未来网络内生安全通信技术

Intrinsic Security Technology for Future Network

闫新成/YAN Xincheng[1,2]，周娜/ZHOU Na[1,2]，
蒋志红/JIANG Zhihong[1,2]
（1. 移动网络和移动多媒体技术国家重点实验室，中国 深圳 518055；
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, Shenzhen 518055, China;
2. ZTE Corporation, Shenzhen 518057, China)

DOI：10.12142/ZTETJ.202301006
网络出版地址：https://kns.cnki.net/kcms/detail//34.1228.tn.20230227.0939.002.html
网络出版日期：2023-02-28
收稿日期：2022-12-23

摘要：网络安全技术是保证未来云网发展的关键技术。针对未来网络安全挑战及现有技术缺陷，提出了一种基于网络可信身份的轻量化密钥验证技术——网络可信通信（NISC）技术。该技术具备近源协同防护和无状态随路验证等特征，目前已在试验网络上验证了其防御网络攻击的有效性和可行性，可以为未来网络安全可信保障提供参考，加速未来云网安全技术研究和产业化进程。

关键词：未来网络；NISC；内生安全；主动防御

Abstract: Network security is a key technology to ensure the future cloud network. To address future network security challenges and the shortcomings of existing technologies, a lightweight key authentication mechanism based on network trusted identity – Network Trusted Communication (NISC) technology is proposed. The technology features such as near-source cooperative protection and stateless follow-the-road authentication. The effectiveness and feasibility of its defense against network attacks is verified on China Environment for Network Innovation (CENI) network, which can provide reference practice for future network security trustworthiness assurance and accelerate the research and industrialization process of future cloud network security technology.

Keywords: future network; NISC; intrinsic security; active defense

1 未来网络的安全挑战

网络的演进是一个开放性和动态性不断增加的过程。5G/5G-A面向医疗、交通、工业等领域，促进通信技术（CT）与信息技术（IT）/运营技术（OT）的融合；6G网络与算力融合，尝试对网络服务进行感知，实现泛在的接入和服务访问。未来的网络除了要提供更快的传输速率、更精准的服务、更智能的连接外，还需要提供更安全可信的传输能力。这就不仅需要安全适应网络，解决由开放性和灵活性所造成的安全问题[1]，还要使网络具备内生的安全能力，基于网络的新特性，更好地发挥网络的安全潜能。

1.1 安全需求

随着网络的演进和发展，融合体系、通信模式和防护主体都发生了变化，这也促使了网络安全架构的发展。

首先，新的网络融合体系对传统互联网协议（IP）安全体系提出了挑战。数字经济发展需要云边端协同的强大算力和广泛覆盖的网络连接做支撑，算网融合已成为重要趋势。算网融合衍生出新的网络结构，但角色多样泛在化、连接多变动态化、信任关系多元复杂化等特点为攻击提供了更多的条件，这会严重加剧攻击程度，因此需要人们重新审视算力网络的安全防护架构与能力[2]。由于IP缺乏安全设计，未来网络需要从架构上解决IP安全问题[3]。

其次，新的网络通信模式对以网络服务为主体的传统防护模型提出了挑战。园区生产网络采用工业总线技术，经IP化改造后，将普遍采用L2/L3层点对点（D2D）的通信模式[4-5]。由于传统的OT网络通信协议缺乏严格的权限管理和验证机制，IP化改造后基于静态配置的网络访问控制策略难以奏效，攻击者可能会假冒合法用户身份进行越权访问[6]，并利用系统漏洞发起网络攻击。现有的IT安全以保护客户端-服务端（C-S）通信模式为主，难以解决OT局域网IP化后访问不受控的问题。

最后，防护主体的变化对传统孤立的防护模式提出了挑战。协同制造使移动通信网络与先进制造技术深度融合：园区内OT设备通过多种方式混合接入企业生产制造网络，园区外不同企业间通过广域网动态构建专网进行协同生产。园区内的局域应用向广域化转变，网络风险由消费领域向产业领域持续渗透，这需要进行多信任主体间的协同防护。行业终端和边缘节点因安全能力不足，也需要端到端地设计安全

方案，提供多点多域的协同防护机制。由于网络广域互联、攻击各个层面容易扩散，海量异构节点存在安全能力差异，针对行业应用的恶意攻击也将不断增加[5]。

在网络架构融合开放的发展趋势下，传统外挂式、补丁式的被动安全防御机制已无法有效支撑未来网络安全性需求，因此需要基于网络“内生安全”的理念去解决网络安全问题[7-9]。目前业界对网络内生安全的研究主要包括网络通信的可信和网络基础设施的可信两方面。本文中的研究主要聚焦于前者，简称为可信通信，即将安全功能作为基本要素耦合到体系结构中，在不借助外力（安全软件、防火墙等）的情况下，实现对网络通信的攻击防范和内生安全保障[15]。

