研究与开发

基于可信网格DSTM的6G分布式自治网络安全机制研究

白杰，黄晓婷，杜海涛
（中国移动通信有限公司研究院，北京 100053）

摘　要：随着6G网络架构向分布式自治范式演进，传统集中式安全机制面临边界消失、身份易伪造和数据泄露等关键挑战。对此，提出分布式安全可信网格（distributed secure and trustworthy mesh，DSTM）系统。该系统通过构建逻辑安全边界，并实施动态安全策略，实现了分布式子网间的多层次身份认证、端到端安全连接、安全隔离与安全策略的动态执行。DSTM系统可与6G分布式网络架构深度融合，为未来6G网络安全体系设计提供重要参考。

关键词：6G；分布式自治网络；DSTM；网络边界；安全锚点
中图分类号：TN929.5
文献标志码：A
doi: 10.11959/j.issn.1000−0801.DXKX250554

Research on a DSTM-based trusted mesh security mechanism for 6G distributed autonomous networks

Bai Jie, Huang Xiaoting, Du Haitao
China Mobile Research Institute, Beijing 100053, China

Abstract: With the evolution of 6G network architecture toward a distributed autonomous paradigm, traditional centralized security mechanisms face significant challenges, such as boundary dissolution, susceptibility to identity forgery and data leakage. In response, a distributed secure and trustworthy mesh (DSTM) system was proposed. By constructing logical security boundaries and implementing dynamic security policies, the DSTM enables multi-level identity authentication, end-to-end secure connectivity, security isolation, and dynamic enforcement of security policies among distributed subnets. The DSTM can be deeply integrated with the 6G distributed architecture, providing valuable insights for the design of future 6G network security systems.

Key words: 6G, distributed autonomous network, DSTM, network boundary, security anchor

0　引言

6G作为空天地一体化全域覆盖的新一代移动信息系统，通过深度融合通信、感知、算力、AI等多维度要素，推动移动通信向综合移动信息服务演进，从而构建“数字孪生、智慧泛在”的

收稿日期：2025−09−15；修回日期：2026−01−19
通信作者：白杰，baijieyj@chinamobile.com
基金项目：国家重点研发计划项目（No.2022YFB2902203）
Foundation Item: The National Key Research & Development Program of China(No.2022YFB2902203)

未来世界[1]。随着第三代合作伙伴计划（3rd Generation Partnership Project，3GPP）首个6G标准研究项目——“6G场景用例与业务需求”正式获批[2]，全球6G标准化工作进入需求分析与技术方案论证的实质性推进阶段。

网络架构是移动通信系统的基础，直接决定网络服务的供给模式、系统运行效率与可扩展性。为支撑6G愿景的实现，6G网络架构的设计至关重要。其中，“分布式”作为6G网络架构的核心特征，已形成业界广泛共识[3]。美国NextG联盟指出，6G将提供分布式云服务和通信系统，在终端设备、网络节点和数据中心之间实现无处不在的计算与负载分布。基于虚拟化技术构建的分布式云和通信系统将提高混合现实、交互式游戏和多感官应用程序等关键用例的灵活性、性能和弹性[4-5]。欧盟Hexa-X项目提出了“网络之网络”的概念，并将其作为6G网络体系架构的关键特征之一[6]。“网络之网络”被定义为一种能够集成多种（子）网络解决方案的网络架构，有效融合不同类型的（子）网络，以实现多样化服务。中国IMT-2030（6G）推进组认为，6G网络架构应从集中式向分布式演进，通过集中+分布协同组网，实现资源、路由、功能等的分布式管理和优化调度，构建具备自生长、自优化、自演进能力的自治网络，从而在大规模复杂组网环境下实现网络资源和网络能力的优化调度，满足6G泛在连接和极致性能的需求[7]。中国移动提出了“三体四层五面”的6G网络架构总体设计[8]，指出6G网络架构将从集中规划式向分布自治式转变，以满足大规模组网下的海量连接和极致性能要求。该架构中的分布式自治网络（distributed autonomous network，DAN）由分布式微云单元（small cloud unit，SCU）及相关协议组成，SCU可在网络中分布式部署，具备自包含和自治能力。华为认为，6G网络将作为一个分布式平台，集成通信、感知和计算能力，可承载不同行业场景中的多样化业务负载[9]。

6G网络架构的分布式变革虽然有助于提升性能与拓展应用场景，但也带来了全新的安全挑战[10]：一方面，大量分布式子网共存导致6G网络面临安全边界模糊、安全机制缺少承载点、安全策略难以快速部署等风险；分布式子网根据需求灵活创建或拆除，也可能带来安全管理上的混乱。另一方面，分布式子网之间通过多种方式互联互通，其连接过程存在身份仿冒、信息泄露等安全隐患。

针对上述安全挑战，需要在整体的安全理念和具体的安全机制两个层面开展深入研究，将安全架构性地而非功能性地融入6G网络[11]，实现“网安一体”的6G安全体系。首先，在理念层面，安全思维应更加重视协作、共识与共享等维度，传统以“防御”为中心的安全理念已难以适应分布式网络互联互通的业务需求；其次，在机制层面，需要重点关注分布式网络与网络之间的身份信任体系与安全防护手段。本文提出6G分布式自治网络安全的核心思路：将每个分布式网络抽象为逻辑节点，在此基础上构建网络与网络之间的多层次认证机制与安全防护机制，以满足6G分布式自治网络之间的可信交互和安全保障需求。本文的主要贡献包括以下两方面。

（1）设计6G分布式安全可信网格（distributed security and trustworthy mesh，DSTM）系统，与6G分布式网络架构深度融合，为未来6G网络安全体系设计提供重要参考。

（2）提出通用DSTM锚点（DSTM anchor，DSTM-A），作为6G分布式自治网络的安全机制承载点，实现分布式网络之间的身份认证、安全互联、安全隔离以及安全策略实施。

1 相关工作

移动通信网络的核心功能是为个人用户提供“连接服务”，实现用户设备（user equipment，UE）之间、UE与互联网之间的通信。移动通信网络一般由接入网、承载网和核心网构成。其中，核心网作为整个移动通信网络的中枢系统，负责用户的移动性管理、会话管理，以及数据路由与转发功能。在2G、3G和4G阶段，移动通信网络相对封闭，核心网通常以集中式的方式部署在运营商机房内，运营商对整个通信网络拥有绝对管控权[12]。这一时期的安全防护重点聚焦于UE与网络间的接口安全（user-network interface security，UNIS）。围绕UNIS，相关安全机制陆续被提出，安全防护手段也不断完善[13]。

