工业 5G LAN 网络安全技术报告

工业互联网产业联盟
中国联通研究院
联通数字科技有限公司
2024 年 10 月

声　　明

本报告所载的材料和信息，包括但不限于文本、图片、数据、观点、建议，不构成法律建议，也不应替代律师意见。本报告所有材料或内容的知识产权归工业互联网产业联盟、中国联通研究院、联通数字科技有限公司共同所有（注明是引自其他方的内容除外），并受法律保护。如需转载，需联系本联盟并获得授权许可。未经授权许可，任何人不得将报告的全部或部分内容以发布、转载、汇编、转让、出售等方式使用，不得将报告的全部或部分内容通过网络方式传播，不得在任何公开场合使用报告内相关描述及相关数据图表。违反上述声明者，本联盟将追究其相关法律责任。

工业互联网产业联盟

联系电话：010-62305887

邮箱：aii@caict.ac.cn

目 录

前　言

3GPP 在 R16 中启动 5G LAN 项目研究，意味着 5G 网络具备了广域局域网的能力，为 5G 网络在工业领域的应用提供了新的思路。5G LAN 可以为工业领域提供定制化的专属广域“局域网”，使得工业终端与企业云随时随地处于一个虚拟化局域网中。5G LAN 的优良特性使得 5G 网络在工业领域应用中发挥重要的作用，必将培育出新工业网络应用场景，促进工业企业数字化转型。

工业领域的数字化升级促进了 IT 和 OT 网络融合，也给工业网络带来了严峻安全挑战，如攻击暴露面扩大、攻击路径增多等，原来封闭的生产网络、业务系统开始向外界开放，工厂内部网络、系统等被攻击的概率增加。5G LAN 在继承 5G 网络安全能力的同时，结合局域网特点也诞生了一些独有的核心安全能力。面向工业领域千差万别的安全需求，不仅能形成统一了工厂设备的连接形式，而且能针对不同的业务场景形成有效的网络安全整体解决方案。

本报告考虑工业领域的网络安全需求，结合工业领域 5G LAN 技术的发展和应用情况，总结了 5G LAN 网络安全相关技术，以及有代表性的行业典型案例，为工业领域的 5G LAN 安全技术应用和推广提供参考依据和指导。

总策划：叶晓煜　谢　攀　李浩宇　张建荣

主编：周晓龙

副主编：柳　兴　荆　雷　鲁华伟　谢　云

编委会成员：

王　哲　陶耀东　冯冬芹　井　柯　刘　旸　俞一帆　文　宏

蒋美景　何　凯　陈丽萍　王新宇　李易凡　刘广祺　谢嘉宇

韩江雪　邱　晨　张博文　王竑达　王维治　傅成龙　葛　然

王宝栋　文　雯　范勇杰　徐乐西　吴　冬　崔莹莹　黄继烨

靳冰祎　谢　璟　田慧蓉　王　磊　刘　程　王　舒　乔思远

毛庆梅　李　艺　陈　昕　黄东华　徐书珩　赖羿明　白小愚

指导单位：中国联合网络通信有限公司政企客户事业群

中国联合网络通信有限公司网络与信息安全部

参与单位：中国信息通信研究院

深圳艾灵网络有限公司

奇安信科技集团股份有限公司

北京双湃智安科技有限公司

中智云物联网有限公司

杭州安恒信息技术股份有限公司

兰州兰石爱特互联科技有限公司

普天信息工程设计服务有限公司

天津市工业互联网研究院

浙江大学

北京交通大学

一、5G LAN 简介

5G LAN 是基于 5G 网络的私有移动局域网，由一组 5G 终端组成，通过 5G 网络连接实现相互通信。这种网络连接可以在同一办公区内，也可以在相隔遥远的不同工厂、园区之间。相较 Wifi、4G 等传统技术，5G LAN 可以提供更为安全、高效、灵活的无线局域网服务。

（一）5G LAN 的起源

5G 技术自 2019 年商用以来，正逐渐与工业制造、能源电力、交通、城市管理、教育等各个垂直行业深度融合，这一趋势已经得到广泛认可。目前，行业各方正在紧密合作，探索各种 5G 行业应用解决方案和服务流程，推动 5G 技术的规模商用和进一步发展。