当前业界非常重视网络内生安全技术研究[10]：科技部专项研究《1.3 内生安全支撑的新型网络体系结构与关键技术》涵盖了网络体系结构内生安全机理、未知网络攻击免疫方法等内容；产业界也在近年来开展了IP网络内生安全的研究，网络5.0产业联盟在《网络5.0技术白皮书》[11]中提出网络需要具备可信管理、可信接入以及可信路由能力等可信通信能力，并强调了抗网络攻击的网络内生安全能力需求；全球标准组织积极研究和制定攻击防御技术相关安全标准；运营商一致认同网络安全可信的重要性，并针对攻击问题提出内生安全能力需求。

1.2 网络攻击分析

网络安全架构设计的目的是建立一个安全的网络环境，保护网络系统免受攻击。要达成网络可信通信的目标，需要先分析网络攻击。传统的IP网络体系设计以设备间通信互联为导向，难以在网络层实现针对网络攻击的检测控制。未来网的典型攻击的特征和原理分析如表1所示。

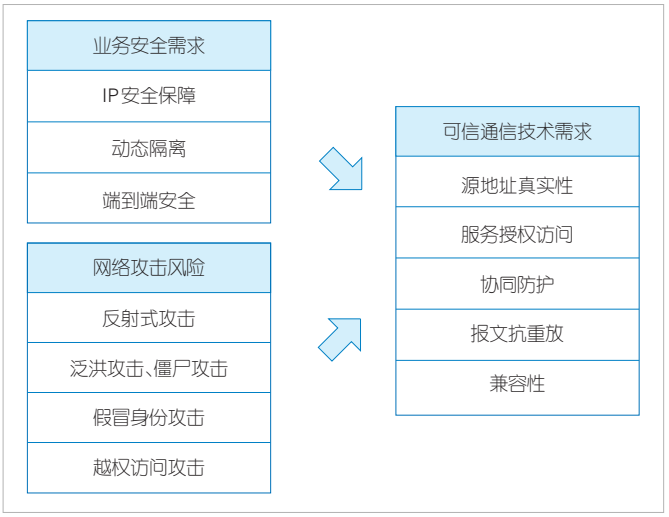
基于网络业务安全需求和所面临的攻击风险的综合分析，我们提出了未来网络可信通信技术需求，如图1所示。为及时、高效、系统地实现可信通信，需要网络尽早检查终端源地址的真实性，并有效验证终端用户访问应用的合法性，确保只有真实终端得到合法授权才能被允许访问行业应用。与此同时，还应考虑跨域场景下的协同防护机制，针对报文重放攻击的防范机制以及对传统终端和网络的兼容性方案，全方位、多角度增强系统安全可信通信能力。

2 可信通信的设计原则与技术体系

网络可信通信（NISC）体系是专门针对未来网络的关键安全需求及现有技术的缺陷而构建的。基于可信的网络架构和IP协议，NISC应具备近源协同防护、无状态随路验证等特征，无须依赖攻击先验知识，能及时、主动识别控制异常的通信数据流，减轻攻击造成的系统危害。在设计可信通信机制时，为了提供体系化的可信通信能力，应考虑具有以下特性的安全防御机制：

1）实时性：借助网络层为业务提供接入域、传输域、目的域等多点防范，尽可能实现自动化接入和靠近攻击源的防护。

2）高效性：打造高效防御阻断系统，减少业务冲击，为未来网络赋予高性价比、精准化攻击检测能力。



▲图1 未来网络可信通信技术需求

▼表1 未来网络典型攻击分析

攻击类型	典型场景	攻击特征	网络固有缺陷
反射式攻击	服务感知网络、协同制造网络	攻击者修改报文中的源地址，利用收发主机或报文数量的放大效应进行攻击	IP通信中报文发送或转发时没有检查源地址的真假
泛洪或僵尸网络攻击	服务感知网络、协同制造网络	攻击者不改源地址，借助网络分布式的特点在多点同时发送正常报文，这会造成受害者链路拥塞或处理能力不足	源主机发送报文时，无须获得接收端的允许，就可随意发送
假冒身份攻击	园区生产网络、协同制造网络	攻击者通过修改报文中的源地址，发起攻击或假冒合法用户身份	IP通信中报文发送或转发时没有检查源地址的真假
越权访问攻击	园区生产网络、协同制造网络	系统检查业务授权时存在漏洞，导致攻击者可绕过该权限检查，访问或操作原本无权访问的高权限功能	利用网络无法感知业务授权，无法进行应用层访问控制

