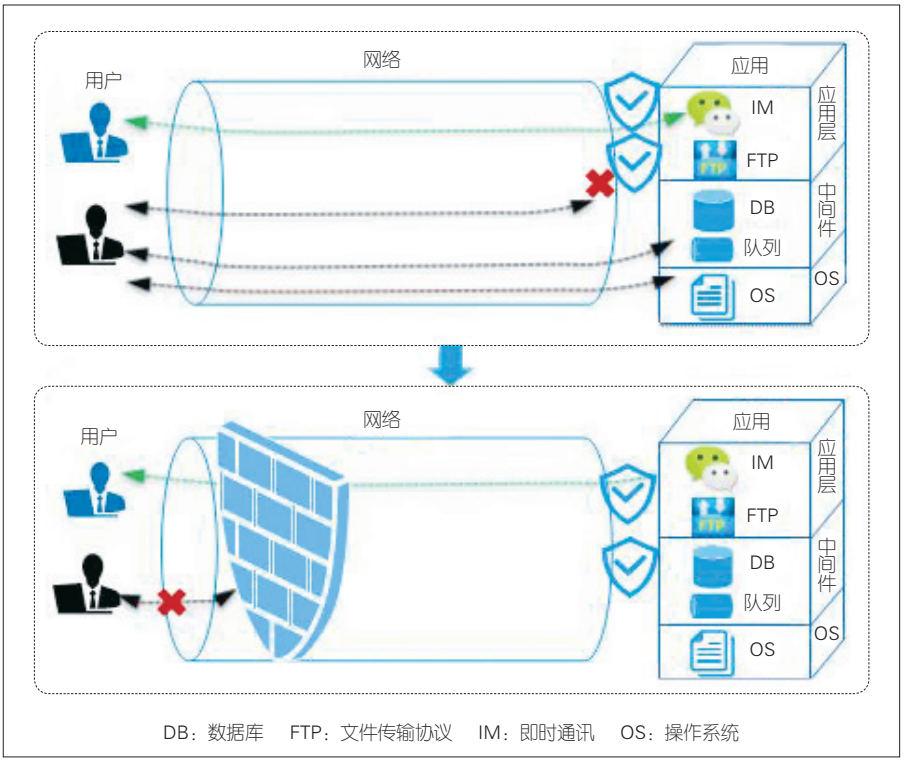
（2）应用层的用户身份真实性防护机制难以在新的业务模型和通信模式下应用。

如图 2 上半部分所示，当前的工业互联网生产线上使用了控制器局域网（CAN）、以太网控制自动化技术（EtherCAT）等各种现场总线协议。接入到总线上的各通信节点，通常属于对等通信体，即按需临时分配主从节点。对等通信模式在越来越多的领域中得到应用，例如车联网、传感器网络等。此外，这种模式在云内容器间通信、5G 服务化架构（SBA）网络中也开始应用。

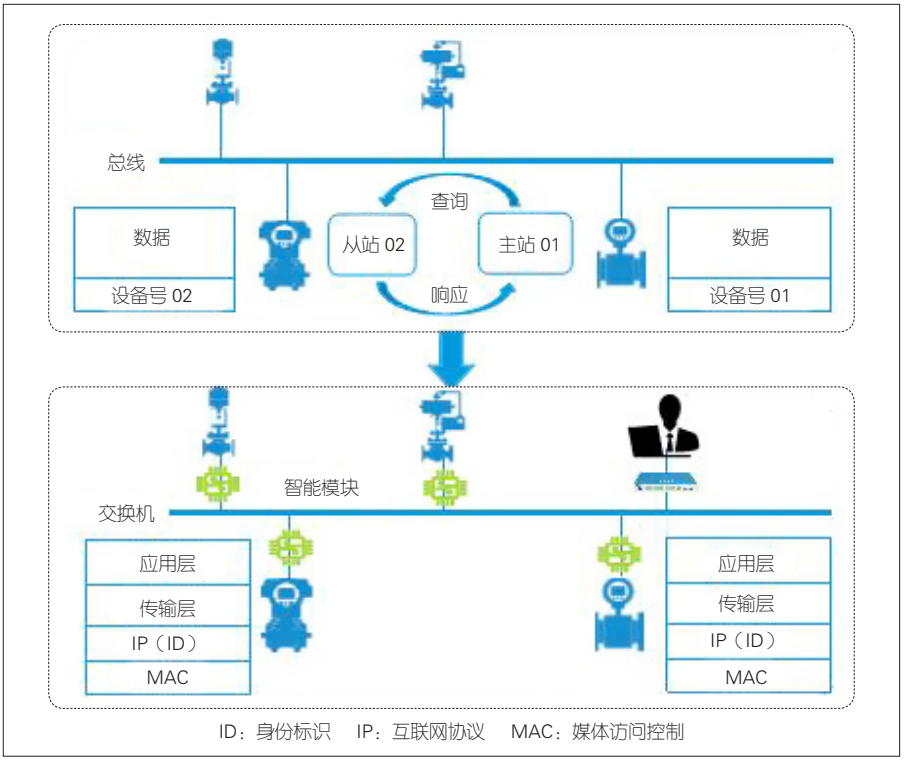
此外，工业领域也纷纷开始了网络的 IP 化改造。由图 2 可知，将总线抽象为 IP 网络交换机，对原有的业务模型和通信模式影响最小。在原有的业务模型下，工业节点可以即插即用，通信身份通常由总线进行标识。相应地，在 IP 改造后的通信模式下，新的身份通过网络来标识比通过应用来标识更具兼容性。在原有的通信模式下，工业节点可以对等访问。如果采用应用层身份来标识，就需要每个通信节点都启用应用层身份验证机制。这将大大增加系统改造的代价。

