5G网络ToB视角下的接入网安全部署策略研究

Research on Access Network Security Deployment Strategy from Perspective of 5G ToB Network

骆　润，李宗林（中国移动通信集团设计院有限公司陕西分公司，陕西 西安 710069）
Luo Run，Li Zonglin（China Mobile Communications Group Design Institute Co.，Ltd. Shaanxi Branch，Xi'an 710069，China）

摘　要：
通过对5G网络在垂直行业（ToB）应用部署中不同企业对自身网络数据安全及接入终端的需求分析的梳理，分析了基于安全需求组网的架构要求关键点，结合5G网络的特性，对传统的PLMN、cell bar、TAC技术点进行分析，对3GPP R16中针对垂直行业增强的非公众网络（NPN）技术进行探讨，给出针对不同企业安全管理需求的网络安全部署策略。

关键词：
5G；ToB；接入安全；部署策略
doi：10.12045/j.issn.1007-3043.2021.04.013
文章编号：1007-3043（2021）04-0061-05
中图分类号：TN929.5
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
It combs the requirements of different enterprises on their own network data security and access terminals in the deployment of 5G network in ToB（vertical industry），and analyzes the key points of the architecture requirements of network based on security requirements. Combined with the characteristics of 5G network，it analyzes the traditional PLMN and cell Bar and TAC technology，discusses the enhanced NPN（non public network）technology for vertical industry in 3GPP R16，and puts forward a network security deployment strategy for different enterprise security management needs.

Keywords：
5G；ToB；Access security；Deployment strategy

引用格式：骆润，李宗林. 5G网络ToB视角下的接入网安全部署策略研究[J]. 邮电设计技术，2021（4）：61-65.

1 概述

1.1 5G网络安全概述

2010年国际电联定义了5G的三大应用场景：eMBB、mMTC、uRLLC。2019年部署商用的为5G的第1个版本，主要满足eMBB的需求，随着2020年5G网络的推进，满足SA能力的5G网络蓄势待发。SA的强大能力，带来了越来越多的垂直行业的支撑能力，5G网络在医疗、教育、港口、工业园区、银行、电厂、钢厂、矿山等行业得到了示范性的应用，随着越来越多的行业对5G网络的应用，面向安全的诉求也随之而来。

5G安全既包括由终端和网络组成的5G网络本身通信安全，也包括5G网络承载的上层应用安全。《5G系统安全架构和流程》（3GPP TS 33.501）中规定：在安全分层方面，5G与4G完全一样，分为传送层、归属层/服务层和应用层，各层间相互隔离；在安全分域方面，5G安全框架分为接入域安全、网络域安全、用户域安全、应用域安全、服务域安全、安全可视化和配置安全等6个域。

1.2 企业ToB网络安全需求分析

随着5G深入千行百业，5G与垂直行业深度融合，行业应用服务提供商与网络运营商、设备供应商一起

收稿日期：2021-03-01

形成了新的网络格局，网络从网与人拓展到网与物、网与系统（人和物协同的群体），网络安全呈现出2个方向：一是5G网络安全、应用安全、终端安全问题相互交织，互相影响，行业应用服务提供商由于直接面对用户提供服务，在确保应用安全和终端安全方面承担主体责任，需要与网络运营商明确安全责任边界，强化协同配合，从整体上解决安全问题，移动通信网络从传统的IT封闭性引入了开放性，对于网络的开放，对于接入外部网络接入点的安全管控是需要在网络部署时务必考虑的工作内容；二是不同垂直行业应用存在较大差别，安全诉求存在差异，安全能力水平不一，难以采用单一化、通用化的安全解决方案来确保各垂直行业安全应用。企业对数据接入安全管控需求包含区域类数据安全（如整体园区数据本地化、区域的接入用户安全管控问题，园区/非园区用户的识别）和特殊区域的接入保密问题（如核心生产区域各类别的UE接入的管控、控制面安全问题等）。本文重点分析不同垂直行业在接入网数据及管控在安全方面的需求及解决策略方案（见表1）。

表1　企业5G接入网络安全需求

安全要求	接入管控	数据安全
低	无	无，可独立监控数据
中	对于整体区域做限制，非合法用户禁止接入	用户面数据在本地管理
高	对于整体区域的接入UE分层级，不同区域有不同的安全管控要求	用户面数据在本地管理，整体区域内存在数据隔离需求