与个人移动应用不同，各个垂直行业对 5G 网络有着各自独特的需求。一些应用场景需要低延时和高可靠性，也有一些应用则需要更大的带宽，还有一些应用场景要求专属网络以确保数据的安全性。因此，不同的应用场景需要不同的技术方案来满足其特定需求。此外，传统通信方式通常采用 TCP/IP 协议来实现终端之间的数据传输，但在垂直行业、特别是工业领域的终端可能缺乏对这些三层网络协议的充分支持，这将导致 5G 网络在垂直行业的应用阻力重重。出于这些需求考虑，5G LAN 的概念应运而生。

3GPP R16 首次提出了“5G LAN-type service”（5G LAN 类型业务），包含“5G Virtual Network group”、“5G LAN Virtual Network”等概念，涵盖了虚拟组管理、虚拟组成员管理、虚拟组会话管理以及

局域网数据交换管理等多项关键技术能力。通过这项技术，可以实现 5G 环境下的虚拟局域网分组管理，更好的应对不同垂直行业需求不同的现状，并且使垂直行业不支持二层通信的顽症得以解决。

（二）5G LAN 的发展

在定义了 5G LAN 的基本功能后，R17 版本又重点针对 5G LAN 的计费进行了研究，提出了组管理事件计费方案。该方案通过对虚拟组的组内、组间等不同计费场景进行计费配置，实现了更灵活的计费方案，为 5G LAN 进一步商用提供了有力支撑。

5G LAN 的标准发展也逐渐完善，其中 3GPP TS 23.501、3GPP TS 23.502、3GPP TS 23.503 分别从系统架构、程序与信息流和策略与计费控制对 5G LAN 进行了研究。IEEE 802 系列标准中 IEEE802.11ax（Wi-Fi 6）、IEEE 802.1Q（VLAN）、IEEE 802.3（以太网），虽不是 5G 标准，但可与 5G 结合形成更强大的网络解决方案，用于实现 5G LAN 的目标。

目前 R18 版本已经冻结。R18 完善了 5G LAN 管理方面的能力：

（1）组成员流量特征实时监控。通过该能力，可以让工业用户通过业务量获得更多的工控系统实时统计数据，从而更好地了解网络和业务的实时状态，监控系统运行状态，及时完成性能分析和故障排除。