工业领域生产现场的安全性很大程度上依赖于物理隔离、技术与产业的封闭性。但在完成 IP 化改造后，网络风险将显著增大。攻击者可以利用一部手机或者其他智能终端，通过交换机或者 Wi-Fi，很容易进入现场网络，从而实施攻击。因此，生产领域的域内风险是工业数字化需要重点考虑的安全问题。在新的通信模式下，尤其是在物 – 物对等通信的场景下，基于网络层的可信通信更具兼容性和经济性，更加有利于工厂的产业数字化改造。

互联网和通信网络的高速发展，极大地提振了人们对社会信息化和数字化的信心。人们希望基于成熟的 IP



▲图 1 用户互联网场景下的防护模式对比



▲图 2 产业互联网场景下的防护模式对比

网络架构和网络生态来构建新型的基础设施，促使更多的社会资产和服务基于 IP 网络进行互联互通。由上述分析可知，网络的安全问题并不一定全都由新的业务模型和攻击手段引入。从图 2 中工业生产领域的例子可以看出，网络的开放性不仅包括基础设施共享和网络边界的模糊，还包括信息化和数字化本身。未来网络对安全的需求，从某种角度讲，不是因为网络变得复杂了，而是因为网络变得太简单了。

对于网络中新的使用者来讲，网络提供基本的安全保障和“接入即安全、通信即安全”的安全能力是生产领域快速实现数字化转型的一个必要条件。这种能力是传统网络体系所不具备的。未来网络应该构建网络的可信通信能力，帮助业务实现高效、便捷和安全的信息化和数字化改造。

2 IP 地址欺骗攻击分析

未来网络的可信通信应该首先聚焦于网络安全的原初问题，即如何解决 IP 地址的欺骗问题，以保障网络身份和位置的真实性。本节将重点分析基于身份和位置的攻击对网络的影响，以便为后续地址真实性技术方向的研究提供依据。表 1 列出了目前 IP 网络中存在的几种典型攻击，这些攻击都与 IP 地址欺骗相关[3]。其中，身份假冒和地址假冒均可单独引发 IP 地址欺骗攻击。

为了避免被溯源和审计，或者达成某些攻击目的，攻击者往往将自己的网络身份和位置进行隐藏，假冒他人身份（或在非法的位置）进行攻击。网络地址在网络系统中有身份位置合一、身份位置分离两种典型表达。当前的网络系统采用身份位置合一的方式。IP 地址兼具身份位置双重含义。在大部分情况下，攻击者对报文中的 IP 地址进行伪造，既是对身份的假冒，也是对位置的假冒。

