国　际　电　信　联　盟

ITU-T

国际电信联盟
电信标准化部门

X.1813

（09/2022）

X系列：数据网、开放系统通信和安全性

IMT-2020安全

IMT-2020专用网络中支持超可靠性和低延迟通信（URLLC）的垂直业务运营的安全和监测要求

ITU-T X.1813建议书

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
万维网安全（1）	X.1140–X.1149
应用安全（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1350–X.1369
智能交通系统（ITS）安全	X.1370–X.1399
分布式账簿技术（DLT）安全	X.1400–X.1429
应用安全（2）	X.1450–X.1459
万维网安全（2）	X.1470–X.1489
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
网络防御	X.1590–X.1599
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
数据保护	X.1770–X.1789
IMT-2020安全	**X.1800–X.1819**

ITU-T X.1813建议书

IMT-2020专用网络中支持超可靠性和低延迟通信（URLLC）的垂直业务运营的安全和监测要求

概要

ITU-T X.1813建议书规定IMT-2020专用网络中支持URLLC的垂直业务运营的安全要求。本建议书确定在IMT-2020专用网络中提供支持URLLC的垂直业务时出现的威胁和风险，描述运营支持URLLC的垂直业务的IMT-2020专用网络的安全部署场景。对通信内容的监测超出了本建议书的范围。

IMT-2020专用网络，也称为IMT-2020非公众网络（NPN），旨在供企业等私有实体单独使用，并且可以利用虚拟和物理元素部署在各种配置中。它将提供IMT-2020承诺的速度、低延迟和其他优势，以支持下一代应用。

在使用IMT-2020专用网络的智能工厂和智慧城市的垂直业务中，许多物联网（IoT）设备使用大规模机器类型通信（mMTC）和超可靠性和低延迟通信（URLLC）。这些通信可能面临安全威胁及其相关风险。此外，这些威胁会破坏支持URLLC的垂直业务的稳定运营。当垂直业务的性能因这些风险而降低时，这是无法保证的。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1813	2022-09-02	17	11.1002/1000/14991

关键词

深层包检测（DPI）、端点发现和响应，多接入边缘计算（MEC）、非公众网络（NPN）、网络监测、性能、IMT-2020专用网络、安全性、用户平面功能（UPF）。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一ID，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联已收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1813建议书

IMT-2020专用网络中支持超可靠性和低延迟通信（URLLC）的垂直业务运营的安全和监测要求

1 范围

本建议书规定IMT-2020专用网络中支持超可靠性和低延迟通信（URLLC）的垂直业务运营的安全要求。这一建议书确定了在IMT-2020专用网络中提供支持URLLC的垂直业务时出现的威胁和风险，描述运营支持URLLC的垂直业务的IMT-2020专用网络的安全部署场景。

在本建议书中，对通信内容的监控不属于隐私保护的范围。

2 参引

下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献均会得到修订；因此本建议书的使用者应查证是否有可能使用下列建议书和其他参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

[ITU-T Y.3102] ITU-T Y.3102建议书（2018）– IMT-2020网络框架

3 定义

3.1 他处定义的术语

本建议书采用下列他处定义的术语：

3.1.1 5G非公众网络[b-3GPP TS 22.261**]**：用于私营用途的5G网络。

3.1.2 攻击[b-ISO13491-1]：设备上的对手试图获取或修改他们无权获取或修改的敏感信息或服务。

注1 – 网络功能（NF）包括但不限于网络节点功能，例如会话管理、移动性管理和传输功能，其功能行为和接口已得到定义。

注2 – 网络功能可以在专用硬件上实现，也可以作为虚拟化软件功能实现。

注3 – 网络功能不是资源，而是可以使用资源进行实例化的任何网络功能。

3.1.3 部署[b-ISO/IEC/IEEE 24765]：项目过程中系统投入运行并解决切换问题的阶段。

3.1.4 域[b-ISO/IEC 14888-1]：在单一安全策略下运行的一组实体。

示例：由一个受权机构或一组受权机构使用相同安全策略创建的公钥证书。

3.1.5 物联网（IoT）[b-ITU-T Y.4000]：一种信息社会全球基础设施，（通过物理和虚拟手段）将基于现有和演进中的、可互操作信息通信技术的事物相互连接，以提供先进服务。

3.1.6 网络监测[b-ISO/IEC 27033-1]：持续观察和审查记录在网络活动和操作上的数据的过程，包括审计日志和警报，以及相关分析。

3.1.7 网络功能[b-ITU-T Y.3100]：在IMT-2020环境中为网络中的处理功能。

3.1.8 系统[b-ISO/IEC 27000]：应用、业务、信息技术资产或其他信息处理构成成份。

3.1.9 利益攸关方[b-ISO/PAS 19450]：对正被考虑、开发或部署的系统有兴趣或可能受其影响的个人、组织或群体。

3.1.10 信任[b-ISO/IEC 25010]：用户或其他利益攸关方对产品或系统按预期行为的信心程度。

3.1.11 垂直业务[b-5G-PPP**]**：从商业角度来看，垂直业务是一种专注于特定行业或具有专门需求的客户群体的业务（例如，汽车业务、娱乐业务、电子卫生业务、工业4.0）。

3.2 本建议书定义的术语

本建议书定义了如下术语：

3.2.1 IMT-2020通信系统：为IMT-2020业务管理IMT-2020通信流程的系统。

注1 – 5G在ITU-T被称为IMT-2020。

注2 – 在本建议书中，IMT-2020通信系统与IMT-2020系统相同。

3.2.2 IMT-2020生态系统：一组利益攸关方，他们相互作用，形成一个稳定运行的IMT-2020系统。

注 – 本术语与5G通信技术的开发相关，其中的利益攸关方来自行业和学术界，他们贡献大量产品、技术和专业知识，使5G价值链在基础设施、网络、平台、业务和应用等不同层面发挥作用。

3.2.3 IMT-2020专用网络：5G非公众网络（见第3.1.1节），利用IMT-2020通信系统的虚拟和物理元素，且目的是只供企业等私营实体使用。

3.2.4 IMT-2020业务：IMT-2020生态系统提供的一种益处。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

5GC 5G核心
AMF 接入和移动性管理功能
DDoS 分布式服务拒绝
DPI 深层包检测
EC 边缘计算
EDR 端点发现和响应
GTP GPRS隧道协议
IoT 物联网
MEC 多接入边缘计算

MEC DP MEC数据平面
mMTC 大规模机器类型通信
NF 网络功能
NMCF 网络监测客户机功能
NMF 网络监测功能
NMSF 网络监测服务器功能
NPN 非公众网络
PLMN 公众陆地移动网络
RTT 往返时间
SBA 基于业务的架构
SMF 会话管理功能
UDM 统一数据管理
UE 用户设备
UID 用户身份
UPF 用户平面功能
URLLC 超可靠性和低延迟通信