进入5G阶段，UNIS安全机制在多个方面得到进一步强化。例如，扩展了用户认证体系，支持切片认证与次认证；采用EAP-AKA’认证方式，提升认证安全性；引入面向应用层的认证和会话密钥管理（authentication and key management for applications，AKMA）机制，向应用层开放认证和密钥管理能力；完善用户面数据完整性保护机制；通过公钥机制生成加密的订阅隐藏标识符（subscription concealed identifier，SUCI），使得用户隐私保护更加全面。

更关键的是，5G新业务场景推动了移动通信网络架构的演进，其中最显著的变化就是核心网功能的下沉，以及由此催生的专网（non-public network，NPN）。5G专网将5G的应用场景向垂直行业拓展，利用5G高带宽、低时延、多接入的特点，为垂直行业提供高效、可靠的连接服务。垂直行业通常要求用户数据甚至控制信令必须保持在组织边界内，即实现“数据不出园区”，以充分保障业务的隐私性和安全性。为此，需要将5G核心网的关键网元，如用户平面功能（user plane function，UPF）、接入和移动性管理功能（access and mobility management function，AMF）、会话管理功能（session management function，SMF）、统一数据管理（unified data management，UDM）等，部署于企业本地，即实现核心网下沉。为了保证业务的正常运行，下沉的核心网仍需通过控制面与大网核心网保持连接。此外，在NPN场景下，UE通常只在所属的专网范围内使用，不会移动到其他专网中，即专网之间不存在互联互通需求。

5G专网的出现，一方面扩展了核心网的物理部署范围，另一方面也增加了网络的暴露面。下沉至企业园区的核心网不仅自身面临物理攻击的安全风险，还可能成为针对运营商大网核心网发起信令攻击、接口攻击等的跳板[14]。由于下沉的核心网不受运营商直接管控，其安全防护能力往往难以保证，下沉的核心网一旦被攻击者控制，将对大网核心网构成严重威胁。

为应对上述风险，5G大网普遍采取单边防御机制，即在运营商大网核心网部署安全网关类设备，对下沉核心网发送至大网核心网的信息进行检查和过滤，以防范专网失陷引发的对大网核心网的攻击。5G核心网下沉安全机制示意图如图1所示。这类安全网关设备的主要功能包括：下沉核心网网元的安全接入和安全通信、下沉核心网与大网之间的信令监测与消息过滤、大网的拓扑隐藏，以及下沉核心网对大网资源的访问控制等[15]。

此外，从2G开始，3GPP便提出了安全域的概念。在同一安全域内，网络节点通常采用相同级别的安全性和安全服务[16]。在不同的安全域之间，如不同的运营商之间，安全域边界由安全网关保护。在5G阶段，引入安全边界防护代理（security edge protection proxy，SEPP）作为运营商核心网控制面之间的边界网关，所有跨运营商的信息传输均需要通过该安全网关进行处理和转发[17]。

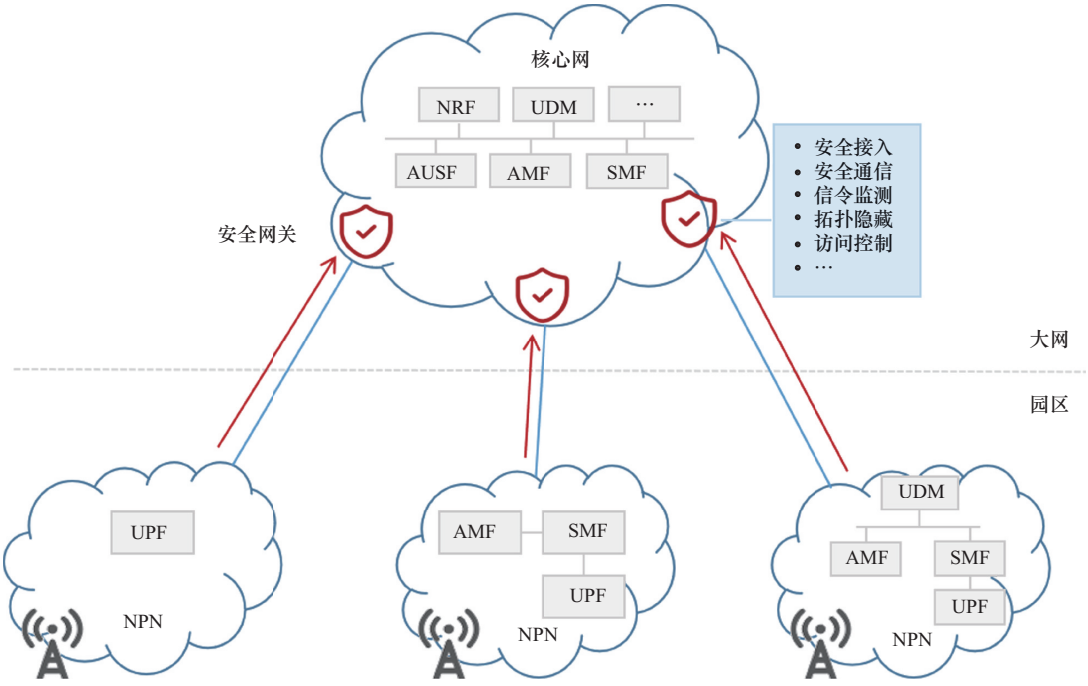

图1　5G核心网下沉安全机制示意图

2　6G分布式网络概述

2.1　关键特性

ITU-R明确了6G的典型场景和关键技术指标，提出了包括沉浸式通信、超大规模连接、极高可靠低时延、人工智能与通信融合、感知与通信融合、泛在连接在内的六大场景[18]。这些场景对网络的泛在连接和极致性能、可靠性和灵活性、海量数据复杂计算能力提出了更高要求，进而驱动6G网络架构向分布式方向演进[19-21]。

与5G网络“按需下沉用户面/控制面”的模式不同，6G网络将由集中式的中心网络和大量差异化、定制化的分布式子网构成。6G分布式网络示意图如图2所示。6G分布式子网包括各类边缘网络、企业专网和园区网络等。中心网络与分布式子网之间、各分布式子网之间将通过互联互通和资源共享协作，实现网络资源和网络能力的优化调度，从而满足6G场景下的多样化业务需求。

2.2　安全挑战

相较于5G专网，6G分布式网络架构具有“异构、协同、灵活、自治”四大新特征：融合移动通信网、卫星互联网、物联网等多种异构网络，通过分布式子网间的互联互通，为用户提供泛在接入服务；分布式子网与中心网络之间、分布式子网之间能够实现信息共享和高效协同，支持实时网络资源调度，保障6G网络服务的连续性[22]；分布式子网可按需创建和拆除，并且灵活提供服务能力，满足用户定制化需求；分布式子网本地具备完整的功能、资源与连接能力，能够独立完成闭环网络流程处理，实现功能自组织、网络自管理。