一些改进的网络系统采用了身份和位置分离的方式。通信端的身份标识与位置标识采用不同的报文字段来表达。身份和位置可以被独立假冒和攻击：

- 身份假冒。身份假冒缺少了身份真实性保障。通信双方难以获知通信对象的真假，很容易发生会话劫持或假冒，从而导致通信数据被进一步篡改和窃取。同时身份的假冒可以使攻击者避免追溯，也可以使攻击事件被否认。因而身份的真实性是可信通信重点保障的目标。
- 位置假冒。位置真实性保障是通信中很容易被忽略的因素。如果网络只保障身份真实性，而不保障位置真实性，位置假冒的报文就仍然可以在网络中传输。这会给通信节点的可用性带来极大风险。如图 3 所示，Alice 发送报文给 Bob，报文被攻击者截获。攻击者将报文源位置标识修改为攻击对象 Charlie 的位置信息。接收者 Bob 如果只验证 Alice 身份信息而忽略其位置信息，会将应答报文回传给 Charlie，从而导致对 Charlie 的反射式攻击。

由此可见，通过单独伪造身份标识或位置标识均可以引发网络攻击。攻击者不仅可以假冒身份标识，伪造通信方身份并发送非法报文，窃取、伪造和破坏通信数据，还可以假冒和篡改位置标识信息，破坏网络服务。很显然，身份和位置两者同时被假冒的情形，也同样能够引发上述典型攻击。为了避免身份伪造形成的多种攻击，未来网络需要同时考虑对身份与位置的保护。

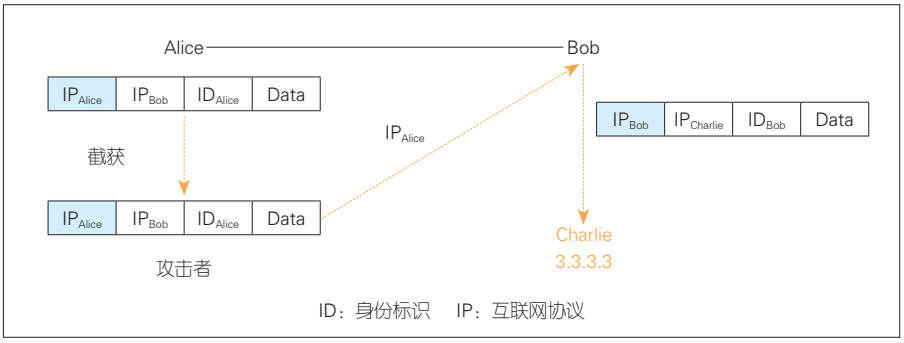
3 可信通信现有方案分析

基于 IP 地址欺骗的网络攻击给网

▼表 1 互联网协议地址欺骗攻击列表

攻击类型	攻击实例	身份假冒	位置假冒
泛洪攻击	TCP SYN Flood、TCP SYN ACK Flood、TCP ACK Flood、TCP FIN Flood、TCP RST Flood、UDP Flood、ICMP Flood、DNS Flood、ARP Flood 等	有效	–
反射攻击	Smurf 攻击、Fraggle 攻击、DNS 放大攻击等	有效	有效
中间人攻击	会话劫持等	有效	–
单包攻击	LAND 攻击、RST 探测器等	有效	有效

ACK：确认字符　FIN：结束标志　RST：复位标志　UDP：用户数据报协议
ARP：地址解析协议　ICMP：互联网控制协议　SYN：同步序列编号
DNS：域名系统　LAND：局域网拒绝服务　TCP：传输控制协议



▲图 3 位置假冒导致反射攻击的案例

络安全带来了巨大挑战。业界在不断探索针对 IP 地址欺骗的防范机制，并针对不同的防护思路推出了多种技术方案。由于 IP 地址具有位置和身份的双重含义，因此这些方案也可以分为两大技术方向：对位置的真实性防护和对身份的真实性防护。同时，网络体系本身也在演进发展。除了现有的网络体系外，还存在改良型和革新型的网络体系。这些体系对 IP 地址的真实性保障，主要体现在对身份的真实性保障上，是在新的网络体系基础上开展的。按技术方向和网络体系，表 2 给出当前典型的地址可信技术方案。

可以看出，基于位置的真实性防护主要借助路由表来实现对源地址真实性的反向验证。我们将其称之为基于位置的访问控制技术。这种方式适应性较强，可以适应于各种以 IP 路由为基础的网络体系。为了实现对身份真实性的防护，典型的方式是采用密码学技术。通过通告其他节点不可获知的私密信息（如基于密钥的签名）可证实本节点拥有的唯一身份。我们将其称为基于身份的可信验证技术。在身份真实性保障技术方案中，有基于当前 IP 体系进行增强的，也有基于身份位置分离架构设计的。革新型的网络体系方案涉及较大的体系架构调整，使之前对于 IP 地址的分析不完全适用。