2 5G网络部署架构与接入安全分析

2.1 5G网络部署架构

5G网络采用SBA架构，SBA架构适用于5G核心网信令面，传统网元间点对点双向接口被单向服务接口取代，一个网元提供的服务理论上可以被任何其他网元（甚至非网元）调用。信令面管控由SBA架构实施；5G网络的数据面5G核心网的会话管理功能主要由SMF（Service Management Function）负责，主要和AMF、PCF、UDM、CHF以及终端、基站进行信令交互，并和UPF（User Plane Function）共同完成用户面管理和执行的功能。图1给出了5G网络架构示意图。

服务化接口包括N11、N7、N10和N40。N11负责基本会话管理、位置订阅等；N7负责会话级的策略管理；N10负责5G新增的连接关系、会话级的用户数据管理；N40负责会话级的计费信息传递。

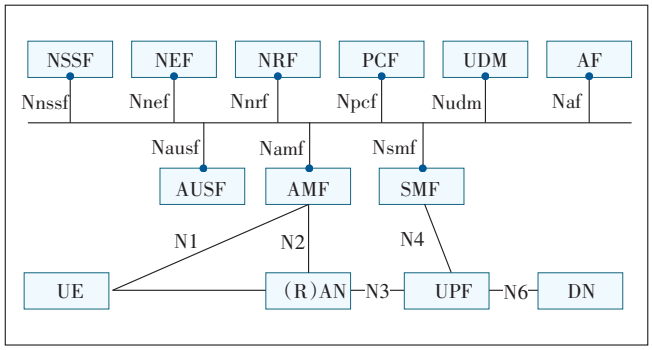

图1　5G网络架构图

非服务化接口包括N4、N1、N2和N3。N4负责和UPF交互，采用PFCP协议，传递会话的策略、流量等相关信息；N1负责和终端交互，传递5G会话相关的NAS消息，通过N11接口透传；N2负责和基站交互，传递5G会话相关的NG-AP消息，通过N11接口透传；N3负责和基站交互，采用GTP-U协议，传递数据。

5G核心网中SMF对应4G核心网的MME会话管理相关功能和SGW-C、PGW-C的功能，除支持IPv4、IPv6和IPv4v6会话类型外，还可支持非IP类型（Ethernet和Unstructured）的PDU会话，用户注册时可不建立PDU会话，只有业务开始时才建立，PDU会话属性在生命周期内均不能改变。

众所周知，5G引入了3种业务分流方式：上行分流（Uplink Classifier）、多归属（Multi-homing）和本地数据网络（LADN）。

a）Uplink Classifier的分流方式通过为目的地址不同的业务流选择不同的UPF，以实现就近接入，卸载本地流量。此功能支持单IP，UE对分流无感知，SMF根据需要插入或删除ULCL的UPF，ULCL的UPF解析上行数据包的5元组，根据SMF提供的上行分流规则向不同的PDU会话锚点UPF转发上行业务流，并将来自链路上的不同PDU会话锚点UPF的下行业务流合并到UE，一个PDU会话可以有多个ULCL，但是只有1个ULCL可以通过N3接口连接AN（接入网）。

b）Multi-homing的分流方式主要为单PDU会话中不同IPv6地址前缀的业务选择不同的UPF。仅支持IPv6，UE有感知（涉及到UE能力，需要UE支持），在上行包中携带不同的IPv6前缀，SMF根据需要插入或删除分流点UPF（BP UPF——Branching Point UPF）。BP UPF将不同IPv6前缀的上行业务流转发至不同的PDU会话锚点UPF，并将来自链路上的不同PDU会话

锚点UPF的下行业务合并到UE。

c）LADN的分流方式主要针对访问固定的本地数据网络的业务，为其选择就近的UPF以卸载流量。LADN的业务区是TA的集合，LADN的信息（如LADN业务区、LADN DNN）配置在AMF上，SMF配置DNN是否为LADN DNN，UE需支持配置DNN是否为LADN DNN。

从5G的架构和基本功能上可以看出，在用户接入和用户面的数据管理上，5G网络对业务的安全存在多种灵活的方式。

2.2 从传统移动通信网角度分析接入安全

2.2.1 PLMN

PLMN是由政府或其所批准的经营者为公众提供陆地移动通信业务而建立和经营的网络。该网络必须与公众交换电话网（PSTN）互连，形成整个地区或国家规模的通信网。PLMN = MCC + MNC，例如中国移动的PLMN为46000，中国联通的PLMN为46001。对于一个特定的终端来说，通常需要维护几种不同类型的PLMN列表，每个列表中会有多个PLMN。不同类型的PLMN的优先级不同，终端在进行PLMN选择时将按照以下顺序：RPLMN、EPLMN、HPLMN、EHPLMN、UPLMN、OPLMN，其他的PLMN。一般来讲，UE开机，进行全频段扫频，解调PSS/SSS，接收MIB/SIB，在SIB消息中可以获知当前小区的PLMN，然后与SIM卡中的PLMN做匹配。一致则驻留，不一致则进行新一轮的扫描，直到一致为止。理论上可以对限制接入的小区配置专用的PLMN，普通的UE就无法接入，从而实现用户的接入安全限制，但实际上PLMN数量有限，无法进行全面宏观地针对全行业分类，在现阶段的实践中不能落地。