5 惯例

本建议书使用下列惯例：

关键词**“要求”**表示必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与该要求有任何偏差。

关键词**“建议”**表示是一项建议的、并非需绝对遵守的要求，因此声称遵守时不一定要按照该要求行事。

关键词**“禁止”**表示必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与之有任何偏差。

关键词**“作为选择可以”**表示允许的一项可选择的要求，不含有任何被建议的意思。该术语并非意味着厂商在实施中一定提供这一可选功能，网络运营商/服务提供商可作为选择提供这一功能。也就是说，这意味着厂商可以作为选择提供这一功能特性，同时仍然声称遵守本建议书提出的规范。

6 概述

IMT-2020系统的架构是为了支持网络运营商的、基于网络功能虚拟化和软件定义网络等技术的数据连接和业务。3GPP [b-3GPP TS 23.501]定义了基于业务的架构（SBA），据此IMT-2020网络的控制平面功能和公共数据存储库是通过一组相互连接的网络功能（NF）来提供的，每个功能都有授权来访问对方的业务。图1描述IMT-2020系统的架构。

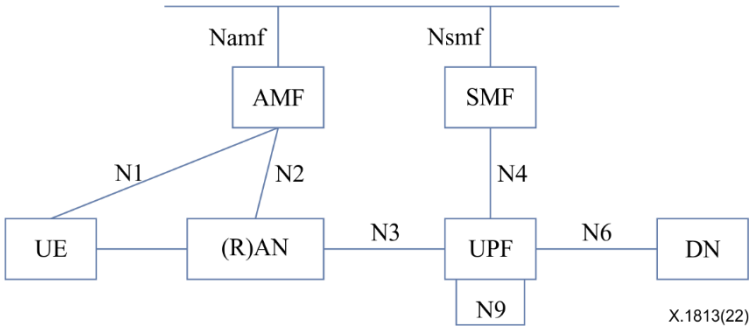


图1 – IMT-2020系统架构

在[ITU-T Y.3102]和[b-3GPP TS 23.501]中定义的IMT-2020系统架构由以下网络功能组成：

– 接入和移动性管理功能（AMF），提供注册管理功能、连接管理功能、移动性管理功能、接入认证功能、接入授权功能、位置服务管理功能、用户设备（UE）移动性事件通知功能等。

– 数据网络（DN），例如，运营商服务、互联网接入或第3方服务。

– 会话管理功能（SMF），提供会话建立、修改和释放功能，用户设备（UE）IP地址分配和管理功能、用户平面功能的选择和控制、计费数据收集和计费接口的支持、用户层功能（UPF）上的计费数据收集控制和协调、下行链路数据通知、字头压缩支持等。

– 用户平面功能（UPF）是处理协议数据单元（PDU）会话的用户平面路径。3GPP支持在一个给定的PDU会话中使用单个UPF或多个UPF进行部署。UPF选择由SMF完成。UPF响应SMF请求，提供用户设备（UE）IP地址/前缀的分配、数据包路由和转发功能、数据包检验功能、用户平面的服务质量（QoS）处理、下行链路数据包缓冲和下行链路数据通知触发等。

– Namf：Namf为核心接入和移动性管理功能识别基于服务的接口。

– Nsmf：Nsmf为会话管理功能标识基于服务的接口。

– UE：用户设备。

– (R)AN：（无线）接入网。

IMT-2020系统架构包含以下参考点：

– N1：UE与AMF之间的参考点。

– N2：(R)AN与AMF之间的参考点。

– N3：(R)AN与UPF之间的参考点。

– N4：SMF与UPF之间的参考点。

– N6：UPF与数据网络（DN）之间的参考点。

– N9：两个UPF之间的参考点。

IMT-2020专用网络的目的是只供企业等私营实体使用，可以利用IMT-2020通信系统的虚拟和物理元素，以各种配置进行部署。IMT-2020专用网络须建立在[b-3GPP TS 23.501]所述的IMT-2020系统架构原则上，包括新引入功能的灵活性和模块化。IMT-2020专用网络的功能架构在附录一中具体说明。

3GPP规范[b-3GPP TS 23.501]预见了各种专用网络的部署场景。在最高层面，专用网络可分为两类：

– IMT-2020专用网络作为独立的完全自成一体的网络得到部署；

– IMT-2020专用网络作为公众陆地移动网络（PLMN）的一个切片与公众网络一起部署。

然而，物联网（IoT）在[b-ITU-T Y.4000]中被定义为一种信息社会全球基础设施，（通过物理和虚拟手段）将基于现有和演进中的、可互操作信息通信技术的事物相互连接，以提供先进服务。在本建议书中，这种垂直业务的主要使用案例是IoT服务。在这种情况下，IoT设备可以是3GPP[b-3GPP TS 22.261]所定义的UE的代表设备。

随着IMT-2020技术进入商业化阶段，IMT-2020专用网络将主要用于构建具有工业IoT设备的IMT-2020垂直业务，如智慧工厂和智慧城市服务，这些业务需要实时性能的超可靠性和低延迟通信（URLLC）。因此，IMT-2020专用网络必须满足安全和性能方面的各种要求，因为它按照[ITU-T Y.3102]处理时间敏感的数据。图2具体说明符合[b-3GPP TR 23.734]的IMT-2020专用网络的整体安全架构。