表 3 给出了现有地址可信技术的对比。可以看出，虽然目前位置标识和身份标识均存在相应的防护技术，但都存在一定程度的不足。基于位置的访问控制技术虽然可以利用路由表和地址列表实现轻量化的位置真实性检查，但由于不对身份真实性进行保障，缺乏地址来源的合法性检查，并不能覆盖 IP 地址欺骗的所有场景。而基于身份的可信验证技术则普遍存在性能较低、兼容性差和不够系统化等问题，难以广泛应用。单纯的身份假冒和位置假冒都可能造成 IP 地址欺骗攻击，因而如果只保障其中一个方面，则无法有效防范所有攻击。

4 可信通信的技术体系与关键技术

互联网地址体系不具备地址真实性验证机制。网络中存在的各种 IP 地

▼表 2 地址可信技术总览

技术方向	网络体系	研究思路	技术方案
IP 网络位置真实性	IP 网络体系	现有 IP 地址保持不变，借助位置、路由等信息验证源地址真实性	SAVA[11] 和 SAVI[12]
IP 网络身份真实性	传统 IP 网络体系（地址改造）	维持现有 IP 语义不变，在地址构造中加入自验证	CGA[13] TrueIP[14]
	改良型 IP 体系（身份位置分离）	使 IP 的身份与位置属性分离，增加身份标识；IP 只标识位置，并负责路由和转发	LISP[15]
		使 IP 的身份与位置属性分离，增加身份标识的自验证机制	HIP[16] New IP[17] MobilityFirst[18]
位置和身份真实性	革新型网络体系	现有 IP 体系不再存在，使用自验证的身份标识来构造全新地址体系	AIP[19] XIA[20]

AIP：可问责互联网协议　IP：互联网协议　SAVI：源地址验证改进
CGA：加密生成地址　LISP：定位器 / 标识符分离协议　XIA：表达型互联网架构
HIP：主机标识协议　SAVA：源地址验证体系结构

▼表 3 现有地址可信技术对比分析

技术方向	网络体系	技术方案	技术手段	技术缺陷
IP 网络位置真实性：基于位置的访问控制技术	IP 网络体系	SAVA 和 SAVI	通过接入位置过滤、地址前缀过滤、自治域过滤实现源地址验证	缺乏身份真实性校验
IP 网络身份真实性：基于身份的可信验证技术	传统 IP 网络（地址改造）	CGA	用公钥的哈希作为 IP 地址的后 64 位	系统性不足，性能低
		TrueIP	用 IP 地址作为公钥	兼容性差，性能低
	改良型 IP 体系（身份位置分离）	LISP	LISP 本身没有涉及安全机制，但一些安全机制如 CGA 等可用于 LISP 架构中	安全性缺失
		HIP	使身份位置分离，增加主机标识层，以负责身份与网络、应用间映射，并将公钥作为身份标识；通过对称秘钥对数据报文进行源身份验证	兼容性差，系统性不足
		New IP	使身份位置分离，采用临时标识符进行身份隐藏；接入路由器采用非对称密钥验证源主机身份，域间采用对称秘钥进行验证	兼容性差，性能低
		MobilityFirst	在名称 /GUID/NA 标识中，GUID 采用公钥哈希	性能低
位置和身份真实性	革新型网络体系	AIP	地址结构为 AD:EID，其中 AD 与 EID 分别为责任域和主机对应的公钥	兼容性差
		XIA	基于 AIP 的思想，加入有向无环图机制	兼容性差

AD：责任域　HIP：主机标识协议　SAVA：源地址验证体系结构
AIP：可问责互联网协议　IP：互联网协议　SAVI：源地址验证改进
CGA：加密生成地址　LISP：定位器 / 标识符分离协议　XIA：表达型互联网架构
EID：端点标识符　MAC：媒体访问控制
GUID：通用唯一识别码　NA：网络地址