（2）跨 SMF 管理 VN Group。该功能可以有效解决 R16“一个 VN Group 只能被一个 SMF 管理”的问题。在当前 SMF 出现故障时自动切

换到其他可用的 SMF 上，从而保证整个 VN Group 的运行不受影响，为工业用户带来更加可靠和高效的网络服务。

（3）跨 VN Group 通信。在 R16 中，跨组通信存在很大的局限性，R18 的方案可以解决该问题，帮助用户将多个群组连接起来，建立范围更大的网络。

（4）组管理和组状态上报增强。该特性可以帮助工业用户实现对组内用户和业务流的精细化管理，提高包括用户认证、权限管理、QoS 控制等方面的灵活性与可靠性。

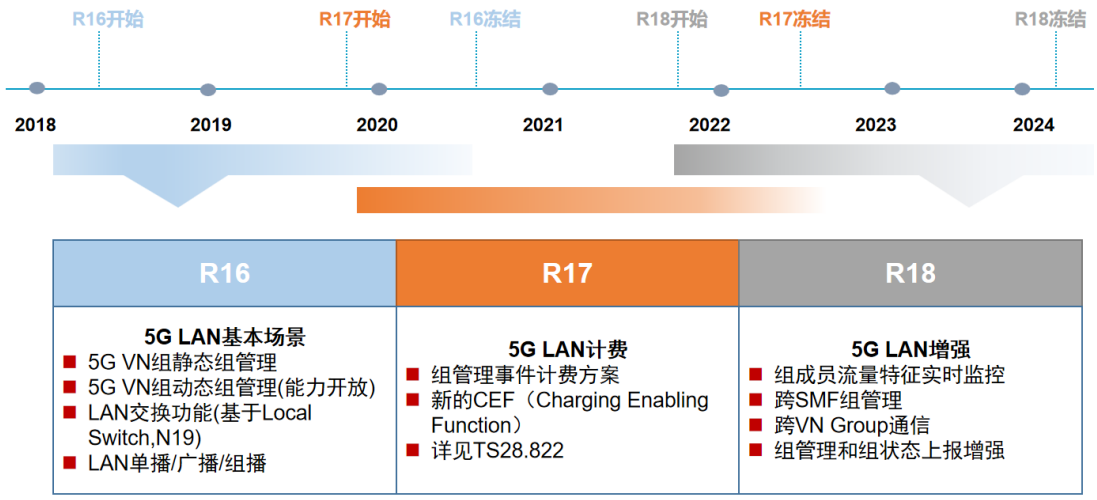

图 1.1 5G LAN 技术演进图

（三）5G LAN 的优势

5G LAN 兼顾移动通信网和无线局域网的优点，可满足复杂多变的通信需求，具体如下：

（1）良好的基础性能：5G LAN 以 5G 无线技术为基础，继承了 5G 无线技术大容量传输数据、大规模设备连接、超高可靠低延迟（uRLLC）可满足生产制造、远程控制等垂直行业对网络带宽、实时

性和精确性要求极高的应用场景。较工业 Wi-Fi，5G 的覆盖范围更广、小区间切换更流畅、运维服务更具标准体系化，可给用户带来更好的网络体验。

（2）优秀的工业适配：5G LAN 解决 5G 系统本身不支持二层通信的难题，具备直接进行二层通信的能力，可以与用户已有数据网络进行连接，实现即插即用和相互访问，省去了引入 AR 的步骤，大大降低了 5G 网络的改造难度，方便工业终端的 5G 无线接入。

（3）灵活的组网方式：5G LAN 具备数据网络组网、本地组网和远程组网三种数据转发能力，既能满足同一个 PSA UPF 下的工厂终端通信，又能满足不同 PSA UPF 下的工厂终端通信，可以帮助工厂终端设备通信灵活组网，同时支持二层数据交换和三层数据交换，具有较高的数据转发效率。

（4）支持广播与多播：5G LAN 支持 UPF 的双检测转发机制，提供类似于以太交换机的数据处理与转发功能，实现终端间的数据转发，可以满足组播、广播的通信需求。UPF 通过检测终端的目的地址并添加路由，在传统上、下行数据转发的能力之上，实现单 UPF、跨 UPF 的终端间的广播、多播，可满足工业终端的多样性通信需求。

二、5G 网络安全关键技术

5G LAN 是建立在 5G 终端接入能力和 5G 网络之上的私有移动 LAN 服务，通过建立“群”，为企业内部终端提供灵活的通信服务，包括终端互通和终端隔离等。**5G LAN 技术是一种基于 5G 的局域网技术，它提供了高速、低时延和高可靠的网络连接，可以支持实时数据传输和网络控制。5G LAN 安全具备多项技术能力，不仅继承了 5G 本身的安全技术，更加具备增强的网络安全技术能力**。本章主要介绍 5G 本身的安全技术。

（一）5G 接入认证安全技术

1、统一安全认证框架

5G 支持多种接入技术，为了更好的支持不同应用场景、不同设备接入 5G 网络，使得用户可以在不同的接入网间实现无缝切换，5G 网络采用一种统一的认证框架，实现灵活、高效地支持各种应用场景下的双向身份鉴权，进而建立统一的认证体系。可扩展认证协议（EAP）认证框架，能够满足 5G 统一认证需求。EAP 认证框架，是一种支持多种认证方法的认证框架，框架本身不提供任何安全性，只规定了消息的封装格式，具体的安全目标依赖于使用的认证方法。

2、基于证书实现用户身份信息保护

在 5G 网络中，每个用户都有一个用户永久身份标识。如果该身份信息在空口暴露，可能出现固定用户进行位置跟踪等安全事件，从而侵犯用户隐私。5G 系统中引入了基于公钥体系的加密机制，对 SUPI

进行加密形成 SUCI，在空口中传递 SUCI 以全面保证用户的隐私在空口不泄露。为支持 SUCI 的计算，首先 SIM 卡需在生产过程中预置运营商公钥，需采用安全方式（如专线、VPN 等方式）将公钥数据传输给供卡商制卡；在用户开机登网等场景下，需要传递 SUPI 时，通过 SIM 卡中的归属网络公钥对 SUPI 进行加密生成密文 SUCI 用于在空口中传输，从而更加有效地保护用户的隐私。在产生 SUCI 时，需要利用 USIM 中预置的归属运营商公钥、采用 ECIES 对 SUPI 进行加密运算，并且根据算法原理，每次使用时产生的 SUCI 也不相同。因此攻击者无法根据 SUCI 推算出 SUPI，也无法利用 SUCI 长时间对用户进行探测，进而无法针对用户进行持续性的跟踪。