与此同时，6G分布式网络架构也带来了新的安全挑战。

（1）大量分布式子网共存，导致安全边界消失、网络拓扑信息易泄露；分布式子网中的核心网功能通常会经过定制化裁剪，导致安全机制缺少承载点；分布式子网灵活按需创建或拆除，也会引发安全管理混乱。

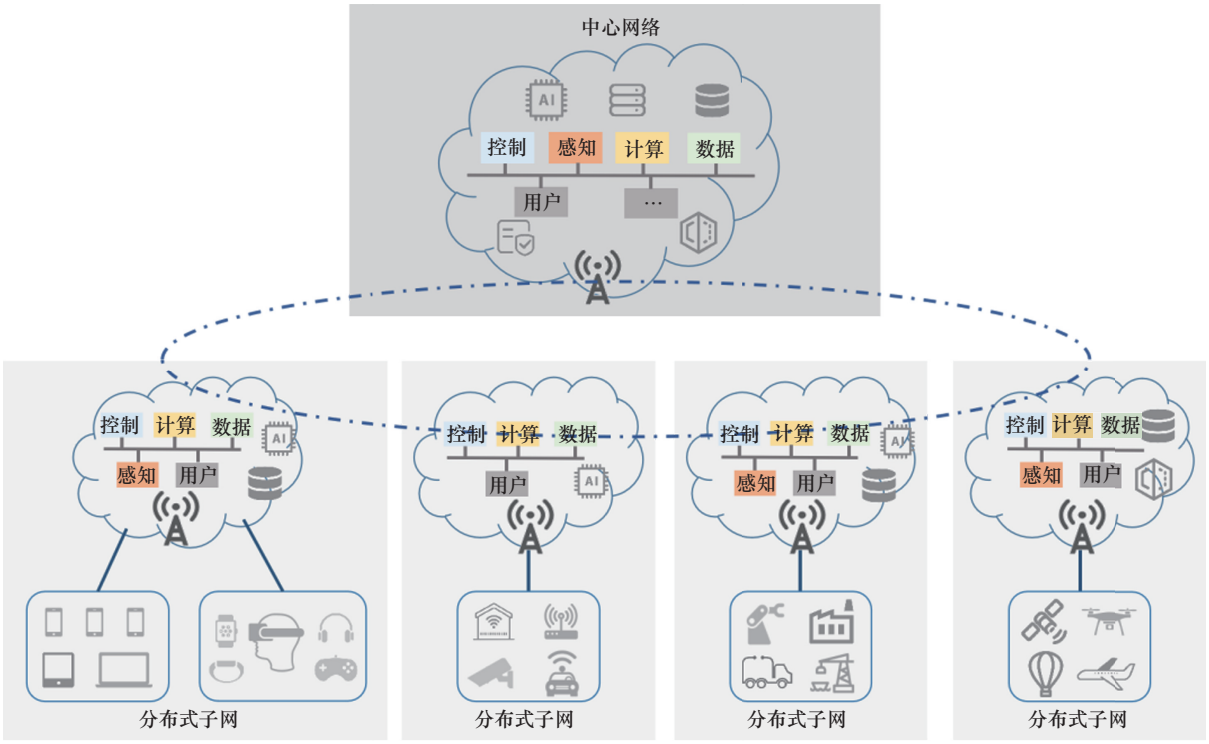

图2　6G分布式网络示意图

（2）分布式子网之间通过多种方式互联互通，子网之间的连接存在身份仿冒、数据泄露等安全问题；分布式子网之间缺少安全协同机制，导致针对用户及网络的安全策略难以灵活快速实施。

当前5G采用的在运营商大网核心网部署安全网关的机制，难以满足6G分布式网络的安全需求。首先，该机制属于单边防御，仅侧重于保护大网核心网，未充分考虑网络之间的协同安全；其次，安全网关预置的安全检查和过滤策略存在单一、固化的缺点，难以满足异构分布式子网之间灵活互联互通的安全需求；最后，安全网关只针对少量特定的下沉专网部署，在大量分布式子网协作的场景下，部署安全网关将会增大组网复杂性和成本。

因此，6G分布式网络需突破传统安全框架，将安全视角从“UE-网络”扩展至“网络–网络”（network-network interface security，NNIS）。通过构建逻辑安全边界、实施动态身份认证与防护机制，直观呈现子网间信任状态与连接关系，并构建通用化、可复用的安全能力，以降低整体安全部署成本。

3　DSTM系统

3.1　设计原则

为应对上述安全挑战，在设计6G分布式自治网络架构时，需要引入新的安全机制。一方面，分布式子网与中心网络之间、分布式子网之间需要实现双向身份认证，这是实现网络间互联互通的前提[23]；另一方面，在分布式子网与中心网络之间、分布式子网之间建立灵活、按需的安全连接，以保障网络之间传输的信令、用户业务数据以及其他信息的机密性和完整性。

为实现上述目标，需要考虑如下设计原则。

（1）在中心网络及每个分布式子网本地，需要设置一个安全锚点，用以代表该网络的身份，从而将网络抽象为一个节点。

（2）该安全锚点需要具备加解密、完整性保护等功能，并能在不同安全锚点之间建立安全连接。

（3）该安全锚点可以是一个独立的网元，也可以作为其他网元的安全组件。与5G专网中部署的安全网关类设备相比，其设计应该更具通用性和灵活性，以适应更广泛的应用场景。

（4）分布式子网中的安全锚点与中心网络的安全锚点可根据需要实现互联互通，共同构成一个逻辑上的安全边界，呈现中心网络和分布式子网之间的信任关系和连接状态。

遵循上述设计原则，本文提出了6G分布式安全可信网格系统——DSTM。该系统基于一种通用的安全锚点DSTM-A，作为6G分布式自治网络的安全机制承载实体，旨在实现分布式网络之间的身份认证、安全互联互通、安全隔离以及安全策略的实施。

3.2　DSTM系统概述

与5G专网相比，6G分布式网络的一个显著变化是业务访问灵活多变。在5G专网场景下，UE在专网覆盖范围内访问业务，且不同专网之间通常不存在互联互通的需求。在6G分布式网络场景下，UE进行业务访问时，可能会从一个分布式子网移动到另一个分布式子网，这两个分布式子网之间就会涉及控制面或用户面的交互，这就要求分布式子网之间能够互联互通。在某些特定场景下，两个分布式子网之间甚至可能需要动态建立连接，并在业务访问完成后拆除连接，以节省设备资源和网络资源。因此，子网之间应能根据实际业务需求，灵活建立连接，以满足差异化的业务需求。

回顾UE与网络间的安全机制：UE侧的通用用户标识模块（universal subscriber identity module，USIM）中存储根密钥，网络侧也存储相同的根密钥，双方基于根密钥实现双向身份认证，并基于根密钥衍生出的一系列密钥，对数据进行加密和完整性保护，进而实现安全接入。借鉴UE接入网络的安全机制，分布式子网也需要类似“USIM”的信任载体，以支持网络间的身份认证、安全连接以及其他安全机制的实施。为此，本文提出每个分布式子网都应具备安全锚点DSTM-A，并基于该安全锚点构建6G分布式安全可信网格（DSTM）系统。