3）系统性：面向全系统构建攻击防护方案，设计系统性的信任链传递机制，多维度、多层次、多位置提供服务节点可信可控防护机制。

基于上述设计原则，NISC技术具体应满足下列要求：

1）源地址真实性要求。针对因IP地址假冒所引发的攻击问题，需要对通信发起端的身份或标识，通过轻量化访问控制技术、密码算法技术进行真实性校验。这样能够增强网络业务通信的可信度，弥补端到端安全访问能力方面存在的不足。

2）服务授权访问要求。在地址真实性得以保障的基础上，端到端通信业务应根据业务认证与访问授权情况，借助密码学机制识别合法报文并实施服务可访问控制，确保业务获取目的端的认证和授权，从而阻止网络攻击行为的发生。

3）协同防护要求。对于通信业务经过不同信任主体的情况，可以基于密钥派生、认证信息共享等机制来实现安全域间的互信传输，并尽量在靠近报文发起源、目标域检测数据报文的合法性，保障多信任主体场景的高效攻击阻断、端到端系统性防御。

4）报文抗重放要求。系统应基于时间校验子、序列号等动态因子对重放报文进行轻量化主动识别和检查，有效避免因非法截获报文引起的重放攻击。

5）兼容性要求。可信通信技术应对传统终端、网络以及传输设备提供兼容性支持。

图2为NISC可信通信体系架构，包括控制面和转发面，分别实现网络可信身份和基于凭证的可信转发。控制面负责用户设备认证、业务授权、网络可信身份生成、可信凭证分配等管理功能，并作为通信系统信任锚点，为转发面源端身份可信检验及业务可访问控制等提供验证依据。转发面基于控制面传递的可信凭证，负责全系统通信过程中的数据随路识别、验证和控制。通过控制面和转发面的信任关联，NISC为未来网络系统安全可信通信提供了系统性保障。

1）控制面包含目标域认证服务器、授权服务器、接入认证服务器等网元：

a）目标域认证服务器由企业或目的应用方部署，对用户设备进行认证并生成验证信息，实现自动化可信企业接入认证，为用户设备安全接入企业应用提供保障。

b）授权服务器也由企业或目的应用方部署，基于细粒度的服务防控策略对成功认证的用户进行服务访问授权，并控制授权有效期，避免因永久授权造成的安全攻击隐患。

c）接入认证服务器由接入网络运营商部署，对用户设备接入网络进行认证，提供源地址真实性验证和抗重放验证依据。

2）转发面除了用户设备、应用以外，还包含接入网关、服务网关和路由器等传输节点：

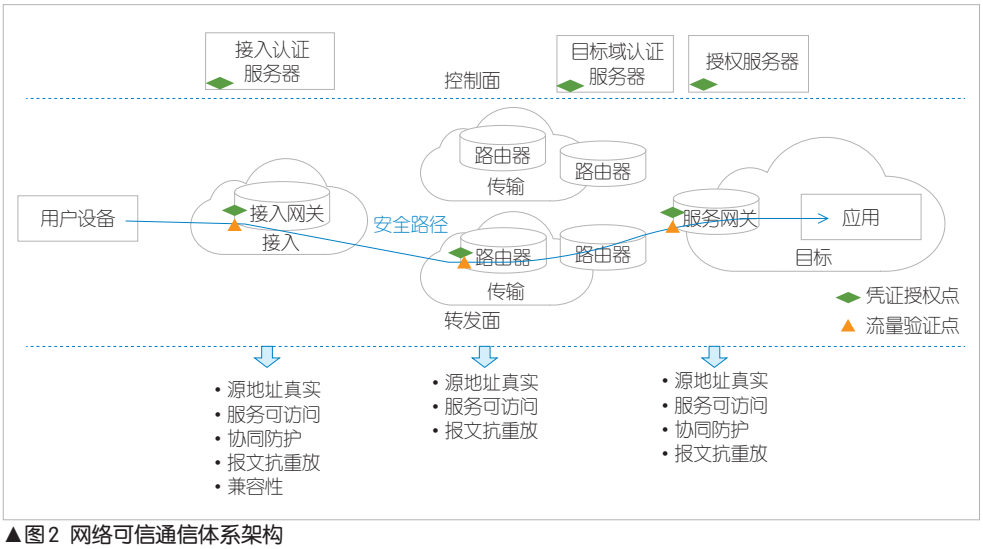
a）接入网关所涉及的功能：用户设备的地址真实性验证；按照运营商或企业需求，针对业务的可访问性执行授权、验证和控制功能；提供通信流量的抗重放验证，从近源端有效避免攻击者因非法截获或恶意构造报文所导致的重放威胁。