3、基于零信任的接入认证技术

零信任体系保障终端可信、通道可信、身份可信，并提供持续信任评估与行为监测能力。对于身份可信，可以通过 IAM 实现身份管理、认证鉴别、权限管理和访问控制，融合零信任智能多因子认证，支持多种认证模式，包括客户端私有密钥、设备指纹、IP 地址、生物身份等。IAM 通常采取集中部署模式，基于 5G LAN 的部署架构，可以按需实施分层部署。对于持续信任评估与行为监测，通过行为记录和审计等方式，持续监控用户行为。针对终端安全事件、违规越权行为、潜在威胁、文件泄露、系统漏洞等状态，及时调整身份认证和访问控制策略。

（二）5G 数据安全保护技术

1、5G 数据加密技术

5G 网络上面承载着很多用户的隐私和敏感信息，需要采用技术措施解决 5G 网络的隐私保护问题。数据加密是 5G 网络中保证数据隐私安全的常见手段，按照实现思路，可以分为静态加密技术和动态加密技术。在实现的层次上，可以分为存储加密，链路层加密、网络层加密、传输层加密等。采用加密技术可以有效保证 5G 网络数据的机密性、完整性和可用性。针对 5G 网络虚拟化和云化的新特点，可以引入一些新的加密技术来保证数据的隐私安全，如同态加密技术。同态加密技术对加密的数据处理得到输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的结果相同。

2、5G 数据防护技术

5G 网络在空口为用户面数据增加了可选的完整性保护功能。在用户需要新建会话时,由核心网根据用户配置信息中的用户安全策略向基站发送无线链路配置消息来告知终端是否启用用户面完整性保护。5G 使用 SEPP 设备进行网间安全保护。SEPP 间的安全传输定义了两种安全保护的机制:一种是基于传输层协议的安全保护机制,即 TLS。这种机制将会导致中间转接商 IPX 失去对信令调整的能力。另一种是基于应用层协议的安全保护机制。这种机制可以灵活的对多个应用层数据集合采用不同的安全保护策略，从而实现了在 SEPP 之间的安全传输，同时也为 IPX 获取相关信息或修改相关信息留下了空间。

3、5G 工业流量防护技术

针对工业应用，采集和分析工业协议的流量，针对加密流量采用非监督学习和监督学习结合的方式，从网络流量特征、协议、流量大小、业务时间、业务操作行为等多维度建立合规基线模型，然后实时对比、分析从而发现数据安全风险事件；针对非加密协议可对操作数据内容、传输文件内容进行还原，利用大数据分析、机器学习等技术建立用户画像、业务画像、数据安全合规基线等，实现批量传输敏感数据、数据跨境传输、接口异常访问敏感数据、接口未授权等安全场景的实时监测与风险事件溯源分析，确保 5G 智能制造行业的应用与数据安全。

（三）5G 网络切片安全技术

1、切片安全隔离技术

5G 网络切片是一组运行在通用物理硬件上的多个 NF 的编排组合，具有独立提供网络服务能力的端到端虚拟网络。由于网络切片共享相同的网络资源，因此切片之间的安全隔离非常重要，做好网络切片的端到端隔离，一方面可以避免切片之间发生资源相互竞争而影响切片的正常部署和运行，另一方面可以避免一个切片的异常（如遭受内部安全威胁或者攻击，影响其他切片的安全），有效防止攻击扩散、切片数据泄露等安全威胁。网络切片是端到端虚拟网络，是由无线接入、承载、核心网构成，因此网络切片端到端的隔离包括切片在接入网、承载网和核心网的隔离实现。

2、切片接入安全技术

用户接入切片的认证能力是在终端接入网络时由 5G 网络执行接入认证来保证接入 5G 网络用户的合法性的基础上，3GPP 还提供了运营商、切片客户配合完成切片认证和授权的机制，保证仅合法用户可接入切片，实现垂直行业对切片网络及资源使用的可控性。切片选择辅助信息及隐私保护能力时在 NSSAI 可以区分不同类型、不同用途的切片。在用户初始接入网络时，NSSAI 指示基站及核心网网元将其路由到正确的切片网元上。切片选择辅助信息对于垂直行业属于敏感信息，5G 网络提供标准的机制，可对传输中的 NSSAI 进行隐私保护。