址欺骗的攻击给互联网环境造成了极大危害。解决身份真实性问题是构建真实可信的互联网环境的基础和前提。在当前 IP 同时包含身份与位置属性的场景下，对身份的攻击往往从地址攻击中表现出来。在未来身份与位置分离的情况下，对身份的攻击可以表现为身份标识的欺骗和位置标识的欺骗。现有技术虽然针对身份标识和位置标识都采取了一定程度的保护机制，但并未彻底解决问题。

图 4 给出了可信通信的问题与技术路线。从互联网可信通信的安全问题、技术需求、防范机制来看，可信通信包含身份保护和位置保护两大技术路线。这两条技术路线同时又存在各自的技术缺陷。

4.1 技术体系和原则

如果要实现广泛应用，可信通信的技术方案应该是一套健全、完善的解决方案。该方案不仅能在网络标识保护过程中融入真实性保障，还可满足高性能系统需求。从目前的技术方案来看，这仍是一个长期而艰巨的挑战。基于对可信通信技术需求和方案的分析，我们先给出未来网络可信通信的基本原则。

（1）可信通信有两个需求维度：身份真实性与位置真实性。这两个需求维度需要被同时满足，即无论采取何种技术方案，都需要对身份和位置同时进行防护。遗漏任何一项都会造成技术方案的不足。

（2）可信通信有两类典型的技术方向：访问控制和密码学。两类技术与身份、位置等网络特性结合，各具优势。综合考虑性能、安全性、兼容性等因素，选择若干技术进行组合，可以有效地实现网络的可信通信。

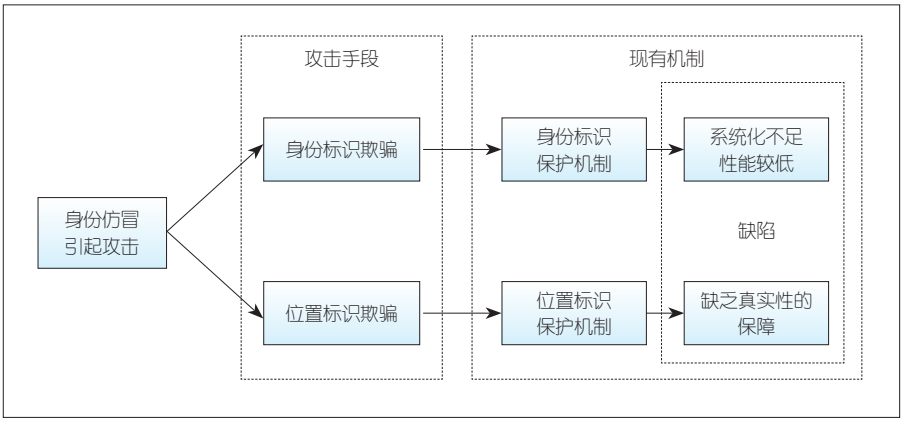
图 5 给出了基于这一原则的可信通信矩阵。为了给未来网络提供完整而又全面的保护，需要同时从身份和位置层面来考虑访问控制可信技术及密码学验证机制，以满足全方位安全可信保障需求。然而，当前的可信通信方案侧重于对位置的访问控制和对身份的密码学验证两个技术领域，忽略了对另外两个技术领域的探索。基于访问控制的身份验证技术，在与当前基于访问控制的位置验证技术结合后，既可以弥补当前访问控制技术的不足，又可以在一定程度替代基于密码学的身份验证技术。

4.2 访问控制技术

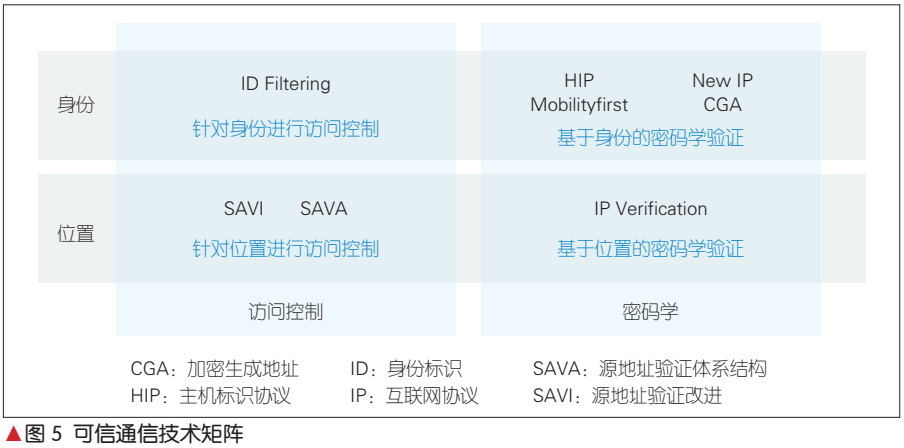
通过检查并过滤 IP 报文的源位置标识或者源身份标识，基于访问控制的可信技术可以阻止携带假标识的非法报文通过。整个基于访问控制的可信技术体系包含三层技术框架：接入网控制、域内网络控制和域间网络控制。构建多层、系统化的身份可信体系可以保障整个业务通信过程的合法性。