2.2.2 CELL BAR

无线接入控制是一种针对话务拥塞的处理机制。通过限制移动设备向基站的连接请求，保护和保证紧急呼叫等关键通信的成功接入。

在5G（NR）中MIB消息中包含“小区禁止”和IE cellBarred小区限制信息，这些信息通过“禁止”或“不禁止”值广播。这个标识允许终端提早检测状态，而不需要接收和解码SIB1。如果一个小区被禁止，那么UE就不允许选择或重选该小区。小区频率限制：如果MIB表示某个小区被禁止，那么UE还将检查同样包含在MIB中的（同频重选）intraFreqReselection标志。如果此标志设置为“notAllowed”，则不允许重选到同频的另一个小区。否则，如果此标志设置为“允许”，则允许UE进行同频（小区）重选。5G（NR）SIB1中有一个“保留给操作员使用”的字段取值为“保留”或“不保留”。如果一个小区被”保留”，那么一个接入等级为11（PLMN Use）或接入等级15（PLMN Staff）的用户可以在该小区接入和重选，该类用户一般位于HPLMN或EPLMN的小区内或相同小区内。如果一个小区被“保留”，那么接入等级为0、1、2、12、13或14的UE将该小区视为“禁止”，不允许接入或重选。

在无线侧，CELL BAR功能可以做一定的接入限制，主要是禁止小区选择和重选接入UE，但是UE可以从别的小区切换过来。CELL BAR暂无法实现特定用户的接入限制。

2.2.3 TAC

跟踪区（TA）被定义为UE不需要更新服务的自由移动区域。TA功能为实现对UE位置的管理，可分为寻呼管理和位置更新管理。UE通过跟踪区注册告知核心网自己的跟踪区TA，当UE处于空闲状态时，核心网络能够知道UE所在的跟踪区，同时当处于空闲状态的UE需要被寻呼时，必须在UE所注册的跟踪区的所有小区进行寻呼。TA是小区级的配置，多个小区可以配置相同的TA，且一个小区只能属于一个TA。针对不同区域可以设置不同的TAC，在核心网侧做接入限制（核心网侧白名单设置，可在MME、AMF上做白名单设置），实现不同区域的用户接入限制。也可以使用切片ID（NSSAI）+TAC做区域白名单限制，管控区域内的用户接入。

3 基于R16的NPN网络接入安全能力分析

3GPP将5G专网分为3类，分别是非公共网络（NPN——Non-Public Network）、5GLAN和时间敏感网络（TSN），本文主要针对NPN网络进行分析和阐述。

NPN是区别于电信运营商公网，为特定用户/组织提供服务的网络，在3GPP TS 23.501的定义中，非公共网络有以下2种类型。

a）独立组网的NPN网络（SNPN——Stand-alone NPN），即独立专网，该网络不依赖于公网（PLMN网络），由SNPN运营商运营（非运营商的网络，例如政府专网、企业专网）。

b）非独立组网的NPN网络（PNI-NPN——Public network integrated NPN），集成于公网的专网，该网络依赖于公网（比如5G网络），由传统运营商运营。

对于PNI-NPN，如果只使用3GPP R15中定义的网络切片，则无法进行访问控制，需要启用受限访问组（CAG——Closed Access Group）去阻止未授权终端接入。

不论是SNPN还是PNI-NPN，NPN都可以实现端到端的资源隔离，为垂直行业或特定群体用户提供专属接入，限制非授权终端接入专属基站或频段，保障客户通信资源独享。

5G NPN是利用5G技术构建的独立于服务大众的PLMN网络的专网。5G NPN支持2种部署模式，即NPN独立部署（实现上不依赖于PLMN的任何网络功能）和公网集成部署（依赖于公网的实现）。