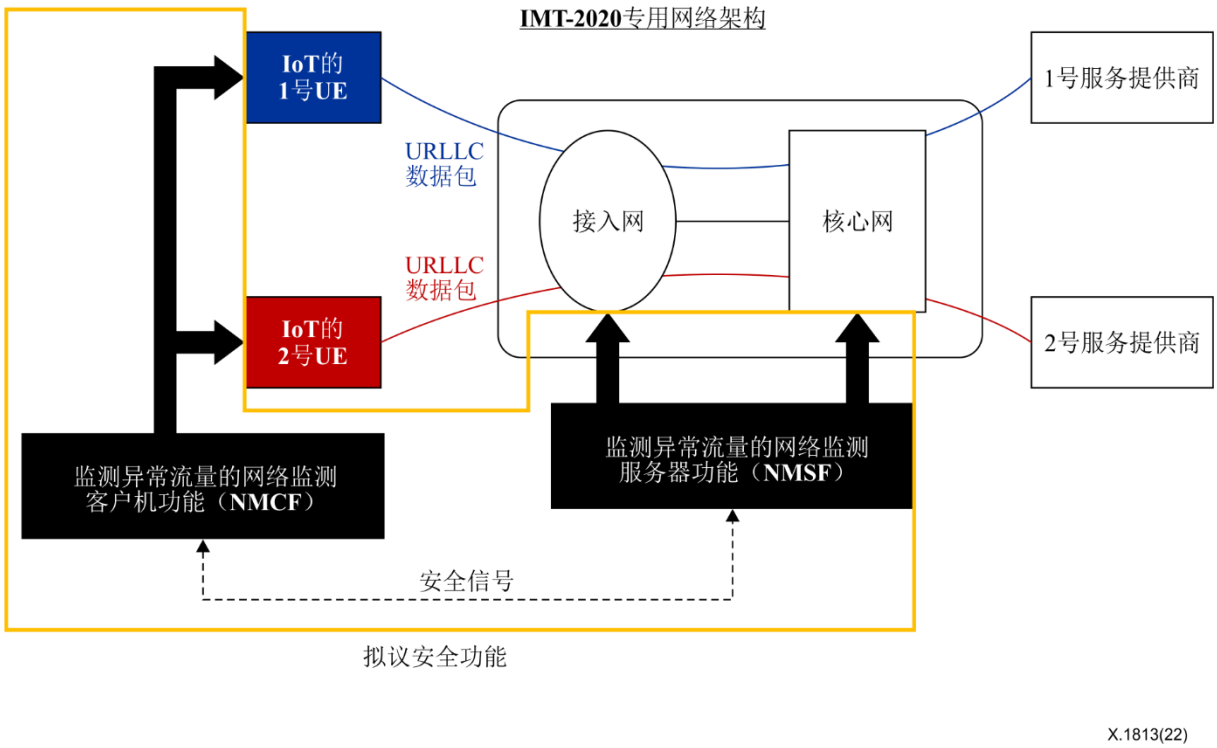


图2 – IMT-2020专用网络的安全架构

从图2可以看出，IMT-2020专用网络的安全架构使运营商能够监测IMT-2020专用网络中网络节点和端点用户设备之间的通信安全情况/性能，以支持URLLC的垂直业务的运行。

7 IMT-2020专用网络中支持URLLC的垂直业务所面临的威胁

IoT给人们带来多种令人兴奋的新机会，如工业自动化和控制系统（IACS）、自治车辆通信、智能电网、高速公路/交通传感器、无人机通信、医疗传感器和AR/VR（大多以自动化方式运行）。IoT业务可能也必须满足IMT-2020业务的URLLC特性。根据[b-3GPP TS 22.261] – 专用网络的目的是只供企业等私营实体使用，只有经授权的UE才有权访问专用网络。

在此种环境中，对垂直业务的威胁，除其他外，被确定为任何能在延迟方面损害IMT-2020专用网络的构成成份和接口的攻击。IMT-2020专用网络可以在有或没有UPF/多接入边缘计算（MEC）的情况下部署。UPF可以通过3GPP定义的N6接口访问互联网。因此，如果IMT-2020专用网络部署有UPF和MEC，那么N6接口就面临很大的攻击风险，因为互联网上任何地方的攻击者都可以访问它。这种攻击是有意或无意地从IMT-2020专用网络外部或内部进行的。

对UPF、MEC和N6接口的威胁可以列举如下：

– 分布式服务拒绝（DDoS）攻击；

– 窥探通信链路的流量/数据；

– IMT-2020专用网络中的UE产生的意外增加的流量或异常流量。

IMT-2020专用网络是由私人利用网络构成成份和接口部署的网络，其中部分是新的，在安全方面与现有网络不同。连接接入网和核心网的N3接口使用IPsec进行安全性能传输。N4接口连接UPF和AMF。该N4接口在4G演进分组核心（EPC）中是封闭的，但在IMT-2020 vEPC中并非封闭。与X6接口相比，N3和N4接口不能通过互联网访问，但是，有可能会出现新型的无意威胁和障碍。

N3和N4接口面临的威胁可以列举如下：

– IMT-2020专用网络实施的访问控制方法不充分；

– IMT-2020专用网络运营商实施的安全措施和程序存在限制。

– IMT-2020专用网络中的网络构成成份设计不当或配置错误，无法满足突然增加的访问需求。

不习惯IMT-2020网络的许多新功能特性方面的专家，也可能成为无意的威胁和障碍。

8 IMT-2020专用网络中支持URLLC的垂直业务面临的风险

IMT-2020专用网络基本上在IoT基础设施中提供高度可信的网络，因为用于新兴IMT-2020垂直业务安全的IMT-2020专用网络已由3GPP标准化。

尽管3GPP和其它安全标准提供了认证、授权和数据保密等常规安全方法，但IMT-2020专用网络仍然会面临大量风险。例如现有安全方法不能摆脱IMT-2020专用网络中UE异常行为带来的威胁。

由于IMT-2020网络拥有更强的以软件为中心的功能特点，因此它们可能会面临更多与软件开发缺陷、程序更新失误以及配置错误有关的风险。因此，由于上述各种威胁，IMT-2020网络存在性能下降的风险。

在此背景下，风险的影响可能包括：

– 垂直业务的不稳定和危险运行：在IMT-2020网络中安营扎寨的IoT设备的异常行为可能会为智慧城市基础设施的正常运行带来威胁。

– 破坏、修改或改变IMT-2020网络基础设施中存储或通信的信息。

– IMT-2020 URLLC业务的性能下降：如果IMT-2020网络不能保证IMT-2020 URLLC业务的低时延要求，则网络可能会面临性能下降，从而给相关的时间敏感型垂直业务造成负面影响。例如，由于智慧工厂是根据URLLC要求设计的，所以如果低延迟要求无法满足，则生产质量或速度可能会下降。这不仅可能导致巨大的经济损失，而且可能导致安全事故。另一示例为，由于各种传感器的连接延迟，安全摄像头的图像质量可能会大幅下降。

有鉴于此，需要为IMT-2020专用网络中支持URLLC垂直业务的运行制定安全要求，以应对上述威胁和风险。

9 IMT-2020专用网络中支持URLLC垂直业务运行的安全功能部署场景

本节确定在IMT-2020专用网络中支持URLLC垂直业务运行的安全功能的部署场景。IMT-2020专用网络安全架构是由网络监测功能（NMF）配置的。NMF由网络监测服务器功能（NMSF）和网络监测客户机功能（NMCF）组成。NMF可以由部署在网络节点中的深层包检测（DPI）功能或专门的DPI网络节点来实现。