b）服务网关控制用户对企业的访问行为：识别并控制服务授权请求报文；按照运营商或企业需求，针对业务的可访问性执行授权、验证和控制功能。

c）路由器针对业务的可访问性实现授权、验证和控制功能：该项功能无须通信路径中所有路由器参与，需要根据业务需求、运营商需求以及网络能力在域边界路由器上部署并启动。

针对跨域通信的情况，除了在接入网关和服务网关执行数据流验证功能以外，中间域也可在其边界路由器部署、启用数据流验证功能，对域间发生的攻击场景形成安全屏障，从而减轻目的端网关处理负担。

面向业务的网络层可信通信通过终端业务身份认证、服务授权、服务访问控制机制全方位构建目标域可访问能力，利用验证信息的统一化生成、动态更新管理以及轻量化抗重



▲图2 网络可信通信体系架构

放机制，为业务访问提供高效的合法性验证依据，增强网络自身抵御攻击的能力。同时，在网络层面实现近源以及近目的的多点攻击防范，及时阻止无合法访问权限的真实地址用户非法访问业务行为，达成流量实时高效检测控制的安全防护系统。

3 可信通信关键技术

网络可信通信关键技术包括源地址真实性检查、服务动态授权机制、跨域协同防护、重放攻击主动检测、终端兼容性，如图3所示。

3.1 源地址真实性检查

传统IP网络缺乏基本的安全性设计，因此仿冒源地址引发的攻击层出不穷，而现有的可信通信技术验证开销大，保护机制不够健全，难以满足多样化应用、海量终端的泛在网络安全需求，因而需要考虑如何系统性地构建高效的业务真实源验证安全机制[12]。

作为信息隐私保护的一种典型技术，基于对称密钥的验证机制具有统一信任锚点，可以利用控制面集中生成或多方协商、派生出具有私密属性的共享密钥，具体如图4所示。统一信任锚点借助该共享密钥对需要验证的信息进行密码学运算，生成相关的通信验证凭证，再下发给报文发起端。发起端在每报文中携带通信验证凭证。收到业务报文之后，转发面验证节点基于事先获取的共享密钥和报文中待验证信息，利用与信任锚点一致的密码学算法生成通信验证凭证，以此对报文合法性进行识别和区分。相对于非对称密钥，对称密钥运算性能更好，可提供更高效的验证和控制机制。

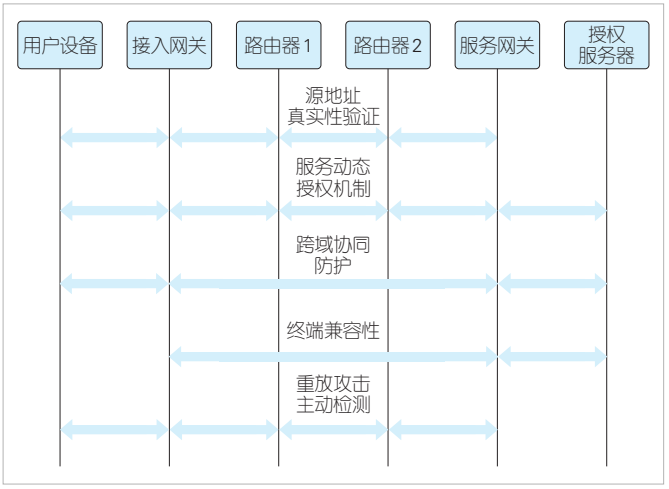
在用户设备接入网络执行认证的过程中，接入认证服务器基于该设备的标识信息（ID）对用户进行认证，采用散列消息认证码（HMAC）算法，并根据共享密钥生成验证码，之后再返回给用户设备。经过地址可信分配后，用户设备获取含有设备标识的地址信息。在业务通信过程中，每数据报文将携带验证码信息，然后由接入网关根据事先获得的共享密钥以及报文中的标识和验证码信息执行用户设备的源地址校验。

基于业务源IP的真实性控制机制提供了面向用户可信身份的认证增强、基于密码学的接入网验证技术，避免因地址假冒引发的网络攻击、信息非法获取等异常操作，实现用户接入云网系统时的轻量化实时验证和网络安全可信传输。