为实现众多DSTM-A之间的灵活连接，网络需要引入集中的控制系统[24]。该控制系统应全面了解各分布式网络的业务需求，并掌握每个安全锚点的能力和运行状态。借鉴业界成熟的软件定义网络（software defined network，SDN）理念，可通过在网络中部署集中控制器，对所有的DSTM-A进行管控。DSTM-A通过北向接口与控制器连接，在控制器的调度下，根据业务需求灵活建立或拆除安全连接，从而实现设备资源和网络资源的优化使用。

分布式安全锚点与集中式的控制器协同工作，共同构成6G分布式安全可信网格（DSTM）系统，其示意图如图3所示。DSTM中的“节点+连接”的架构形成了清晰的网络安全边界，使每个分布式子网的工作状态、连接情况等信息全局可见。由于DSTM-A能够以插件的形式嵌入6G核心网网元中，DSTM系统也就可以自然融入6G分布式网络架构，并以内生的方式增强6G分布式网络的安全性。

3.3　DSTM实现

在DSTM系统的调度和架构支持之下，每个分布式子网中的DSTM-A实体需要具备如下功能，以保障整个6G分布式自治网络的安全运行。

（1）建立信任关系

支持身份认证功能，包括在接入网络时实现分布式子网与中心网络之间的双向认证，在业务交互中实现分布式网络之间的双向认证。具体包括信任凭证管理功能，适用于分布式子网内部的集中式公钥基础设施（public key infrastructure，PKI）/证书授权（certificate authority，CA）机制，以及适用于分布式网络之间互联的分布式区

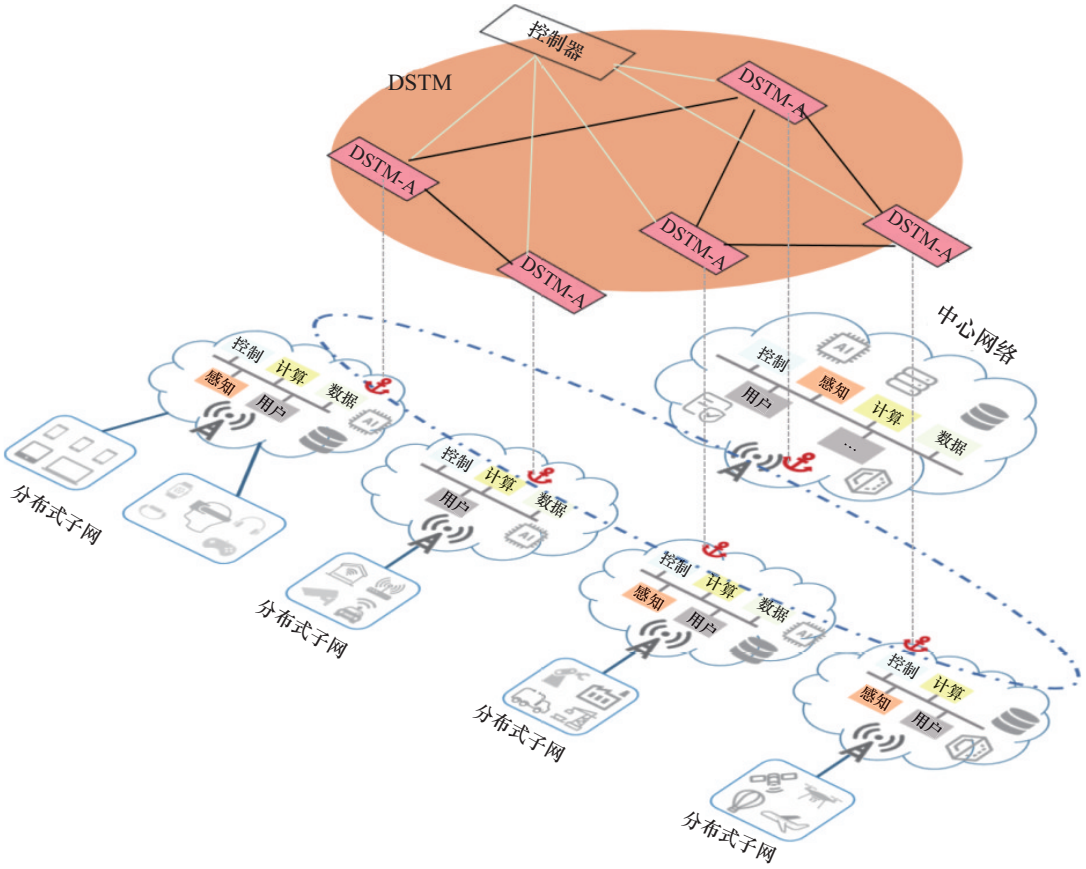

图3　6G分布式安全可信网格系统DSTM示意图

块链机制等。

（2）建立安全连接

支持安全连接的协商与建立功能，确保分布式网络之间数据传输的安全性。具体包括密钥管理功能，并兼容主流安全协议，如互联网安全协议（Internet protocol security，IPSec）/因特网密钥交换协议（Internet key exchange，IKE）、传输层安全性协议（transport layer security，TLS）、快速UDP网络连接（quick UDP internet connection，QUIC）等。

（3）实现安全隔离（安全网关）

通过DSTM-A实施以下安全网关功能，实现分布式子网与中心网络之间、分布式子网之间的安全隔离。一，网络拓扑隐藏。通过信令代理机制，对消息进行重组与转发，双向屏蔽网络暴露面，从而实现拓扑隐藏功能。二，信令监测。对信令消息格式进行规范性检查，识别异常消息，并对其采取过滤或重传等纠错处理措施；监控全局信令，检测和防范异常信令逻辑攻击。例如，信令行为不完整攻击，如应发往所有同类对端网元的消息却没有逐一发送的异常行为。三，网络隔离。通过代理转发功能，可在中心网络与分布式子网、分布式子网之间配置不同的虚拟专用网络（virtual private network，VPN），实现不同安全域的隔离与防护。

（4）执行安全策略

针对6G分布式子网之间灵活多变的互联互通业务需求，安全策略常面临随业务动态变化、缺少承载点等问题[25]。一方面，用户可能在不同分布式子网间移动，并在目标分布式子网中开展业务，相应的安全策略需应用于目标分布式子网

中。另一方面，分布式子网自身也存在安全协同、动态防御等需求，需要对整个子网或者子网中的网元实施新的安全策略。基于DSTM系统，在控制器的统一编排和调度下，DSTM-A能够接受并执行控制器下发的安全策略，对本分布式子网实施安全管理，并对移动到本子网的用户执行相应策略，从而实现安全策略的“业务随行”。