NMSF可被配置为独立的与UPF或MEC分开的网络节点。具体而言，NMSF须与UPF或MEC的输入或输出相耦合，以便它们能够监测其中的数据包。

NMSF有以下三种部署场景：

A) 在MEC中NMSF作为一个节点得到集成。

B) NMSF作为一个单独的节点实施，监测从UPF输出的数据包。

C) 配置多个NMSF，使第一个MNSF被集成为MEC中的一个节点，第二个NMSF被实施为一个单独节点，以监测从UPF输出的数据包。

在这三种部署场景中，NMSF是否被分配指定的IP是一个实施问题。在所有这三种部署场景中，NMCF都被集成到UE中。

图3具体描述IMT-2020专用网络安全架构中的部署场景A，其中配置了多个NMCF和NMSF。

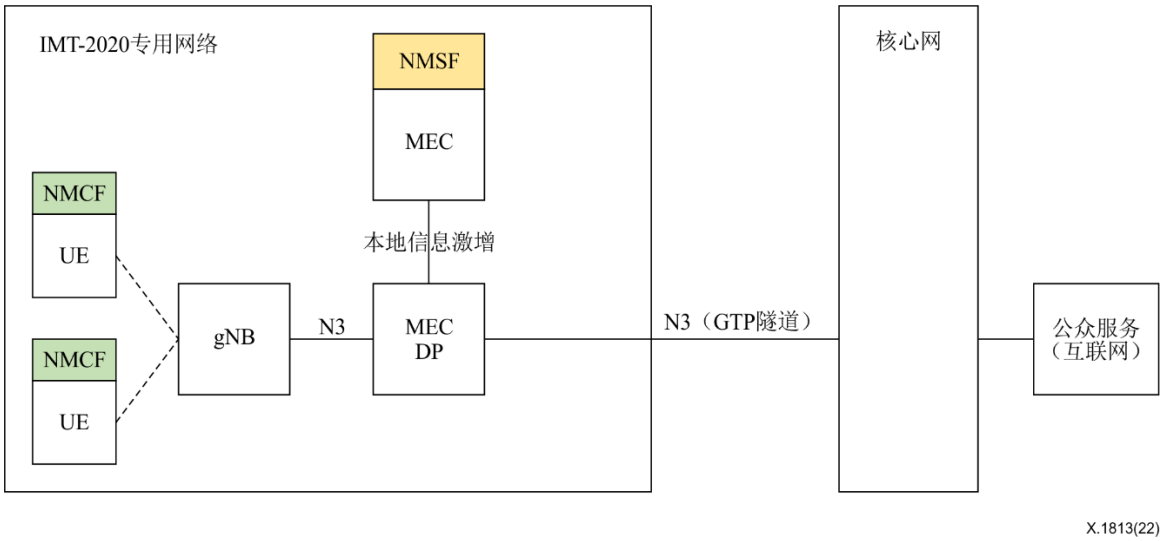


图3 – 部署场景A

图3显示，NMCF可以被集成到各自的UE中，特别是与gNB进行通信的IoT设备。在IoT设备上安装NMCF是保证IMT-2020专用网络的安全和URLLC性能的有效解决方案之一。NMCF可以用软件实现，也可以被称为端点发现和响应（EDR）实体或微型引擎（ME）。NMCF服务器可以位于IMT-2020专用网络或边缘云或公众网络域（互联网）内。UE以无线方式与gNB连接。每个UE向gNB发送数据包或从gNB接收数据包。gNB通过N3和N4接口与IMT-2020核心网络或本地网络连接。数据包流经N3和N4接口。

如果一个IP地址被分配给NMSF，则NMCF和NMSF通过N3和N4相互通信，在NMCF和NMSF之间交换安全信号，如NMCF处的监测结果。

在场景A的情况下，虽然在图3中未予显示，但额外的NMSF也可被集成至MEC数据面（MEC DP），这样两个NMSF就可以同时监测专用网络流量和进出UE的公众网络流量。NMSF也可以被配置为与MEC分离的独立实体。

图4具体描述IMT-2020专用网络安全架构中的部署场景B，其中配置了多个NMCF和NMSF。

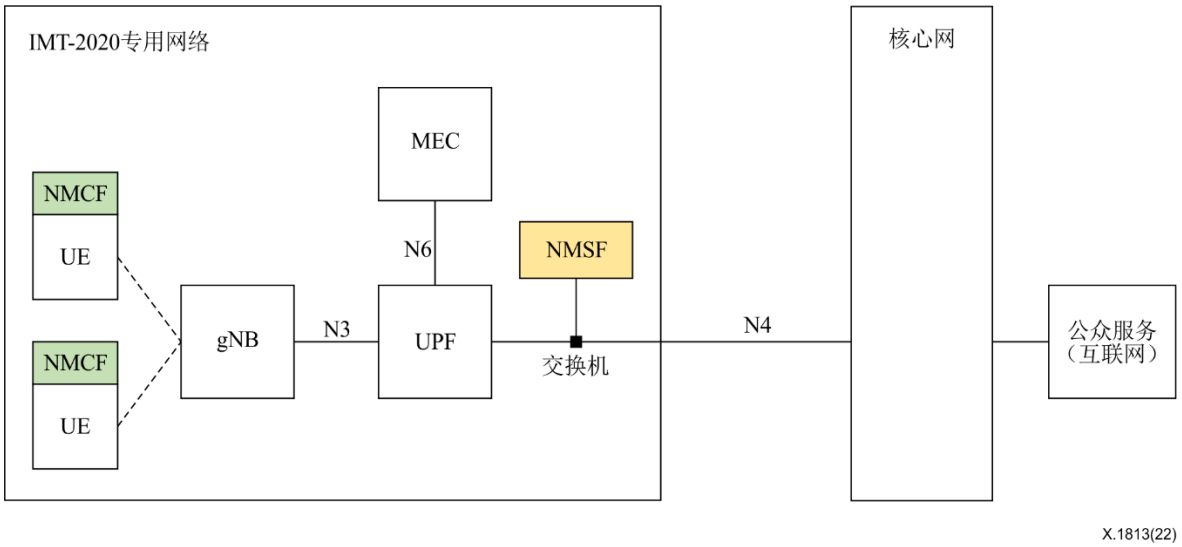


图4 – 部署场景B

如图4所示，NMSF在UPF之外作为一个单独节点，监测由UPF输出的数据包。可使用交换机来镜像来自UPF的数据包。如果给NMSF分配一个IP地址，则NMCF和NMSF通过N3和N4相互通信，以交换安全信号，如在UE（客户机节点）产生的监测结果。如果IMT-2020专用网络使用节点到节点的加密功能，如IPSec，则NMSF可被配置在解密数据包从节点输出的位置。