3.1 PNI-NPN网络接入流程分析

首先，可以由PLMN ID和CAG ID来确定一个CAG，用户和CAG的关系与签约类似，启用了CAG的小区只允许签约用户接入。用户在签约CAG时会在订阅信息中配置2个信息，一个是该用户支持的CAG列表（Allowed CAG list），该列表存储当前用户所能接入的全部CAG小区的ID，另一个是该用户是否只能通过CAG小区接入网络的标识（CAG-only indication），配置了该标识的用户只能通过CAG小区接入网络。

初始接入和小区重选过程中，NG-RAN node需要广播自身支持的CAG ID和相应的PLMN ID信息（每个NG-RAN node最多广播12个CAG ID），未配置CAG-only indication的CAG用户可以根据自己的Allowed CAG list选择可接入的CAG小区，也可以选择订阅的公共PLMN小区接入网络。配置了CAG-only indication的CAG用户只能根据自己的Allowed CAG list选择可接入的CAG小区接入网络。核心网可以根据用户的订阅信息对用户的身份进行鉴权。

由于PNI-NPN依赖于PLMN的网络功能，因此对于未配置CAG-only indication的用户应支持PNI-NPN和PLMN网络间的切换。其中从CAG小区到PLMN小区的切换需要基站或者核心网确认用户是否配置了CAG-only indication。从PLMN小区到CAG小区的切换需要基站或者核心网判断目标基站的CAG ID是否在用户的Allowed CAG list中。

未配置在相应Allowed CAG list中的用户无法进行网络访问。

PNI-NPN依赖于PLMN，结合CAG ID实现对PLMN的拓展，可以实现不同用户访问的隔离，但应对CAG的划分做充分的分析。

3.2 SNPN网络接入流程分析

独立部署的NPN，用PLMN ID和NID（Network identifier）的组合标识，PLMN运营商可以重用其PLMN ID，同时使用NID区分各个专网，或者使用为专网预留的PLMN ID。SNPN的RAN将广播PLMN+NPN ID。SNPN的UE用SUPI标识，如果UE设置为SNPN接入模式，则该UE只能通过Uu接口接入并注册到SNPN。UE初始注册时，会带上PLMN ID和NID，NG-RAN将这些信息带给AMF。用户在NPN中的签约信息包括了统一接入控制（UAC——Unified Access Control）信息，在网络拥塞时，SNPN可以阻止UE接入。

已在SNPN注册的UE可以通过SNPN接入PLMN的非3GPP互通功能（N3IWF——Non-3GPP Interworking Function），从而访问PLMN的服务。这时，UE需要同时向PLMN注册。SNPN对于PLMN来说，相当于非可信non-3GPP接入的角色。对于网络触发的QoS保障请求，SNPN根据SLA合约从NWu接口的DSCP（Differentiated Services Code Point）字段中映射SNPN所要求的QCI并予以执行，同时使用NWu接口的N3IWF IP地址和DSCP字段标识设置其包检测过滤器。对于UE请求的QoS，UE使用与SNPN同样的5QI（non-3GPP接入请求IPSEC SA的5QI）。此种接入方式，类似于网络下发私有的PLMN广播，普通公网用户无法接入网络。

4 网络接入安全部署策略分析

面向企业角度的数据和用户安全需求，通过对5种网络接入安全管理技术分析，从实现效果、成本及部署场景上做如表2和表3所示的策略总结。

现阶段，整体上针对有数据本地安全诉求的需求建议部署下沉式的本地UPF，针对用户接入安全管控，建议初期采用成本较低的切片+TAC的方式，即NSSAI-ID+TAC，同时结合核心网的白名单进行网络接入的整体控制，而面向更加严格的数据管控要求，在未来可以考虑NPN网络的部署，实现高度定制化的能力来实现用户的接入管控。

5 总结展望

5G在各类垂直行业中的融合应用将会越来越丰富，其特点与垂直领域高度相关，安全风险也呈现持续动态变化的特点，5G网络通过灵活的设计和安全方面的增强，对垂直行业的安全需求有一定的支撑能

表2　企业5G接入网络管控部署策略

技术方式	部署方式	效果	成本	建议部署场景	备注
PLMN	针对企业接入用户分配启用与公网不同的PLMN	可实现用户接入限制	低	密闭场景，例如：煤矿井	需做统一的PLMN规划，PLMN数量限制，需要做好全网协调统一
CELL BAR	开启BAR能力，做UE接入限制	不可实现用户接入限制	低	–	–
TAC	划分限制接入区域为相同的TA，并结合切片（NSSAI）在AMF上部署白名单	可实现用户接入限制	低	广泛应用，隔离区域较为简单的场景均可应用	需切片能力辅助，需运营商配合
PNI-NPN	部署NPN网络，启用CAG	可实现用户接入限制	高	隔离区域较多，接入安全要求严格的区域	NPN网络支持，短期内无商用产品
SNPN	部署SNPN网络，向企业开启网络网络控制面功能	可实现用户接入限制	极高	隔离区域较多，且对控制接入安全管控能力要求较高的大型工业园区	短期内无商用产品，且公网用户无法接入