DSTM-A对外提供3类接口，分别是北向接口、南向接口和东西向接口。DSTM-A的逻辑系统架构及接口关系示意图如图4所示。

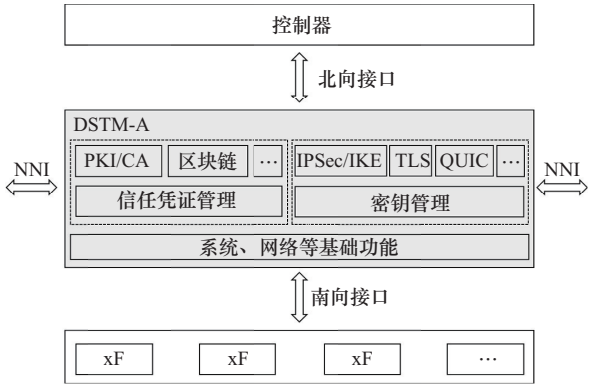

图4　DSTM-A的逻辑系统架构及接口关系示意图

北向接口：DSTM-A通过北向接口与控制器相连，在控制器的调度下，多个DSTM-A之间能够灵活、按需建立或拆除安全连接。同时，接受控制器下发的安全策略，并对本子网执行安全策略。

南向接口：DSTM-A通过南向接口与6G核心网网元相连。作为6G中心网络及分布式子网内核心网网元的“安全经纪人”，不同网络内的核心网网元跨网络通信时，数据可通过DSTM-A进行转发，以保证数据传输的安全性。

东西向接口：DSTM-A之间的接口，即网络到网络接口（NNI）。DSTM-A通过NNI进行身份认证，建立信任关系，同时建立安全连接，呈现分布式网络之间的连接状态。

DSTM-A可以作为独立的形态部署和运行，也可以作为插件（Plug-in）形态嵌入未来6G核心网网元，与6G分布式网络架构融为一体。

3.4　信任建立

3.4.1　代理级别认证

信任的建立通常通过实体之间的双向认证来实现。作为分布式子网的安全锚点，DSTM-A具备代替所在子网与中心网络进行认证或子网间进行互认证的功能。在一些信任关系满足由DSTM-A代替子网实现认证的场景下，所在子网的DSTM-A完成认证之后，该子网的其他网元可不再执行网元级别的认证。该方式可称为“代理级别的认证”。考虑到6G网络需与前几代通信网络保持兼容，提出了两种实现流程，即传统集中式方式和分布式方式，运营商可根据实际业务需求选择使用。传统集中式方式与前几代移动通信网的信任架构和体系相吻合，可减少对已有设备的改造。例如，在使用传统PKI方式时，若分布式子网A与分布式子网B中的DSTM-A之间需要进行相互认证，分布式子网A中的DSTM-A_A将其公钥证书发给分布式子网B中的DSTM-A_B，DSTM-A_B则携带证书向CA机构进行证书查询，并接收CA机构返回的查询结果。DSTM-A_B根据CA机构返回的证书状态完成对DSTM-A_A的认证。

如果采用传统集中式方式，每个自治网络属于不同的信任域，就会有不同的CA发布证书，由于信任域的相互隔离导致数字证书不能跨域使用。分布式的方式可以通过区块链实现CA机构之间相互协作[26]。CA机构向区块链发布证书，依赖方通过区块链查询证书及其状态。分布式方式DSTM-A_B对DSTM-A_A的认证如图5所示。图5流程实现的前提是DSTM-A_A已经将其证书注册到区块链上，且区块链已对该证书进行存储和状态维护。与传统集中式方式流程不同的是，DSTM-A_B向区块链而非CA机构进行证书查询。

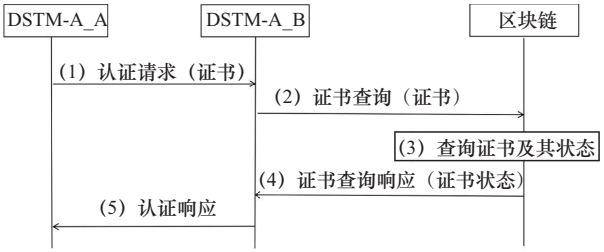

图5 分布式方式DSTM-A_B对DSTM-A_A的认证

在一些对信任需求高的场景下，由DSTM-A代理子网实现认证可能并不足以实现子网网元与其他子网网元之间的认证。因此，本文还设计了网元级别的认证机制。

3.4.2 网元级别认证

与代理级别认证类似，网元级别认证也提供了两种实现方式，包括传统集中式方式和分布式方式，运营商可根据实际业务需求进行选择。

传统集中式方式的实现前提是各分布式子网的DSTM-A之间已完成相互认证。其流程如下：子网A的网元NF_A先要通过DSTM-A_A的认证（如采用OAuth协议），获得由DSTM-A_A颁发的访问令牌（token）。凡是DSTM-A_A颁发的token，均会携带DSTM-A_A的标记属性。由于DSTM-A_B此前已经完成对DSTM-A_A的认证，因此会信任携带DSTM-A_A标记属性的token。当NF_A携带token向NF_B发起认证请求，NF_B会将token转发至DSTM-A_B进行验证。DSTM-A_B会根据前期与DSTM-A_A的认证结果返回token验证结果。验证成功后，NF_B根据token验证的结果向NF_A返回认证响应。

若采取分布式方式，则通过区块链存储各子网DSTM-A为其子网网元发布的token，从而大大节省DSTM-A的存储和计算开销[27]。各DSTM-A通过查询区块链来验证来自其他子网网元的token验证请求。分布式方式实现网元级认证流程如图6所示。

3.5 安全连接

3.5.1 数据安全传输

6G分布式网络之间通过安全连接实现数据传输的安全性，这也是NNI安全的重要组成部分。在多样化、个性化的6G业务场景下，分布式网络之间可通过多种方式实现互联互通，例如运营商专线、共同互联网，甚至通过分布式网络（中心网络或分布式子网）连接。这就要求DSTM系统具备建立灵活安全连接的能力，以适配不同网络状态、不同连接条件下的差异化需求。