图5具体描述IMT-2020专用网络安全架构中的部署场景C，其中配置了多个NMF。

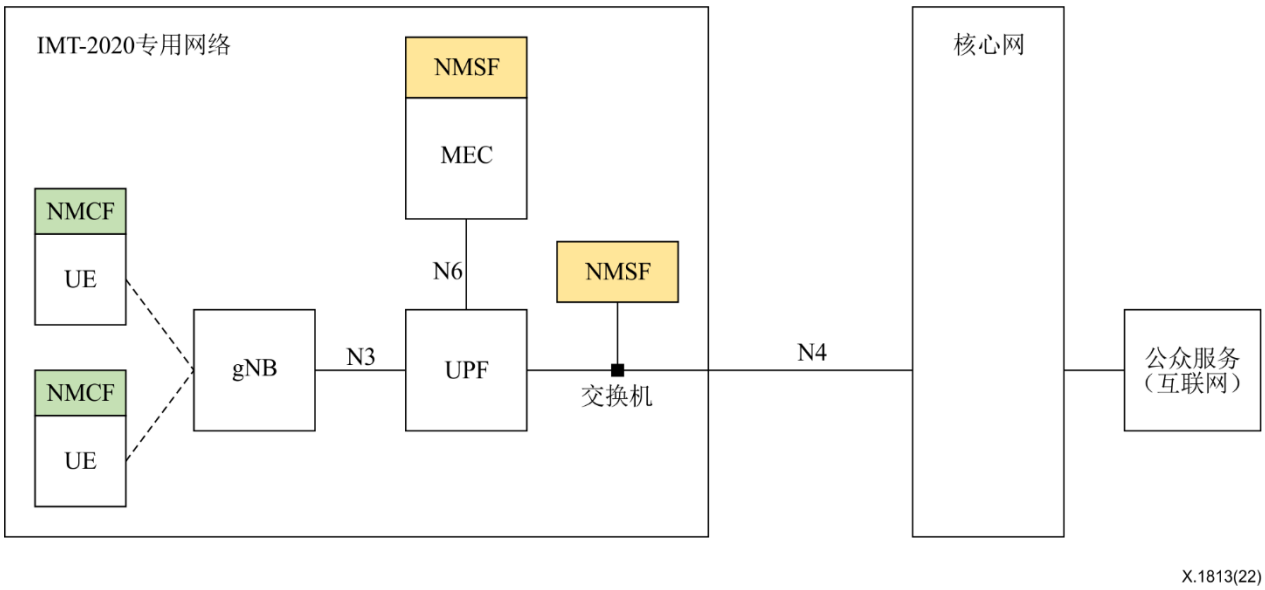


图5 – 部署场景C

从图5可看出，NMSF不仅被集成至MEC，而且在UPF外作为单独节点得以实现，以监测UPF输出的数据包。如果IP地址分别分配给NMSF，则NMCF和NMSF通过N3和N4相互通信，以交换安全信号，如在UE（客户机节点）处产生的监测结果。如果IMT-2020专网使用节点对节点的加密功能，如IPsec，则NMSF可被配置在从节点输出解密数据包的位置。

上述三种场景并不相互排斥，使用哪种模式取决于成本或网络特性等。NMSF和NMCF的多种不同部署也是可能的，例如，NMSF可与UPF和/或MEC一起被集成至任何一个网络节点。

因此，从网络功能架构的角度而言，可通过使用安装在MEC和/或UPF上的NMSF和安装在IoT设备上的NMCF，以及NMSF和NMCF之间的信令协议进行安全和性能监测。

10 IMT-2020专用网络中支持URLLC的垂直业务操作的安全和监测要求

本节确定了IMT-2020专用网络中支持URLLC垂直业务操作的安全和监测要求。与传统网络相比，IMT-2020专用网络需要更高级别的安全性和性能，因为大量数据在众多客户端设备、传感器和对其进行控制的中央服务器之间交换。此外，根据[ITU-T Y.3102]，在边缘区域也必须满足IMT-2020 URLLC的要求。

对于NMSF和NMCF的IMT-2020专用网络部署场景，支持URLLC垂直业务运行的一般安全和监测要求包括：

a) 需要监控和检测UE和IMT-2020专用网络的异常行为，以降低安全风险。

b) 需要监控支持URLLC的垂直业务的性能。

c) 需要向网络管理员报告UE和IMT-2020专用网络的异常行为，以便解决问题并及时恢复URLLC的能力。

另外，本文建议使UE和IMT-2020专用网络异常行为可视化，以便更有效地解决这些异常行为。附录C描述了监测结果的可视化。

10.1 NMSF的安全

NMSF的安全要求包括以下内容：

a) 要求NMSF至少提供在客户端节点和服务器节点之间发送和接收的镜像数据包的功能，从而获得至少一个镜像数据包。客户端节点是UE或物联网设备。数据包镜像是一种实时收集和分析特定节点所交换数据包的技术。NMSF可以拥有用于数据包镜像的交换功能。

b) 要求NMSF根据镜像数据包中包含的信息，确定威胁IMT-2020专用网络安全和性能的异常行为或安全问题。

c) 如果IP地址被分配给NMSF，则要求NMSF从NMCF接收使用TCP包格式的安全检查包，并基于接收的安全检查包计算往返时间（RTT）。

使用TCP包格式的安全检查包如图6所示。

X.1813(22)

图6 – 使用TCP数据包格式的安全检查数据包

表1 – 安全检查包的字段

字段	字节长度	说明
用户标识（UID）	4	该字段指示UE的用户ID。
长度	2	该字段指示监测结果字段的字节长度。
监测结果	可变	该字段指示UE的活跃信息、CPU的使用和内存的使用情况。

d) 如果没有为NMSF分配IP地址，NMSF需要使用用户数据报协议（UDP）数据包格式将安全检查数据包从NMCF发送到服务器节点，并根据镜像的安全检查数据包计算往返时间（RTT）。

使用UDP包格式的安全检查包如图7所示。

X.1813(22)

图7 – 使用UDP数据包格式的安全检查数据包

表2 – 安全检查包的字段

字段	字节长度	说明
UID	4	该字段指示UE的用户ID
长度	2	该字段指示监测结果字段的字节长度
监测结果	可变	该字段指示UE的活跃信息、CPU的使用和内存的使用情况

e) 建议NMSF根据安全和性能状态，对妨碍URLLC要求的异常行为发出告警。当检测到威胁安全和性能的异常行为时，NMSF会向用户发出告警，以便用户能够正确应对异常行为。然后，NMSF向安全控制器发送告警信息，指示安全控制器对异常行为采取适当措施，即关闭网络。告警信息通过3GPP信令协议提供的N3和N4接口发送。

基于NMSF镜像的性能/安全性监控的详细特征可以通过附录A的标准算法执行。

10.2 NMCF的安全

NMCF的安全包括以下内容：

a) NMCF需要在单个客户端节点或物联网传感器的计算资源上运行，建议使用最少量的资源，以便以适当的方式执行相关功能。

b) NMCF需要收集客户端节点通过网络发送或接收的数据包或内部信息。

c) 要求NMCF基于所收集的数据包或内部信息，监控和确定与包括NMCF本身在内的客户端节点相关的网络安全威胁。如果内部信息的指示值等于或大于门限值，则NMCF确定存在网络安全威胁。内部信息的示例包括客户端节点的CPU使用率、客户端节点内存的用率等。

d) 如果将IP地址分配给NMSF，则NMCF需要使用包括图6所示监控结果的TCP包格式生成安全检查包，并将安全检查包发送给NMSF。

e) 如果IP地址没有分配给NMSF，则NMCF需要使用包括图7所示监控结果的UDP数据包格式生成安全检查数据包，并将安全检查数据包发送到服务器节点，以便NMSF可以建立安全检查数据包镜像。