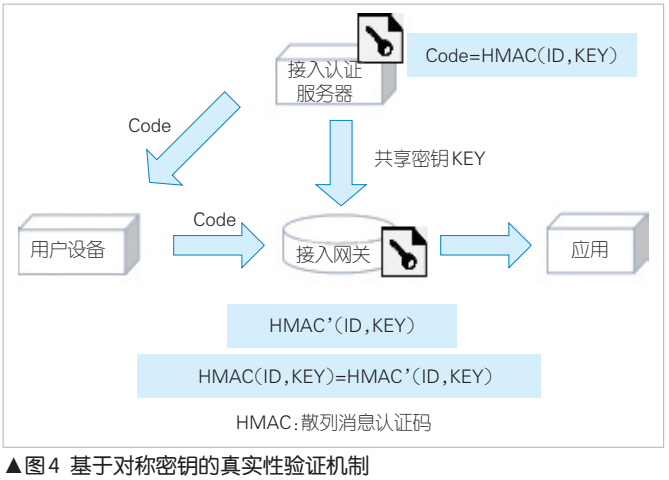
3.2 服务动态授权机制

为了及时阻止未经许可的流量恶意注入，避免非法访问对应用系统带来的不利影响，在充分保证终端用户源地址真实的同时，目标应用系统的可访问性也应得到关注。端到端通信业务中如何确保终端用户获取目的端访问授权、如何高效识别数据报文的合法与否等问题均值得深入研究[13]。

服务动态授权全方位构建了目标域鉴权、授权和网络验证机制。如图5所示，服务端基于终端的信任度、应用系统资源占用情况、应用访问控制列表等策略，对合法访问应用的终端进行动态授权，并在数据转发层面由网络节点对其业务流量进行合法性验证，及时阻止无合法访问权限的真实地址用户非法访问业务的恶意行为，实现对应用系统的有效防护。服务动态授权利用验证信息的统一化生成、一致性表达、动态更新管理机制，为用户访问业务提供高效的合法性验证依据，构建流量实时高效检测控制的安全防护系统。该机制兼具动态授权和无状态过滤的优点，既能主动防范针对主机身份的网络攻击，又能有效抵御反射性攻击、泛洪攻击和中间人攻击等各种分布式拒绝服务（DDoS）攻击，增强了系统主动抵御攻击的可信通信能力。



▲图3 网络可信通信的关键技术



▲图4 基于对称密钥的真实性验证机制

3.3 跨域协同防护

在传统防护模式中，当终端用户访问企业应用系统时，运营商网络对用户进行接入认证，并作为管道承载用户与应用间的业务认证。当运营商网络与企业应用系统处于不同信任域时，用户和接入网络、用户和应用系统分别建立信任关系，独立进行认证、授权和验证。这种基于二元信任的攻击防御模式[14]传输开销大，验证效率低。这种攻击防御架构无法尽早在接入网络对针对应用系统的攻击进行近源检测和防护，因此防护效果滞后，给应用侧的防御系统带来较大压力。

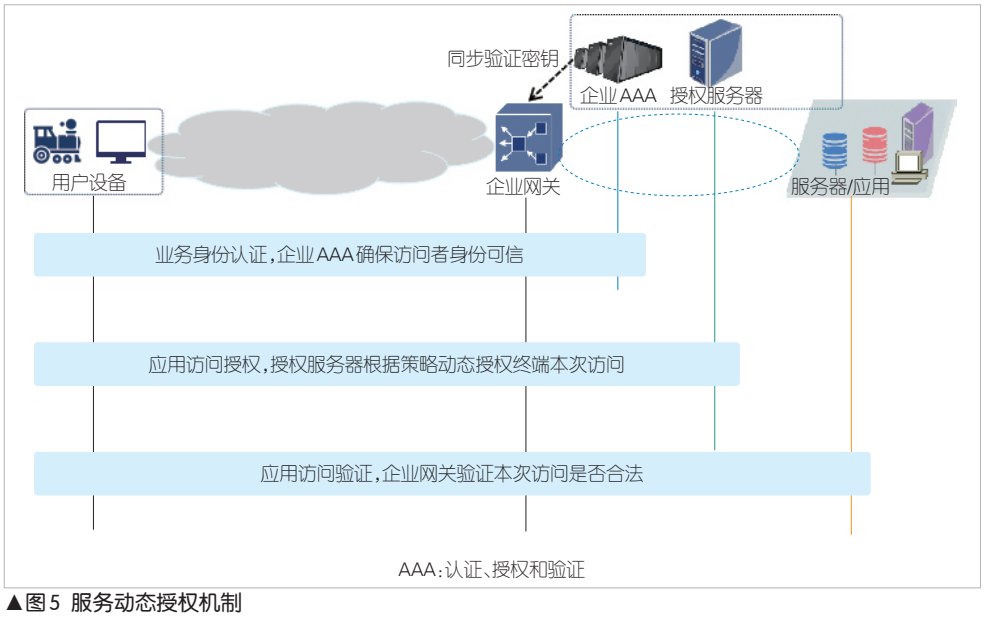
跨域协同防护机制的工作原理如图6所示。该机制通过不同信任域间的信任协商，以运营商网络为锚点派生出企业的验证密钥。以此为基础，企业网络在用户业务认证时，派生出用户的企业应用会话密钥。终端用户基于终端身份、企业身份及企业会话密钥生成验证码，并在运营商网络、企业网络中对用户访问企业应用进行多点随路验证，以从近源端抵御对企业应用的攻击。其中，密钥派生和验证码生成机制如图7所示。