表3　企业5G接入网数据安全部署策略

部署方式	数据本地处理能力	成本
非下沉UPF	不可以	低
下沉UPF	可以	高

力，随着3GPP R16的新技术陆续在现网部署，可以进一步地满足企业对安全管控的诉求，本文分析了企业视角下的安全需求，并对现有的网络技术以及3GPP R16中的NPN网络等新技术的接入安全满足情况进行了分析，5G网络必须结合垂直行业各自特点和诉求，充分考虑需求的不同后，进行网络组网架构及技术的选择。

参考文献：

[1] Service requirements for the 5G system：3GPP TS 22.261[S/OL].[2021-01-24]. https://www.3gpp.org/ftp/Specs/archive/.

[2] Radio Resource Control（RRC）protocol specification：3GPP TS 38.331[S/OL].[2021-01-24]. https://www.3gpp.org/ftp/Specs/archive/.

[3] System architecture for the 5G System（5GS）：3GPP TS 23.501[S/OL].[2021-01-24]. https://www.3gpp.org/ftp/Specs/archive/.

[4] 一篇文章带你了解非公共网络[EB/OL].[2021-01-24]. https://www.sohu.com/a/335816703_340656.

[5] 中国信息通信研究院IMT-2020（5G）推进组．5G安全报告[EB/OL].[2021-01-24]. http://210.56.209.71/zh/documents/1.

[6] SIDDIQUI M S，ESCALONA E，TROUVA E，et al. Policy based virtualised security architecture for SDN/NFV enabled 5G access networks[C]// 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks（NFV-SDN）. IEEE，2016.

[7] LY A，YAO Y D．A Review of Deep Learning in 5G Research：Channel Coding，Massive MIMO，Multiple Access，Resource Allocation，and Network Security[J]. IEEE Open Journal of the Communications Society，2021（99）：1-1.

[8] 陆海涛，李刚，高旭昇．Security of 5G Network Elements and Access Control[J]. 中兴通讯技术，2019，25（4）：19-24，55.

[9] MILDH，GUNNAR，SKOELD，et al. 5G WIRELESS ACCESS：REQUIREMENTS AND REALIZATION[J]. IEEE Communications Magazine Articles News & Events of Interest to Communications Engineers，2014.

[10] E D AHLMAN，PARKVALL S，PEISA J．5G Wireless Access[J]. Iice Trans Commun，2015，98（8）：1407-1414.

[11] VAEZI M，DING Z，POOR H V. Multiple Access Techniques for 5G Wireless Networks and Beyond‖Filter Bank Multicarrier Modulation[J]. 2019，10.1007/978-3-319-92090-0（Chapter 3）：63-92.

[12] WANG Q，FANG Y，CORPORATION Z. Security Solution in 5G Cloud Core Network[J]. Designing Techniques of Posts and Telecommunications，2018.

[13] GUPTA A，JHA R K，DEVI R. Security Architecture of 5G Wireless Communication Network[J]. International Journal of Sensors Wireless Communications and Control，2018.

[14] DAT P T，KANNO A，YAMAMOTO N，et al. 5G transport and broadband access networks：The need for new technologies and standards[C]// 2015 ITU Kaleidoscope：Trust in the Information Society（K-2015）. IEEE，2016.

[15] DAHLMAN E，MILDH G，PARKVALL S，et al. 5G wireless access：requirements and realization[J]. Communications Magazine，IEEE，2014，52（12）：42-47.

[16] FANG D，QIAN Y，HU R Q. Security for 5G Mobile Wireless Networks[J]. IEEE Access，2017.

[17] HAN B，WONG S，MANNWEILER C，et al. Security Trust Zone in 5G Networks[C]// International Conference on Telecommunications. IEEE，2017.

[18] OLIMID R F，NENCIONI G. 5G Network Slicing：A Security Overview[J]. IEEE Access，2020（99）：1-1.

作者简介：
骆润，咨询师，主要研究方向为无线通信和网络规划；李宗林，咨询师，主要研究方向为无线通信。