DSTM-A之间通过安全协议建立安全连接，目前常见的安全协议包括IPSec/IKE、TLS、QUIC等。

（1）IPSec/IKE

IPSec是一系列为IP网络提供安全服务的协

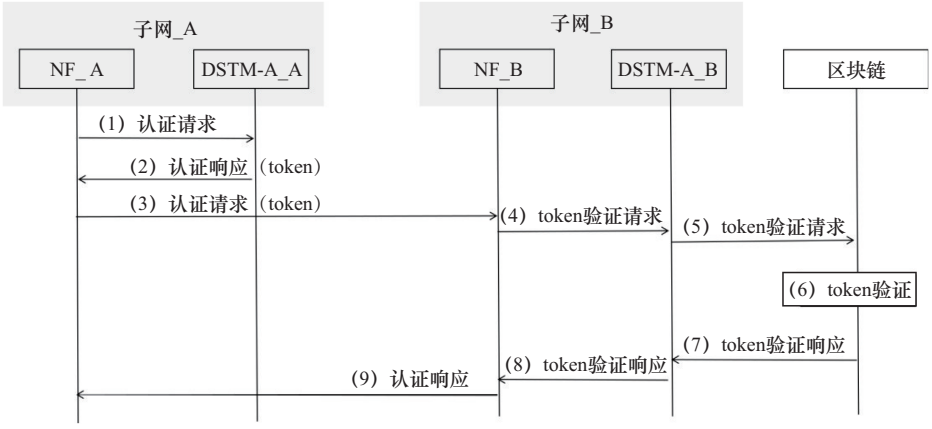

图6 分布式方式实现网元级认证流程

议集合[28]，能够在两个设备之间建立一条 IPSec 加密隧道，以确保通过该隧道传输的数据安全。

IKE 是一种用于在 IPSec 中协商密钥的协议[29]，允许通信双方在建立 IPSec 安全连接之前协商和交换密钥。IKE 采用迪菲-赫尔曼（Diffie-Hellman，DH）算法在不安全的网络上安全地分发密钥，并建立 IPSec 安全联盟，极大地提高了安全性。IKE 协议的最新版本是 IKEv2，其特点是简化了安全联盟的协商过程，提高了协商效率且增强了协议本身的安全性。

（2）TLS

TLS 是一种安全通信协议，用于在网络中提供加密通信和数据完整性保障[30]。TLS 支持端到端加密，确保数据在传输过程中不被篡改，并具有灵活性、兼容性、扩展性等特点，是目前互联网上应用最广泛的加密协议之一。当前 TLS 协议的最新版本是 TLS 1.3，其在性能和安全性方面都有显著提升。

（3）QUIC

QUIC 是一种用于替代传输控制协议（transmission control protocol，TCP）的新型网络传输协议[31]。它基于用户数据报协议（user datagram protocol，UDP）提供与 TCP 类似的可靠传输服务，同时解决传统 TCP 在延迟和拥塞控制方面的不足。QUIC 集成了流量控制、连接管理和安全加密等功能，优化了传输性能，通过多路复用机制解决队头阻塞问题，具备低时延连接建立、灵活的拥塞控制和丢包恢复机制，是一种高速、低时延、安全、稳定的网络传输协议。

3.5.2　密钥管理与交换

密钥是 DSTM-A 之间建立安全连接的关键参数，也是实现数据机密性和完整性的基础。传统方式下，两个 DSTM-A 之间通常基于非对称密钥协商生成对称密钥，如使用 DH 密钥交换算法。在 6G 分布式网络复杂多变的互联互通场景中，仅依赖传统方式可能会降低安全连接建立的效率。因此，可以考虑结合其他方式，如通过区块链或控制器实现密钥交换，或协同使用多种方式，以提升不同场景下建立安全连接的效率。

（1）通过区块链实现密钥交换

利用区块链去中心化、防篡改、多方共识等特点[32]，由区块链向 DSTM-A 分发用于计算对称密钥的密钥材料。具体流程为：DSTM-A 先将密钥材料上传至区块链；当两个 DSTM-A 需要建立安全连接时，它们分别从区块链获取对应的密钥材料，各自基于密钥材料分别计算出对称密钥，继而完成安全连接的建立。

（2）通过控制器实现密钥交换

通过控制器分发用于计算对称密钥的密钥材料，也是一种高效快捷建立安全连接的方式。当两个 DSTM-A 需要建立安全连接时，它们先将密钥材料发送至控制器，再由控制器转发给对方，双方根据获取的密钥材料分别计算出对称密钥，然后建立安全连接。

4　案例分析

DSTM 系统将一种通用的安全锚点作为未来 6G 分布式自治网络的信任与安全机制承载点，以实现分布式网络之间的身份认证和安全连接。本节基于 DSTM 系统，针对特定应用场景的实施过程进行推演，设计详细的运行分析流程，以说明该系统的安全性和可靠性。