• 接入网验证可通过深度融合身份认证与地址分配功能，基于动态主机配置协议（DHCP）Snooping 等来构建源信息合法性校验机制（ID Filtering），并增强接入设备中过滤表的真实有效性，以实现近源端防御，进而在数据报文的首跳节点扼制攻击的形成与传播。借助高可信的身份认证和轻量级的访问控制技术，可以实现身份和位置的双重保护。提供高效的源节点真实性验证机制可以解决现有技术中低性能和真实性缺失的问题。

• 域内验证采用地址过滤表方式。在同一管理域下的路由设备，可在设备上构建过滤表，并将路由前缀与设



▲图 4 可信通信的问题与技术路线



▲图 5 可信通信技术矩阵

备的入端口进行关联。源域的边缘路由器可以通过该过滤表对收到的报文进行前缀验证，从而防止主机假冒任意地址。域内验证与接入网验证结合能够实现完整的域内可信防护机制。

• 域间验证可以通过在边界路由器上构建一个验证规则表，将路由器的每个入口与一组有效的源地址块或者域信息相关联，以用于过滤伪造的报文。

4.3 密码学验证技术

针对身份与位置的密码学验证技术主要包括基于对称密钥的验证技术和基于非对称密钥的验证技术。

（1）对称密钥方案

在基于对称密钥进行验证的方案中，通信双方通过密钥协商或预共享的方式生成系统的共享密钥。源端使用共享密钥生成验证码，同时验证端使用共享密钥验证源端身份。将对称密钥验证方案应用于端到端系统的多点验证时，借助报文路径上多个节点与源节点协商生成的对称秘钥，源主机在发送报文前会针对身份或位置产生校验码，在报文到达中间节点时对身份、位置进行可信验证。该方案无须改变 TCP/IP，与现有系统兼容，可以从不同层面增强系统的防御控制能力。首先，该方案可通过源域节点实现对源端的验证，并通过目的域对源端进行校验，可以全方位提供报文来源真实性保障；其次，该方案不仅对身份标识进行验证，还考虑了基于位置的密码学防护（IP Verification），从验证对象层面改善现有技术的不足，实现了最终应用或业务的全面保护。

（2）非对称密钥方案

基于非对称密钥的验证技术利用公私钥管理技术，在转发面上通过私钥进行签名，同时通过公钥进行验签。该方案主要包括两类分支：基于数字证书机制和基于自认证的密钥管理机制。类似于对称密钥方案，非对称密钥方案也拥有实现全系统的多点验证机制。该方案在报文中添加针对身份或位置的签名信息，由报文途经的多个节点对报文的发起端依次进行身份、位置验证，最终可实现近源防护、目的节点保护等多重安全保障，具备较好的系统性防御效果。

4.4 技术对比分析

一种理想的身份可信技术方案应尽可能优化以下几个特性。

（1）身份或位置欺骗防御能力：鉴别伪造身份 / 位置（前缀）的能力，包括准确性、实时性等（还应结合追溯定位技术为审计追查提供基础）。

（2）可部署性：针对当前网络基础设施应具备良好的兼容性，支持增量部署，为运营商提供部署激励。

（3）开销：包括方案的存储开销、计算开销、带宽开销等，也包括对网络性能造成的影响。

根据以上 3 个特性，我们对“基于访问控制的可信”和“基于密码学的验证”两种攻击防御技术方案进行对比，如表 4 所示。

在身份攻击的防御能力方面，方案 1 从接入网、边界、域间 3 个层面分别对源地址、地址前缀、域 3 个粒度进行访问控制，粒度相对较粗，在某些情况下存在一些防御难题（如业务面地址的真实性不足等）；而方案 2 是一种直接确认源主机位置 / 身份标识所有权的方法，真实性程度高，防御准确性好。方案 1 和方案 2 都可部署在第 1 跳接入路由器上，进行近源防护，实时性基本相同。方案 1 根据位置进行追踪，在移动性及多宿主的场景下，无法直接定位身份；而方案 2 可依赖密钥来关联信息，进而直接定位身份，追溯性较好。