f) 建议NMCF向物联网设备用户显示所有异常UE操作告警。

就NMCF而言，收集到更准确数据的可能性更高；NMCF也可能在出现问题时停止运行，例如，正常运行的设备电源被关闭。因此，NMSF的性能安全监控至关重要。

然而，对连接到IMT-2020专用网络的大量UE的各数据流实施监控可能会给NMSF带来很大负担，这种情况下需要与NMCF合作，以有效监控对网络造成的威胁。

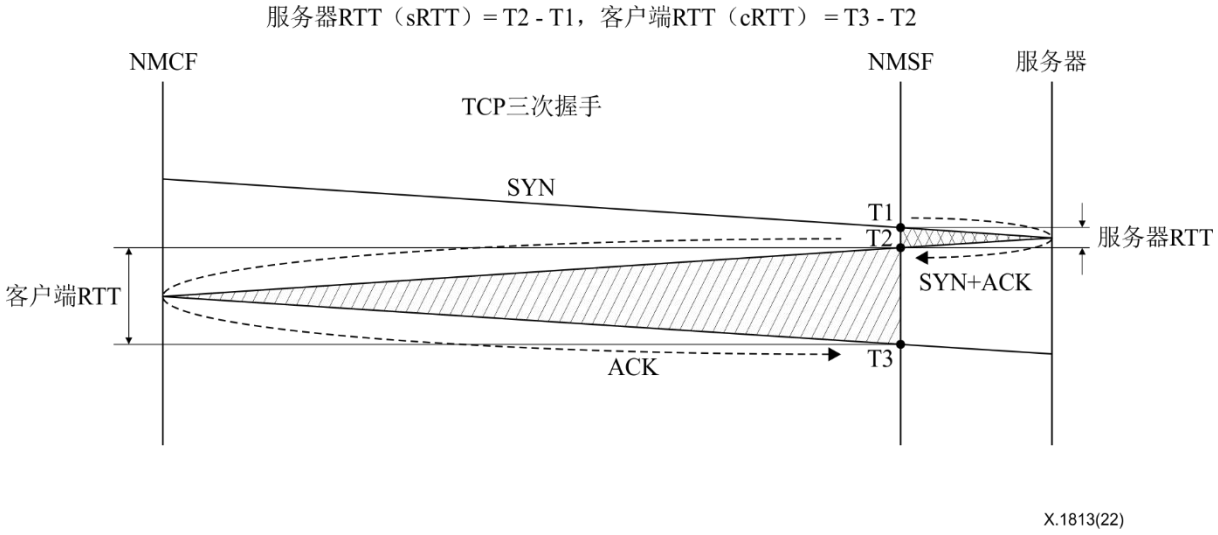
可以通过附录B的标准算法实现NMCF要求的详细特征。

附件A
NMSF的特性

（此附件是本建议书不可分割的组成部分。）

根据本建议书，NMSF依据镜像数据包或与镜像数据包相关的信息，确定威胁安全性和性能异常行为的发生。依照通信业务要求（IMT-2020或LTE），NMSF通过计算与IMT-2020专用网络性能或安全性相关的指标或参数，再将计算结果与参考值进行比较，确定是否发生了异常行为。这里，通信业务需求可以从物联网设备的接入信息中获知。

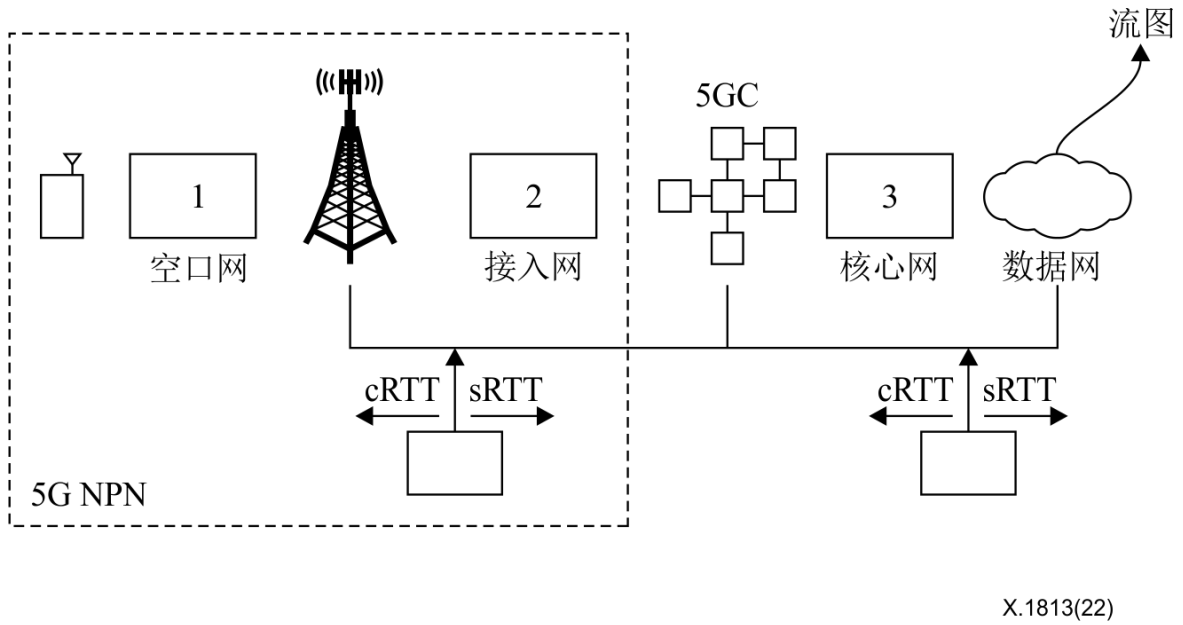
图A.1显示了一种测量往返时间（RTT）的方法，该方法使用镜像数据包作为与IMT-2020专用网络的性能指标或与安全性相关的指标，并根据RTT确定威胁IMT-2020专用网络安全和性能的异常行为。



图A.1 – RTT的测量

参考图A.1，在与发送和接收同步信号（SYN）相关的三次握手场景中，NMSF通过使用网络用户和服务器之间的镜像数据包计算网络的RTT。例如，在提取并存储NMCF（即客户端）与NMSF服务器（或MEC）之间交换的三个数据包（SYN、SYN + ACK和ACK）的发送和接收时间点后，NMSF在T1、T2和T3之间至少会获得一条时间信息。NMSF通过T2（T2 – T1）减去T1计算NMCF服务器的RTT（sRTT），通过T3 – T2计算客户端的RTT（cRTT）,并通过sRTT + cRTT或T3 – T1计算整个网络的RTT。凭借对每次行为进行的计算，NMSF可以算出整个网络的RTT。

NMSF通过确定sRTT、cRTT和网络RTT是否满足IMT-2020专用网络的URLLC要求，分析对IMT-2020专用网络性能或安全的威胁。图A.2显示了如何在IMT-2020专用网络中使用sRTT和cRTT识别性能劣化区域。



图A.2 – 识别IMT-2020专用网络中的性能劣化区域

除RTT之外，各种其他指标也可用于确定性能或安全威胁的指标。该指数的典型示例包括响应等待时间信息，此信息表示NMSF服务器（或MEC）从与客户端所发内容请求相关联的URL接收到与内容相关联的首批数据的响应等待时间；响应等待会话数量信息表示处于未接收到客户端发送请求响应状态的会话数量；BPS、CPS、TPS、HTTP 40x或50x错误；从镜像包获得的关于数据发送和接收的信息；从多个镜像包获得的统计信息；以及表示连接到物联网设备或NMCF服务器的可能性的活跃信息。

可通过使用这些指标，以各种方式实现用于确定性能和安全威胁的算法。例如，NMSF基于流量信息（OSI 3或OSI 4层）确定网络安全威胁是否存在，流量信息包括关于数据包流的信息和关于协议的信息（OSI 7层）。

除上述之内容外，可以采用各种技术，包括使用网络安全威胁检测数据包的信息开展安全威胁检测（例如，当从预定源IP到目的地IP或服务器的BPS或URL请求区段上的连接数超过预定门限值时，则将其确定为安全威胁），基于流量信息的安全威胁检测（例如，使用基于流量分布图的聚类技术，确定是否已出现超过预定门限值的流量，然后确定在IMT-2020专用网络中是否已发生安全问题）、基于协议信息的安全威胁检测、基于异常的检测、基于签名的检测或基于误用的检测、状态协议分析检测以及基于规范的检测。NMCF和NMCF服务器之间的通信内容也可能包含在NMSF的分析内容中。