协同防护方法通过在不同信任域间建立信任协同机制，共享认证结果，协商信任凭证，构建基于用户、网络和应用的跨信任域协同防护和无状态随路验证机制。一套凭证即可验证用户身份与访问合法性，实现多点验证、近源防护，提高了防护系统的实时性、高效性与系统性。

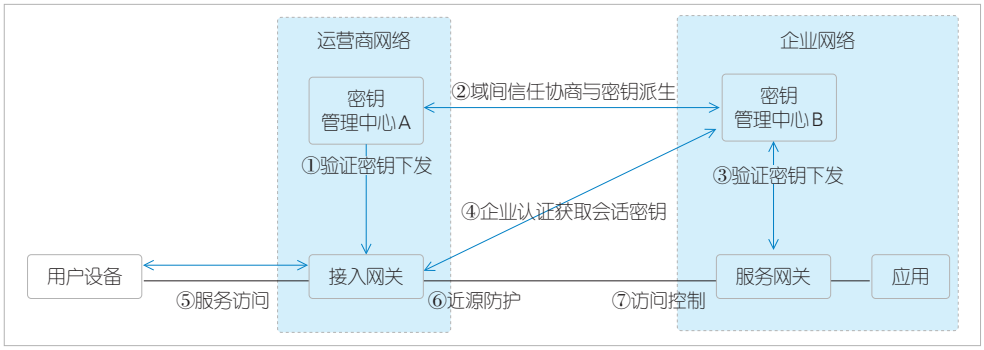
3.4 重放攻击主动检测

在可验证信息中添加时间校验子、序列号等动态信息，便于接入网关在用户设备发起业务流程时，及时基于动态信息对数据包进行检查与控制，有效抵御报文重放攻击。

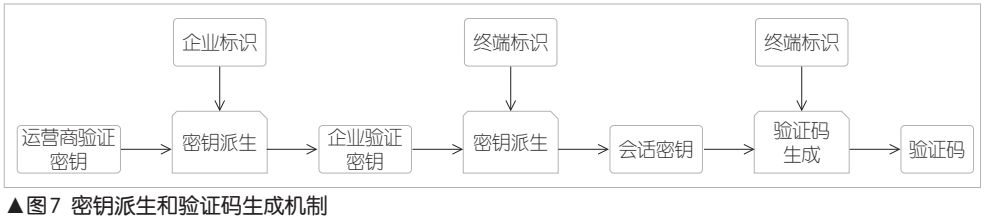
在如图8所示的重放攻击主动检测机制中，用户设备向接入认证服务器发起接入认证请求。认证成功后，接入认证服务器为用户设备分配终端密钥和系统时间，接入网关记录该系统时间，并结合网关本地时间计算、保存时间差。用户设备根据系统时间和设备本地时间计算时间差。当发送报文时，用户设备先根据时间差和设备本地时间生成时间校验子，再根据获取的终端密钥、时间校验子、序列号等生成校验码，最后发送数据包，包括校验码、时间校验子和序列号等信息。接入网关接收到用户设备发送的数据包后，根据保存的时间差和网关本地时间来确定系统时间，然后检验数据包中动态信息与校验码，以此识



▲图5 服务动态授权机制



▲图6 跨域协同防护机制



▲图7 密钥派生和验证码生成机制

别、控制因重放攻击引发的非法报文。

3.5 终端兼容性

未来网络中海量终端、产业弱终端均为攻击者提供了更多的攻击条件，严重加剧攻击程度，因此需要考虑终端兼容的可信通信机制，以减弱对性能差、安全能力不足或者传统终端所造成的影响。在终端无须感知的情况下，可考虑由接入网关代替终端完成可信通信相关安全功能：一方面需验证报文所经接入网关的真实可信；另一方面，对终端是否可访问服务进行控制。