从可部署性方面看，方案 1 无需扩展协议，只需对交换机、路由器进行少量软件升级即可；而方案 2 需要扩展地址和路由协议以及密码体系的支持，实际部署难度大。

从开销上看，方案 1 需要在接入和边界路由器上建立过滤规则表，并依据源报文中的字段进行过滤，不在源报文中增加新的字段，也不涉及复杂的运算，故开销较小；而方案 2 需要进行密钥管理，不仅要在报文中增加签名或校验码，还要在验证节点上进行加解密的运算，故系统开销较大。

总体来说，基于密码学验证机制的方案安全能力好，但部署难度和开销都较大；基于访问控制的方案可部署性好，开销也较小，但安全能力相对较弱。就目前来看，很少有哪一种方案或技术能够在各个方面都做得很优秀。安全能力与部署能力的矛盾始终是一个巨大的挑战。

5 技术应用建议

针对上文提出的技术原则和技术方向，基于访问控制和密码学验证两类技术的分析和比对，两类技术方向各有优劣，适用于不同场景。未来网络需要面临多样化的应用场景，不仅需要满足高带宽、超高吞吐、超低时

▼表 4 攻击防御技术对比分析

技术方案	防御能力			易部署性	资源开销		
	准确性	实时性	可追溯性	协议兼容性	计算开销	存储开销	带宽开销
方案 1：访问控制技术	较好	好	较差	较好	小	小	小
方案 2：密码学验证技术	好	好	好	较差	大	较大	较大

延的网络需求，还要考虑海量资源受限的弱终端接入。未来网络可信通信需要具备高效轻量化的可信验证和转发机制。但由于未来网络承载着高资产价值，因此也需要考虑高安全性的需求。本文中，我们在如下几个方面提出建议：

• 性能是未来网络大部分应用场景优先考虑的因素。优先选择深度融合身份认证与地址分配的基于访问控制技术，可以兼顾防御能力、易部署性和性能。

• 为了实现业务端到端安全可信通信，基于访问控制的可信技术往往需要实现全系统部署。因此，当应用场景需要全网进行防护但无法整网全面部署时，或者需要高级别安全保障时，可考虑基于密码学的验证机制。

• 对于基于密码学的两大类机制（非对称和对称方案），虽然对称算法需要借助控制面体系来辅助完成数据面的安全标识和密钥传递，但在路由转发层面的验证性能优势显著。结合网络安全策略的按需检验机制，可以构建灵活高效验证转发能力的通信体系，满足未来网络高吞吐高效传输演进需求。因此，对于基于密码学的验证机制而言，对称算法的方案更值得推荐。

• 基于访问控制的可信技术从是否属于该网络的合法信息方面来进行判断和控制。基于密码学的验证机制从身份真实性角度来判断和保障。两类技术方向分别解决不同场景的攻击问题。在需要系统性高级别安全保障的情形中，两类机制的融合可以实现全方位、全系统的安全防护。

6 结束语

未来网络可信通信技术通过在IP网络中构建可信的网络标识，建立以网络为核心的端到端的可信关系，实现了域内域间的信任传递，不仅能确保网络标识可验证、可追溯、不可篡改，还可有效提升网络身份在端到端通信中的真实性交互能力，充分保障了业务和应用未来的持续发展。本文中，我们在全面分析身份假冒诱发成因及其形成的若干典型安全攻击的基础上，针对现有可信通信技术系统性的不足，从身份标识和位置标识的角度，结合不同技术方向的维度，深入分析了各技术方向的适应性，为未来网络架构的设计提出安全可信防护建议。

致谢

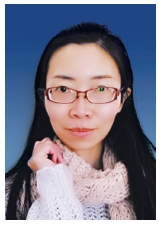
本研究得到中兴通讯股份有限公司谭斌、王继刚、黄兵、周继华、马彧、吴华强、彭少富等专家的帮助，谨致谢意！