在 6G 分布式自治网络架构下，设定如下安全应用场景：不同分布式子网内的核心网网元期望建立跨网络的端到端可信通信链路。DSTM 系统运行流程如图 7 所示。

（1）参数定义

Net：分布式子网。例如，子网 N 表示为 Net_N，N 为网络编号或名称。

NF：核心网网元。例如，子网 N 中的网元 1

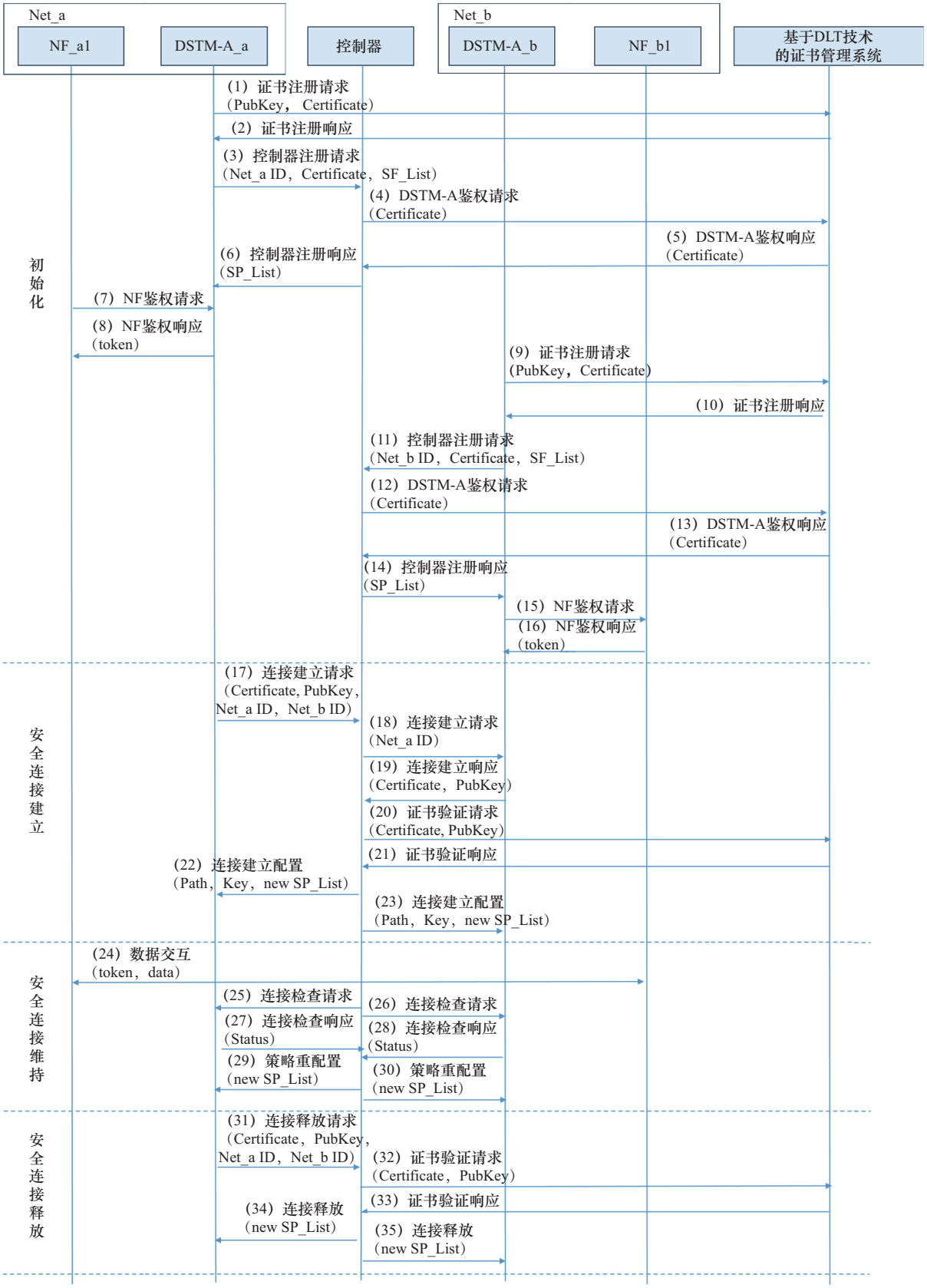

图7 DSTM系统运行流程

表示为NF_N1。

SF_List：设备或服务所能提供的安全能力列表，为一个能力与状态的集合。

SP_List：由控制器制定并下发给DSTM-A节点的安全策略列表，规定网络中各类安全操作的规则和要求。

Certificate：签发的证书，用于验证DSTM-A节点的身份。

token：由DSTM-A生成，用于验证网元节点之间的身份。

Key：会话密钥，用于加密和解密数据，确保数据传输的安全性。

PubKey：公共密钥，与证书共同使用。

Path：传输路径，表示从源节点到目的节点的数据传输路线。

Data：在网络中传输的各类数据信息，包含用户的业务数据和网络控制信令数据等。

Status：子网当前状态信息集合，反映子网的实时网络状况。

（2）端到端可信链路构建运行推演

初始化阶段：

步骤 1：分布式子网Net_a中的DSTM-A_a节点向基于分布式账本技术（DLT）的证书管理系统发起请求，基于区块链构建去中心化公钥基础设施（DPKI），将分布式子网Net_a的证书、认证凭据等信息上传至区块链，为后续身份认证和信任验证作准备。

步骤 2：DSTM-A_a获得系统响应。

步骤 3：DSTM-A_a向控制器发起注册，提供子网的标识、证书及其安全能力信息。

步骤 4：控制器收到DSTM-A的注册请求后，对其证书进行验证。

步骤 5：验证通过，控制器与DSTM-A建立信任关系，同时意味着分布式子网Net_a完成身份验证。

步骤 6：控制器保存DSTM-A提供的子网信息，并根据其安全能力动态生成初始安全策略，并下发至该DSTM-A节点。

步骤 7：核心网网元向其所属子网的DSTM-A进行注册。

步骤 8：注册完成，网元获取DSTM-A下发的token，用于后续跨网络设备间的身份认证与信任建立。至此，子网Net_a初始化阶段完成。

步骤 9～16：子网Net_b的初始化过程与Net_a一致。

安全连接建立阶段：

步骤 17：DSTM-A_a发起“建立从子网Net_a到子网Net_b的可信链路”的业务需求，并将安全需求发送至控制器，包含子网证书、公钥、源子网标识与目标子网标识。控制器负责建立不同子网的DSTM-A间的NNI安全连接。

步骤 18：控制器将源子网的连接建立请求转发至目标子网的DSTM-A。

步骤 19：目标子网DSTM-A响应连接请求，将其子网证书与公钥发送至控制器。

步骤 20～21：控制器利用PKI/CA机制，通过证书、时间戳等信息完成源子网和目标子网的身份验证，防止欺诈、重放等攻击。

步骤 22～23：控制器根据业务需求与两个子网的安全能力，选择最优传输路径，制定新的安全策略并生成会话密钥，随后将路径信息、新安全策略、会话密钥分别返回给源子网与目标子网的DSTM-A。至此，分布式子网间的端到端可信通信链路完成建立。

安全连接维持阶段：

步骤 24：源子网与目标子网内已完成注册的网元，可通过已建立的可信链路进行数据交互。交互数据分别由所属子网内的DSTM-A进行透明转发，DSTM-A通过token验证网元身份，确保数据安全可信。

步骤 25～26：在两个子网的数据交互过程中，控制器负责维持子网间的安全连接，并根据业务需求

和自身安全策略分别对子网间的安全连接进行检查。

步骤27～28：源子网与目标子网内的DSTM-A分别向控制器上报所在子网的实时网络状况。

步骤29～30：控制器根据子网的状态信息，实时调整安全策略，确保子网间端到端可信链路的保持。

安全连接释放阶段：

步骤31：业务完成后，源子网的DSTM-A向控制器发送连接释放请求。

步骤32～33：控制器对该释放请求进行验证。

步骤34～35：控制器分别通知源子网和目标子网，拆除安全连接、释放资源，同时根据子网状况重新调整安全策略。

5 结束语

6G网络架构向分布式演进，其在满足泛在连接和极致性能要求的同时，也带来了新的安全挑战。大量分布式子网共存并实现互联互通，导致安全边界消失、安全机制缺少承载点，同时面临身份仿冒、信息泄露等安全问题。现有5G专网安全机制未充分考虑网络之间的协同，难以满足6G分布式网络灵活互联互通的安全需求。

针对上述问题，本文深入分析了6G分布式自治网络的关键特性和安全挑战，提出了6G分布式安全可信网格（DSTM）系统及其核心组件——通用安全锚点（DSTM-A），以期为6G分布式网络安全架构的详细设计提供参考。DSTM系统突破传统“集中式安全网关”的局限，采用“逻辑边界+分布式锚点”的架构设计，适配6G分布式网络拓扑，为6G网络安全体系提供“内生安全”解决方案；DSTM-A支持灵活部署（可作为独立网元或集成插件），作为6G分布式网络安全机制的承载实体，能够实现分布式网络之间的多层次身份认证、安全互联互通、安全隔离以及安全策略实施，满足6G分布式网络之间的信任和安全保障需求。

DSTM在构建6G分布式子网逻辑安全边界、实施动态身份信任与防护机制等方面展现出良好的应用潜力，但在资源受限的边缘分布式子网、子网网络拓扑高度动态变化、全局状态一致性要求极高等场景中，其适用性或面临显著挑战。未来，将从以下3个方向对DSTM进行优化，以进一步提升分布式安全可信机制的效能与适应性。首先，针对资源受限的分布式子网，设计轻量化安全锚点和安全协议，在确保网络性能的前提下降低资源消耗，实现性能与安全的有效平衡。其次，引入人工智能技术，对网络行为进行智能化实时分析与威胁预测，构建智能感知与响应机制。最后，设计向后量子密码迁移的机制，预留支持后量子密码算法的接口，以应对未来量子计算带来的潜在安全威胁。

参考文献：

[1] Liu G Y, Huang Y H, Li N, et al. Vision, requirements and network architecture of 6G mobile network beyond 2030[J]. China Communications, 2020, 17(9): 92-104.