3、切片管理安全技术

切片的管理安全包括两个部分，一是通过管理手段保证切片的可用性；二是保证切片管理过程的安全。针对切片的可用性，切片管理系统提供实时的切片安全监控、应急处置以及故障恢复能力，实时掌握切片的运行情况、可能的被攻击情况及故障状况，通过联动对应的安全设备进行处置，并及时对故障进行修复，从而保障系统的可用性。针对切片管理过程的安全，一方面是管理信令的安全保护；另一方面是切片生命周期管理和维护管理。为了保障切片管理的安全，要设置相应的安全保护机制。

（四）5G 网络安全增强技术

1、5G 网络安全态势感知

传统网络基于 IP 的单一化寻址路由机制已经难以适应目前 5G 网

络承载的多样化业务需求，缺乏数据传输安全能力以及对终端行为的感知能力。人工智能技术以 SDN 和 NFV 技术为基础，实现控制层面与传输层面的能力解耦。基于实时更新优化的智能路由模型，可实现对于网络整体态势的实时感知，配部署网络安全传输设备，建立智能化安全防护模型，形成针对用户的恶意访问行为的精确感知，从而构建一个集网络安全态势感知、数据安全智能路由、恶意行为告警及网络安全防护功能于一体的传输网络安全体系，从根源上杜绝如分布式拒绝服务攻击等恶意行为对 5G 网络造成的安全隐患。

2、5G 终端行为感知与管控

相比于传统网络，为满足物联网、车联网以及智慧城市等应用环节的网络能力需求，5G 网络在 mMTC 场景下需支持每平方千米 100 万用户的接入数量，超大规模的终端接入能力必定伴随着由挟持终端发起的 DDoS 攻击的风险。因此，终端行为的感知与管控能力是 5G 网络 mMTC 场景下必不可少的安全防护能力。通过在网络侧收集终端用户的行为信息，充分利用机器学习技术针对多源数据的辨识能力，训练一个具备识别用户实时状态的终端行为的管控模型，从而在网络侧形成针对终端异常或恶意行为的感知、识别、管控的一体化能力，进一步提升 5G 网络的运行效率，增强网络的可靠性。

3、区块链助力 5G 数据安全

5G 网络使得网络速度提升，数据量随之高速增长，对数据的安全性保护和隐私性提出了更高的要求。区块链的分布式、自组织特性，

可用于构建数据共享、分散协作、去中心化的松散的生态环境，其用密码学的手段为交易去中心化、隐私信息保护、历史记录防篡改、可追溯等提供技术支持，天然适用于对数据保护要求严格的场景，同时，区块链去中心化也为网络资源共享提供了新的解决思路。以区块链为代表的应用密码技术将为网络重构安全边界，建立设备间的信任域，实现安全可信互联。同时，终端去隐私化的关键行为信息上链后，即会分布式存储在区块链各节点中，保证数据的安全性和可用性，促进构建智能协同的数据安全防护体系。

三、5G LAN 安全防护关键技术

5G LAN 的二层组网功能可以提供更加灵活、高效和安全的网络连接方式，符合工业领域对网络的要求。它可以使用虚拟局域网（VLAN）来实现逻辑隔离和网络划分，从而满足不同的应用需求。此外，5G LAN 还可以支持多个广播域和多个网段的划分，以便更好地管理和控制网络。5G LAN 安全防护关键技术在网络中的位置具体如下图：