参考文献

[1] WANG J H, WANG Y, XU M W, et al. Separating identifier from locator with extended DNS [C]//2012 IEEE International Conference on Communications (ICC). Ottawa, ON, Canada: IEEE, 2012: 2747–2751. DOI:10.1109/icc.2012.6363725
[2] 闫新成，毛玉欣，赵红勋 . 5G 典型应用场景安全需求及安全防护对策 [J]. 中兴通讯技术，2019, 25(4): 6–13. DOI: 10.12142/ZTETJ.201904002
[3] 徐恪，朱亮，朱敏 . 互联网地址安全体系与关键技术 [J]. 软件学报，2014, 25(1): 78–97. DOI:10.13328/j.cnki.jos.004509
[4] MCPHERSON D, BAKER F, HALPERN J. Source address validation improvement (SAVI) threat scope [R]. 2013
[5] CAIDA. State of IP spoofing [EB/OL]. [2021–07–16]. http://spoofer.cmand.org/summary.php
[6] CAIDA. CAIDA’s annual report for 2018 [EB/OL]. (2019–03–20)[2021–07–16]. https://www.caida.org/about/annualreports/2018/
[7] USC/ISI, MIT LCS, ICSI. NewArch project: future–generation Internet architecture [EB/OL]. [2021–07–16]. http://www.isi.edu/newarch/
[8] WU J, WU Q, XU K. Research and exploration of next–generation Internet architecture [J]. Chinese journal of computers, 2008, 31(9): 1536–1548. DOI: 10.3724/SP.J.1016.2008.01536
[9] 网络 5.0 产业和技术创新联盟 . 下一代泛在全场景 IP 协议 [EB/OL]. [2021–07–16]. http://www.network5.cn/
[10] Baidu. WannaCry [EB/OL]. [2021–07–16] https://baike.baidu.com/item/WannaCry/20797421?–fr=aladdin
[11] WU J, BI J, LI X, et al. A source address validation architecture (SAVA) testbed and deployment experience [R]. 2008
[12] NORDMARK E, BAGNULO M, LEVY–ABEGNOLI E. FCFS SAVI: first–come, first–served source address validation improvement for locally assigned IPv6 addresses [R]. 2012
[13] AURA T. Cryptographically generated addresses (CGA) [C]//Information Security, 6th International Conference. Bristol, UK: IETF, 2005
[14] SCHRIDDE C, SMITH M, FREISLEBEN B. True–IP: prevention of IP spoofing attacks using identity–based cryptography [C]//Proceedings of the 2nd international conference on Security of information and networks. North Cyprus, Turkey: ACM, 2009. DOI:10.1145/1626195.1626229
[15] FARINACCI D, FULLER V, MEYER D, et al. The Locator/ID Separation Protocol (LISP) [R]. 2013
[16] IETF. Host identity protocol [EB/OL]. [2021–07–16]. https://www.rfc–editor.org/rfc/rfc5201
[17] 网络 5.0 产业和技术创新联盟 . 网络 5.0 技术白皮书 [R]. 2019
[18] RAYCHAUDHURI D, NAGARAJA K, VENKATARAMANI A. MobilityFirst [J]. ACM SIGMOBILE mobile computing and communications review, 2012, 16(3): 2–13. DOI:10.1145/2412096.2412098
[19] ANDERSEN D G, BALAKRISHNAN H, FEAMSTER N, et al. Accountable Internet protocol (aip) [C]//Proceedings of the ACM SIGCOMM 2008 conference on Data communication. Seattle, WA, USA: ACM, 2008: 339–350. DOI:10.1145/1402958.1402997
[20] HAN D, ANAND A, DOGAR F, et al. XIA: efficient support for evolvable Internetworking [C]//The 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI’12). San Jose, CA, USA: ACM, 2012

作 者 简 介

闫新成，中兴通讯股份有限公司网络安全首席系统架构专家、移动网络与移动多媒体技术国家重点实验室未来网络研究中心副主任，教授级高工；从事电信行业 20 年，曾主持国家科技重大专项 5G 安全课题，获得多项科技奖励，拥有专利 40 余项。



周娜，中兴通讯股份有限公司技术预研系统工程师；主要负责网络安全、无线通信安全和未来网络安全等技术研究工作。

蒋志红，中兴通讯股份有限公司技术预研系统工程师；主要研究方向为网络安全、5G 通信安全和未来网络可信通信。