当终端经传输设备发出报文时，接入网关应确定待转发数据报文的类型。如果是服务授权请求报文，则使用接入网关的密钥对接入网关的信息进行密码学计算并生成验证值，这便于后续的传输设备对报文的源身份进行验证。在保障身份真实性的基础上，后续设备为该报文生成预授权，并转发该报文。给用户设备返回的服务授权响应报文应携带授权检验信息。接入网关代替用户设备存储相关的授权检验信息。如果传输设备确定待转发的数据报文类型是服务请求报文，则对该报文添加存储的授权检验信息。接入网关之后的传输设备对数据报文携带的授权检验信息进行验证。若验证通过，则转发该数据报文。

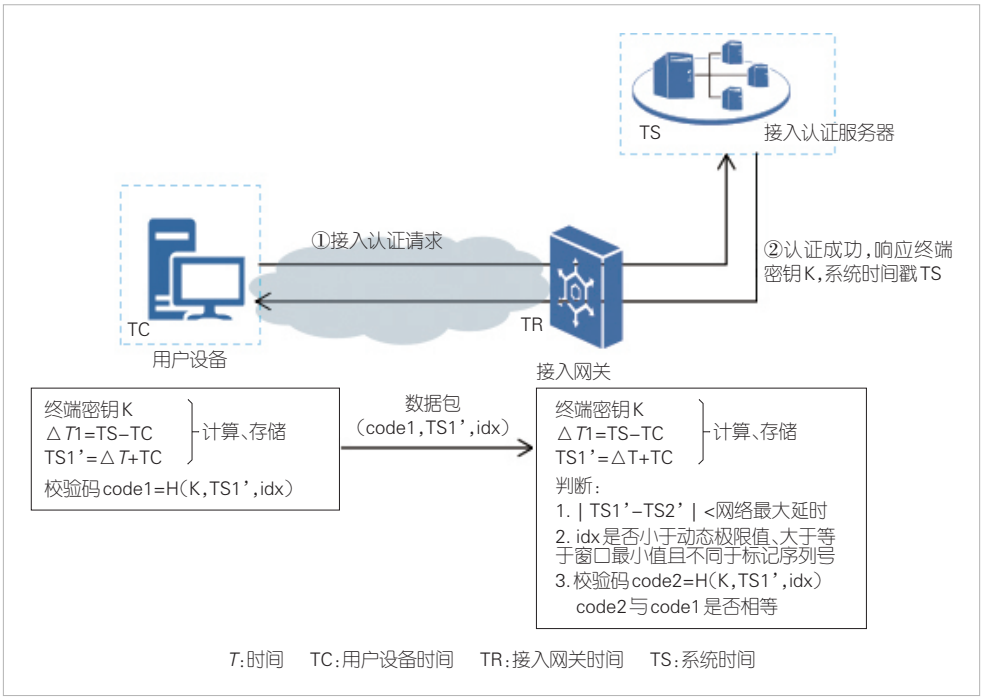
4 技术应用实例

基于NISC体系，中兴通讯进行了原型研制，并在中国信息通信研究院的协助下，在未来网络试验设施（CENI）深圳分系统开展了源地址真实性和服务动态授权技术跨域试验。

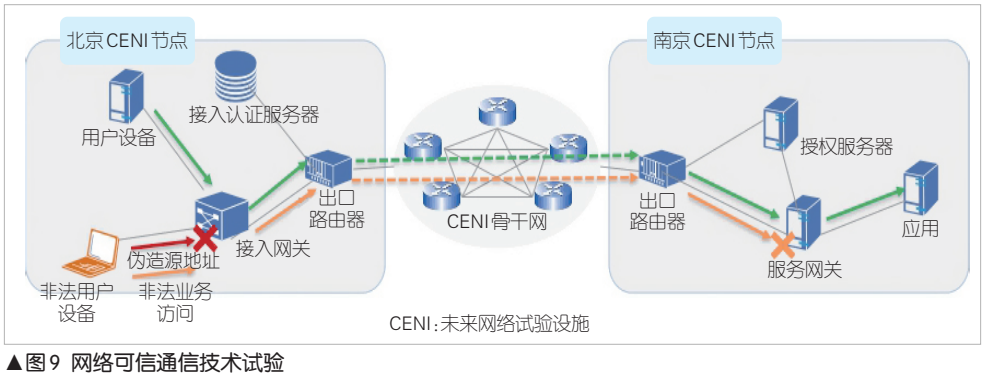
如图9所示，在NISC技术试验中，接入网关为用户设备提供源地址真实性检查功能，服务网关和授权服务器提供业务动态授权防御功能。整个系统利用认证服务器进行基于用户设备标识的认证，实现自主式便捷身份可信认证；支持基于对称密码学的身份可信机制，实现增强型高效地址真实性验证，以及面向应用业务的可信通信功能。经验证，本防御体系可实时检测并防范未认证用户，非法地址终端导致的泛洪、反射、中间人、越权访问等网络攻击，有效增强内生的系统性可信通信能力，实现未来云网系统的高效可信。通过对现有路由器和交换机等网络设备进行软件升级，可以有效防御绝大多数典型网络攻击，避免因额外部署流量清洗系统或防火墙等专用安全设备所带来的网络复杂、流量迂回和资本性支出（CAPEX）、运营成本（OPEX）增加等问题，可以在简化网络部署和运营的前提下实现网络安全性能的提升。

5 结束语

网络安全已成为社会发展、国家安全的基础需求。随着未来网络的不断发展，基于先验知识的被动防御模式已无法



▲图8 重放攻击主动检测机制



▲图9 网络可信通信技术试验

满足新型信任关系下的安全需求。因此，本文分析了未来网络面临的安全挑战，探讨了网络内生安全的技术要求和设计原则，提出了NISC技术。该技术具备近源协同防护、无状态随路验证等特征。未来，我们将继续探索分布式服务授权和精细化防控方案，促进可信通信技术在实际应用中的发展，如服务感知网络、园区生产网络、协同制造网络等。

致谢

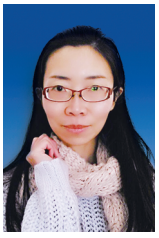
本研究得到中兴通讯股份有限公司谭斌、罗鉴、周继华、宋琳、武天元等专家的帮助，在此表示感谢！

参考文献

[1] 中国移动研究院. 5G-Advanced安全技术演进白皮书 [R]. 2022
[2] 中国移动. 算力网络安全白皮书 [R]. 2022
[3] CLARK D D, PARTRIDGE C, RAMMING C J, et al. A knowledge plane for the Internet [J]. Computer communication review, 2003, 33(4): 3-10. DOI: 10.1145/863955.863957
[4] SIST. Industrial communication network-network and system security part3-3: system security requirements and security assurance levels: IEC 62443-3-3 [S]. 2013