附件B
NMCF特性

（此附件是本建议书不可分割的组成部分。）

对于NMCF服务器和NMSF的集成，需要一个用于在NMCF（或NMCF服务器）和NMSF之间交换安全信息的协议。

首先，NMCF通过使用自身业务所需的物联网设备状态、系统状态或日志信息以及RTT，确定是否存在网络安全威胁。业务所需物联网设备的状态包括CPU负载、内存的使用、存储的使用和活跃信息。例如，当内存的使用等于或大于预配置的门限值或RTT大于预配置的门限值时，则NMCF确定已发生威胁安全和性能的异常行为。另一示例指出，当日志信息指示IP被禁止的实体试图登录客户端节点或者发生了未知过程时，则NMCF确定已发生了威胁安全和性能的异常行为。

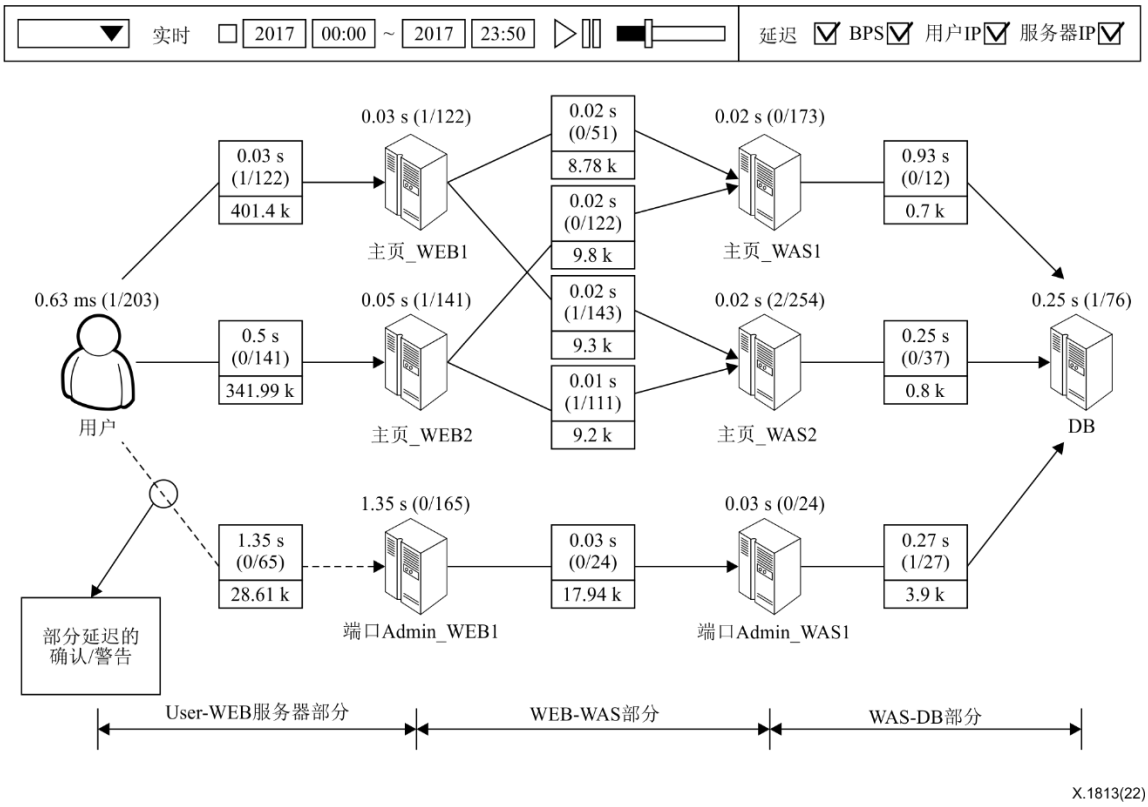
NMCF接下来将所确定的关于是否存在安全威胁的监控结果值发送给NMCF服务器或NMSF。换言之，NMSF实时接收终端感知的网络安全威胁监控结果。此时，应该从由NMCF服务器收集的关于NMSF的NMCF和分析内容的信息中识别物联网设备，使得由同一物联网设备生成的内容可以与其他内容区分开。

上述方法可以通过在诸如NMCF之类的端点执行威胁监控来减轻中央NMSF的负担，且可因此提高针对网络性能和安全威胁的监控水平。

附件C
监控结果的可视化

（此附件是本建议书不可分割的组成部分。）

图C.1举例说明了使用NMSF的网络/系统性能和安全监控的可视化。



图C.1 – 网络/系统性能和安全监控的可视化示例

参考图C.1，基于性能指标或安全指标的分析结果可实现实时可视化，然后作为告警提供给用户。网络管理员能够利用这些结果立即应对威胁。换言之，分析结果是从性能和安全角度加以解释。一旦检测到异常行为，网络管理员就会收到告警信号。

期望的结果是可视化能够直观且清楚地表达网络中实体之间的链接。实现可视化，使得NMSF生成与性能和安全相关的指标对象，同时在可视化的空间中实现所生成的对象，并生成展示网络业务流的流图。为此，将通过生成与第一实体相关联的性能/安全性指示符，与第二实体相关联的性能/安全性指示符，以及与第一实体和第二实体链路相关联的性能/安全性指示符来获得对象。

为提高清晰度，基于与链接相关联的性能/安全性指标对象化，在流图的第一实体和第二实体之间画线。为便于区分可以添加颜色。换言之，根据与链接相关联的性能/安全指示符，至少可以实现颜色、形状和厚度中某一指标的明显可视化。