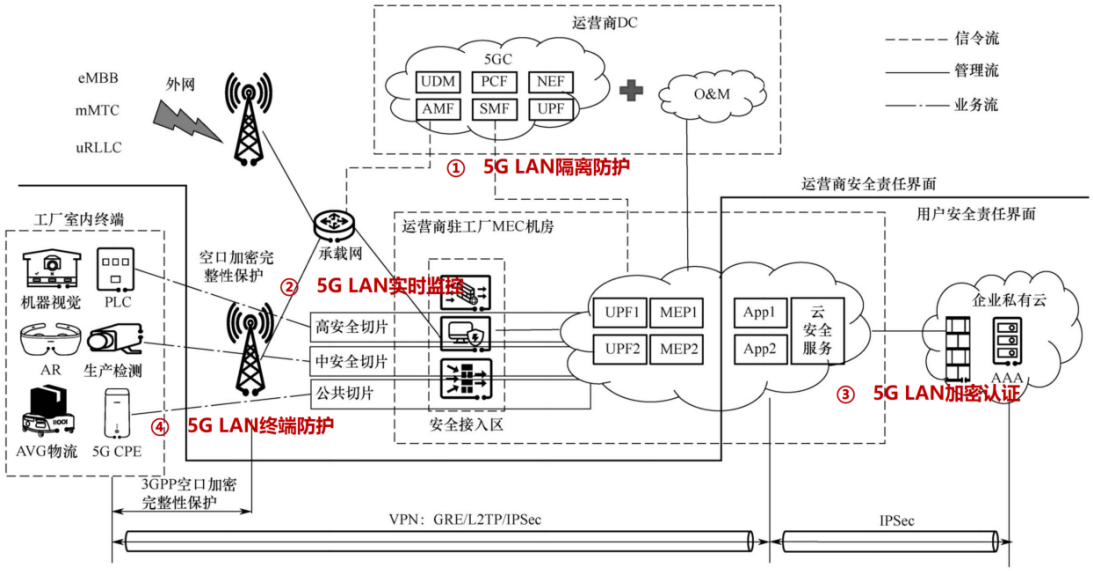

图 3.1 5G LAN 安全关键技术全景图

（一）5G LAN 隔离防护技术

跨 SMF 管理 VN Group 可以有效地解决一个 VN Group 只能被一个 SMF 管理的问题，该问题会导致容灾能力不足，一旦该 SMF 出现问题，整个 VN Group 都会受到影响。跨 SMF 管理 VN Group 能够使得多个 SMF 可以同时管理一个 VN Group，从而提高了系统的可用性、容灾能力和稳定性。在 SMF 出现故障时自动切换到其他可用的 SMF 上，从而保证整个 VN Group 的运行不受影响，为工业用户带来更加可靠和高效的网络服务。

基于 5G LAN 的工业互联网承载多个业务系统，应按照业务相对隔离、信息按需互通的原则进行各子网的设计。在网络层面，保证不同的业务系统部署在独立的 VLAN 中，同时划分不同的安全域，各安全域之间采取边界防护措施，保证各业务系统和子网的独立；在应用和数据层面，各业务系统采取身份认证、访问控制等措施阻止非法访问，保持应用和数据的独立性。

5G LAN 边缘组网隔离包含三平面隔离和安全域划分。三平面隔离是指服务器和交换机等应支持管理、业务和存储三平面物理/逻辑隔离。对于业务安全要求级别高并且资源充足的场景，应支持三平面物理隔离；对于业务安全要求不高的场景，可支持三平面逻辑隔离。安全域划分是指 UPF 和通过 MP2 接口与 UPF 通信的 MEP 应部署在可信域内，和自有 APP、第三方 APP 处于不同安全域，根据业务需求实施物理/逻辑隔离。 另外，可通过特定的技术确保网络安全，如 N4 流量采用 IPSec 等技术建立安全通道、开启防地址欺骗策略防止 UPF 上、下行流量中的地址欺骗、在物理端口执行 ACL 过滤策略、通过 URL 黑名单方式对 WAP 推入的恶意消息拦截过滤、通过 GRE 等隧道对不同业务类别流量进行控制和隔离、在 UPF 公网侧部署抗 DDoS 设备等。

（二）5G LAN 实时监控技术

组成员流量特征和性能监控对于工业用户来说非常重要，因为他们对网络和业务的运行状态更加关注。这意味着在 5G 网络中，工业用户可以获得更多的业务流和性能统计数据，从而更好地了解网络和

业务的实时状态。此外，5G LAN 还支持实时性能监控和告警，以及高级的日志分析和故障排除功能，这些功能可以提高网络的可靠性和稳定性。总的来说，5G LAN 为工业用户提供了强大的网络管理和监控工具，以确保他们的业务能够顺利运行。

性能监控和告警功能可以及时发现网络中的异常行为或安全威胁。5G LAN 提供高级的日志分析和故障排除功能，帮助管理员深入了解网络的运行情况和潜在的安全问题。通过分析日志数据，可以发现潜在的安全漏洞或攻击行为，从而采取相应的防范措施。