[2] 3GPP TR 22.870 V17.0.0.2024 Study on 6G use cases and service requirements[S].

[3] Wang C X, You X H, Gao X Q, et al. On the road to 6G: visions, requirements, key technologies, and testbeds[J]. IEEE Communications Surveys & Tutorials, 2023, 25(2): 905-974.

[4] Next G Alliance. Roadmap to 6G[R]. 2022.

[5] Next G Alliance. 6G distributed cloud and communications systems[R]. 2022.

[6] Hexa-X. Initial 6G architectural components and enablers[R]. 2021.

[7] IMT-2030(6G)推进组. 6G网络架构展望白皮书[R]. 2023.
IMT-2030 (6G) Promotion Group. 6G network architecture vision white paper[R]. 2023.

[8] 中国移动. 中国移动6G网络架构技术白皮书[R]. 2022.
China Mobile. China mobile 6G network architecture technology white paper [R]. 2022.

[9] 华为. 6G: 无线通信新征程白皮书[R]. 2022.
Huawei. 6G: A new journey for wireless communication white paper[R]. 2022.

[10] Wang M H, Zhu T Q, Zhang T, et al. Security and privacy in 6G networks: new areas and new challenges[J]. Digital Com-

munications and Networks, 2020, 6(3): 281-291.

[11] 金梁, 楼洋明, 孙小丽, 等. 6G无线内生安全理念与构想[J]. 中国科学(信息科学), 2023, 53(2): 344-364.
Jin L, Lou Y M, Sun X L, et al. Concept and vision of 6G wireless endogenous safety and security[J]. Science in China (Information Sciences), 2023, 53(2): 344-364.

[12] He Y, Yu F R, Zhao N, et al. Secure social networks in 5G systems with mobile edge computing, caching, and device-to-device communications[J]. IEEE Wireless Communications, 2018, 25(3): 103-109.

[13] 3GPP TS 33.501 V17.5.0. 2023 Security architecture and procedures for 5G system[S].

[14] 3GPP TR 33.757 V17.0.0. 2024 Study on security for PLMN hosting a NPN[S].

[15] Luque-Schempp F, Panizo L, Gallardo M D M, et al. Toward zero touch configuration of 5G non-public networks for time sensitive networking[J]. IEEE Network, 2022, 36(2): 50-56.

[16] 3GPP TS 33.210 V15.0.0. 2015 Network domain security (NDS); IP network layer security[S].

[17] 齐旻鹏, 粟栗, 彭晋. 5G网间互联互通安全机制研究[J]. 移动通信, 2019, 43(10): 13-18.
Qi M P, Su L, Peng J. Research on 5G inter-network interconnection security mechanism[J]. Mobile Communications, 2019, 43(10): 13-18.

[18] ITU-R M.2160.2023 Framework and overall objectives of the future development of IMT for 2030 and beyond[S].

[19] IMT-2030(6G)推进组. 6G分布式网络技术的应用场景及需求研究[R]. 2022.
IMT-2030 (6G) Promotion Group. Research on application scenarios and requirements of 6G distributed network technology[R]. 2022.

[20] Dang S P, Amin O, Shihada B, et al. What should 6G be?[J]. Nature Electronics, 2020, 3(1): 20-29.

[21] Zuo Y P, Guo J J, Gao N, et al. A survey of blockchain and artificial intelligence for 6G wireless communications[J]. IEEE Communications Surveys & Tutorials, 2023, 25(4): 2494-2528.

[22] Nguyen D C, Ding M, Pathirana P N, et al. 6G Internet of Things: a comprehensive survey[J]. IEEE Internet of Things Journal, 2021, 9(1): 359-383.

[23] Lee J H. Secure authentication with dynamic tunneling in distributed IP mobility management[J]. IEEE Wireless Communications, 2016, 23(5): 38-43.

[24] 袁和昕, 刘百祥, 阚海斌, 等. 基于区块链和去中心不可否认属性签名的分布式公钥基础设施方案[J]. 中国科学(信息科学), 2022, 52(6): 1135-1148.
Yuan H X, Liu B X, Kan H B, et al. Distributed public key infrastructure scheme based on blockchain and decentralized undeniable attribute-based signature[J]. Science in China (Information Sciences), 2022, 52(6): 1135-1148.

[25] Fang D F, Qian Y, Hu R Q. Security for 5G mobile wireless networks[J]. IEEE Access, 2017, 6: 4850-4874.

[26] Papageorgiou A, Mygiakis A, Loupos K, et al. DPKI: a blockchain-based decentralized public key infrastructure system[C]//Proceedings of the 2020 Global Internet of Things Summit (GIoTS). Piscataway: IEEE Press, 2020: 1-5.

[27] Patsonakis C, Samari K, Roussopoulos M, et al. Towards a smart contract-based, decentralized, public-key infrastructure[M]// Cryptology and Network Security. Cham: Springer International Publishing, 2018: 299-321.

[28] IETF RFC 4301.2025 Security architecture for the Internet protocol[S].

[29] IETF RFC 7296.2014 Internet key exchange protocol version 2 (IKEv2)[S].

[30] IETF RFC 8446.2018 The transport layer security (TLS) protocol version 1.3[S].

[31] IETF RFC 9000. 2021 QUIC: A UDP-based multiplexed and secure transport[S].

[32] Gao W C, Hatcher W G, Yu W. A survey of blockchain: techniques, applications, and challenges[C]//Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN). Piscataway: IEEE Press, 2018: 1-11.

[作者简介]

白杰（1982− ），男，中国移动通信有限公司研究院工程师，主要从事通信网安全研究工作。

黄晓婷（1992− ），女，中国移动通信有限公司研究院项目经理，主要从事通信网安全研究及安全标准化工作。

杜海涛（1978− ），男，博士，中国移动通信有限公司研究院技术经理、正高级工程师，主要从事通信网安全、量子安全、信息安全等研究工作。