[5] MANOJ R, TRIPTI C. An effective approach to detect DDos attack [M]. Advances in Computing and Information Technology. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013: 339-345. DOI: 10.1007/978-3-642-31600-5_33
[6] IETF. Source address validation Improvement (SAVI) threat scope: RFC 6959 [S]. 2013
[7] 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
[8] 闫新成, 周娜, 蒋志红. 未来网络可信通信技术 [J]. 中兴通讯技术, 2021, 27(5): 52-59. DOI: 10.12142/ZTETJ.202105011
[9] 中兴通讯. IP网络未来演进技术白皮书 [R]. 2021
[10] WU J P, WU Q, XU K. Research and exploration of next-generation Internet architecture [J]. Chinese journal of computers, 2009, 31(9): 1536-1548. DOI: 10.3724/sp.j.1016.2008.01536
[11] 网络5.0产业和技术创新联盟. 网络5.0技术白皮书 [R]. 2021
[12] AAZHANG B, AHOKANGAS P, ALVES H, et al. Key drivers and research challenges for 6G ubiquitous wireless intelligence [EB/OL]. [2023-01-05]. https://www. researchgate. net/publication/336000008_Key_drivers_and_research_challenges_for_6G_ubiquitous_wireless_intelligence_white_paper
[13] YANG X W, WETHERALL D, ANDERSON T. TVA: a DoS-limiting network architecture [J]. ACM transactions on networking, 2008, 16(6): 1267-1280. DOI: 10.1109/tnet.2007.914506
[14] 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
[15] 徐恪, 冯学伟, 李琦, 等. 安全可信的互联网体系结构与端到端传送关键技术 [J]. 中兴通讯技术, 2022, 28(6): 17-22. DOI: 10.12142/ZTETJ.202206004

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，正高级工程师，江苏省“333高层次人才”；曾主持或参与国家科技重大专项课题，获多项省部级科技奖励；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；主要负责IP网络安全、移动通信安全和未来网络安全等技术研究工作。