通过设置部署网络安全态势感知探针，实时监测网络安全状态，识别异常流量，及时发现网络攻击行为，提供实时的预警和报警信息，帮助用户及时采取安全措施，保障信息系统的安全。还可通过安全管理中心进行全系统安全态势的集中统一管理，及时识别网络攻击，采取有效的应对措施。

（三）5G LAN 加密认证技术

5G LAN 借助于 5G 技术的加密与认证机制，能够提供更高级别的安全保障。这包括使用强加密算法对数据进行加密传输，以及使用认证机制对终端进行身份验证，确保只有授权终端可以接入网络。

对于接入 5G LAN 网络的终端设备采用接入认证，防止 5G 公网终端非法接入 5G LAN 网络。可采用的措施包括：独立建设用户 AAA 设备，让企业自行管理 5G LAN 的用户，只有在企业 AAA 设备中的合法用户才能接入 5G LAN 网络；在 5G LAN 网络中对接入终端进行二次

认证，采用企业自主可控的二次认证方案和设备，只有通过二次认证的终端才能接入 5G LAN 网络，防止非法用户接入。

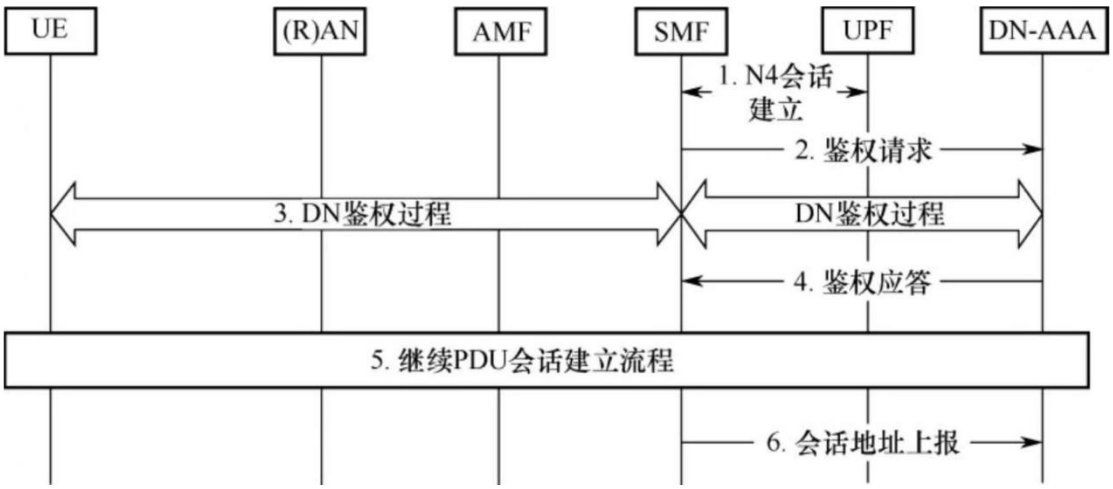

图 3.2　5G LAN 的二次认证流程

（四）5G LAN 终端防护技术

5G LAN 技术允许在 LAN 内为 5G 终端提供终端互通或终端隔离等灵活的通信服务。通过设置访问控制策略，可以限制不同终端之间的通信，减少潜在的安全风险。在基于 5G LAN 建立的工业互联网系统中，各种设备需采用安全措施提升自身的安全。

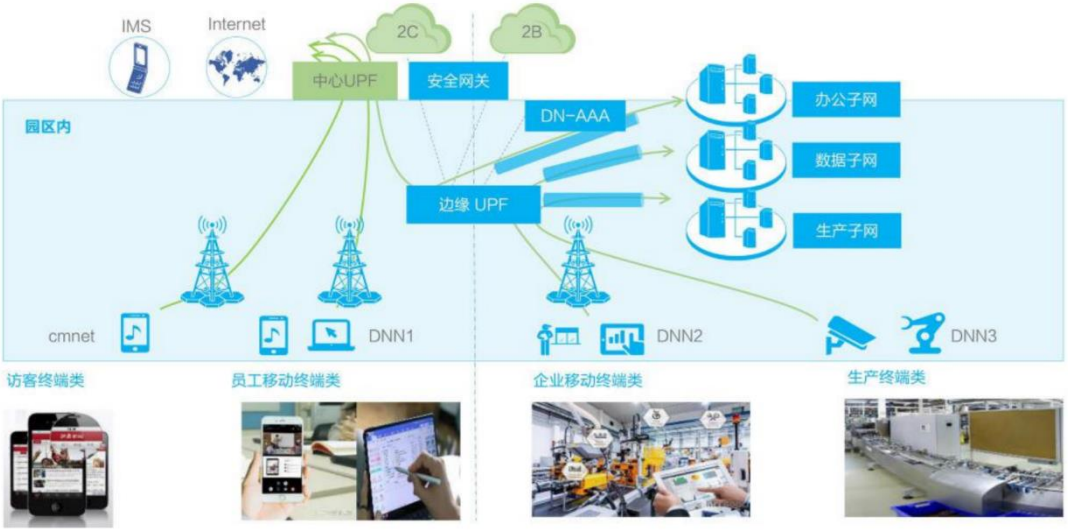

图 3.3　5G LAN 基于用户的终端隔离防护

安全防护的重点是数量众多的终端设备，以防止病毒、木马通过终端设备侵入系统为主要保护目标，采取的主要措施：减少不必要的功能和应用，操作系统和应用软件都遵循系统最小化原则；应用基于“白名单”和“黑名单”相结合的防护技术，在系统稳定运行后通过规则匹配、深度学习等方法自主建立合法的“白名单”，在没有特征库的情况下也能发现病毒和网络攻击等异常情况；使用端口管控工具控制外部移动设备的接入，并对所有接入的移动存储设备进行审计。

四、典型案例

（一）工业 5G LAN 数据安全管理应用案例

1、背景

工业控制网络是工业生产的“核心大脑”，用于监控、管理工业生产过程中的智能终端设备，确保生产的稳定性和可靠性，提升生产效率，在关键信息基础设施领域得到广泛应用。为适应新时期工业控制系统网络安全形势，进一步指导企业提升工控安全防护水平，夯实新型工业化发展安全根基，2024 年工信部印发《工业控制系统网络安全防护指南》，使用、运营工业控制系统的企业适用本指南，防护对象包括工业控制系统以及被网络攻击后可直接或间接影响生产运行的其他设备和系统。

5G 与工业互联网的深度融合，大量工业设备接入网络，由于工控设备安全防护相对薄弱，存在被非法访问控制的风险，导致生产中断或设备损坏。需进一步提升工业企业的工控安全保证能力，保护工业设施免受攻击，在石油化工、汽车、智能制造等工业领域，满足工业 5G LAN 网络中数据加密传输、身份认证、数据安全等需求。

中国联通联合中智云物联网打造工业 5G LAN 数据安全测试床，面向工业领域由于工控系统老旧、系统性能低、无法与互联网通讯、无有效的安全维护人员和体系等情况导致在 IT 领域使用的身份认证技术措施无法直接应用到工业控制领域的问题。针对 5G+工业互联网场景对工业数据安全的迫切需求，提出了一套针对工业领域全链路数

据安全防护的技术方案。

2、应用场景与需求

在工业互联网场景下，数据在采集、传输和存储过程中面临着安全风险。如果数据被恶意获取或泄露，可能导致用户隐私曝光，损害用户信任和企业声誉。若第三方机构或合作伙伴参与数据共享和处理，一旦数据共享失控或处理出现错误，可能会引发法律责任和用户隐私泄露的风险。

工业企业在数字化转型过程中面临的数据泄露风险，恶意攻击风险、数据传输风险、安全防护能力不足等数据安全问题。工业互联网领域中的数据安全保护涉及多个关键环节。首先，访问控制与身份验证构成确保仅授权端到端能够接触数据。其次，数据加密与隐私保护技术构成保障端到端数据机密性和隐私安全。最后，采用高级加密手段对信息实施安全编码，确保数据在传输和存储过程中不会被未授权访问或篡改。

本案例通过工业 5G LAN 满足云、管、端数据传输安全、身份认证等方面的安全需求，提升主机身份鉴别、网络设备安全接入、用户认证、传输加密等安全能力。

3、解决方案

5G-LAN 功能场景:网络规划方案 5G-LAN 组网架构支持二层组网，不同的 UPF 进行 5G-LAN 组网后，相互之间可直接进行通信，完成 5G-LAN 组网架构后，可实现如下功能：