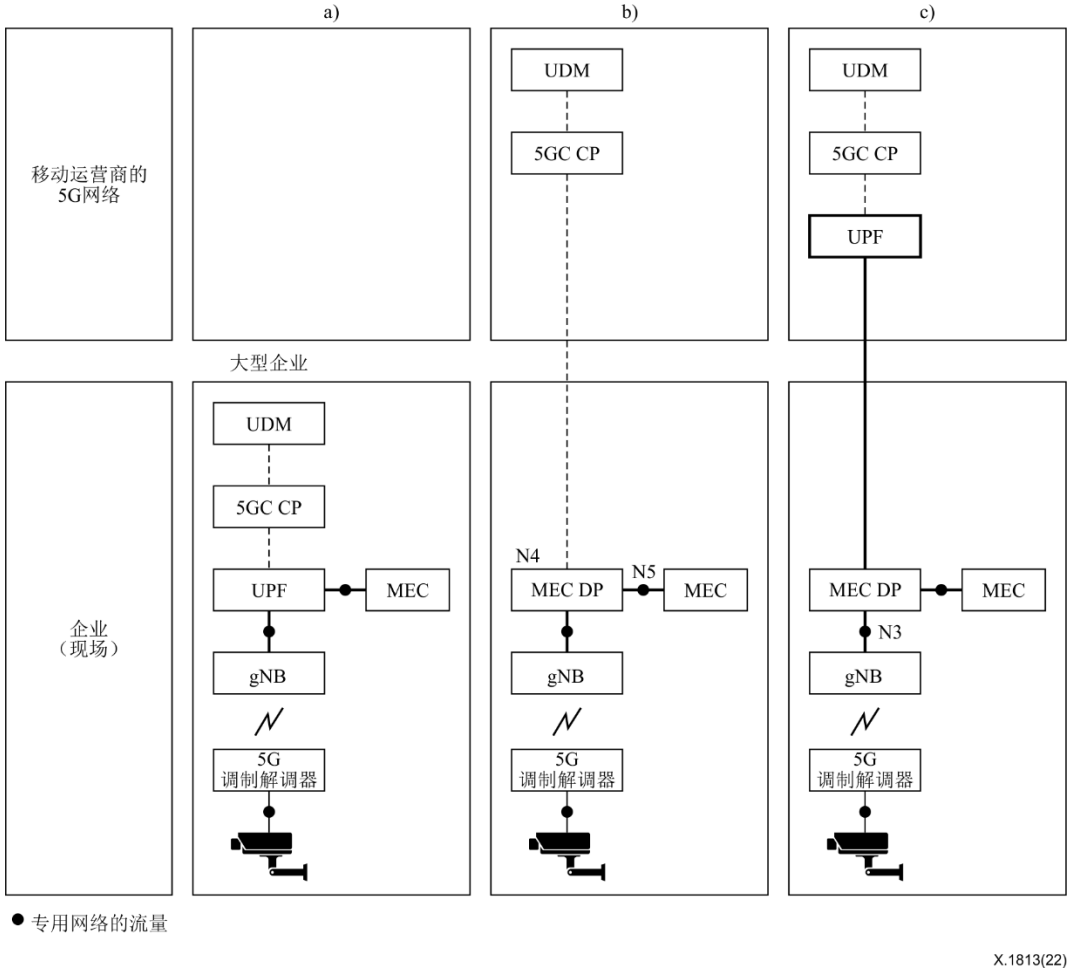
通过使用这种可视化功能，可实现所有业务部分的可视性和清晰性。这不仅可以通过管理网络业务来加强预防网络业务出现的问题，亦使网络能够轻松应对智慧工厂和智慧城市等庞大物联网基础设施中的威胁。

附录一

面向垂直业务的IMT-2020专用网络使用案例

（本附录不构成本建议书的组成部分。）

本建议书基于三种类型的IMT-2020专用网络架构，如图I.1所示。



图I.1 – 三种类型IMT-2020专用网络的部署

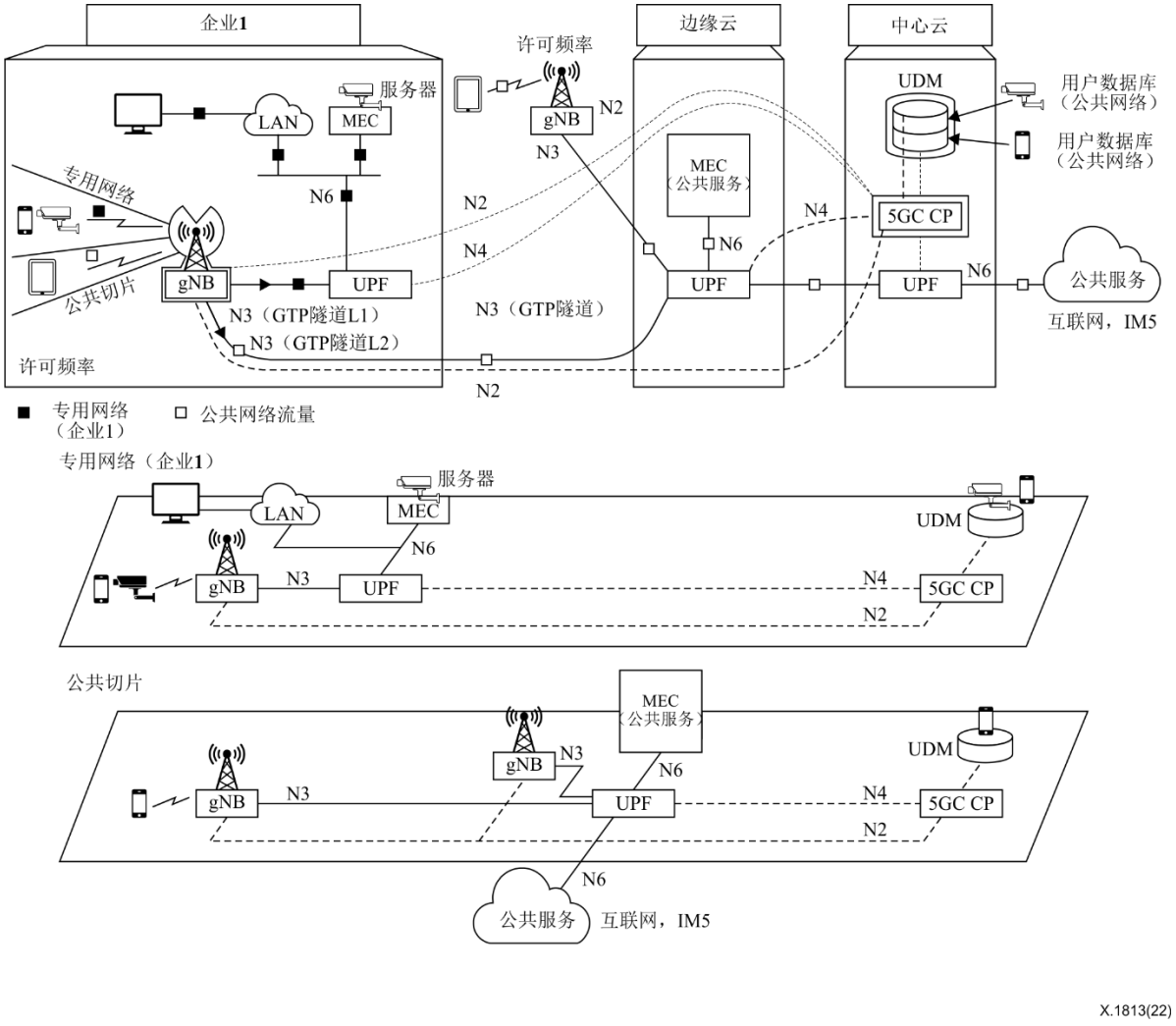
根据[b-Harrison]，IMT-2020专用网络可以作为完全隔离的(a)独立网络部署，也可以部署为与公共网络（b或c）相结合的PLMN的一部分，如图I.1所示

针对(a)，专用网络与公共网络的实体是分开的，可提供完全的数据安全。由于设备和应用服务器之间的网络延迟在几毫秒之内，因此可以实现URLLC应用服务。

针对(b)，gNB、UPF和MEC部署在企业内部。在这种架构中，RAN和控制平面在专用和公共网络之间共享，且可以提供增强的安全性并减少延迟。

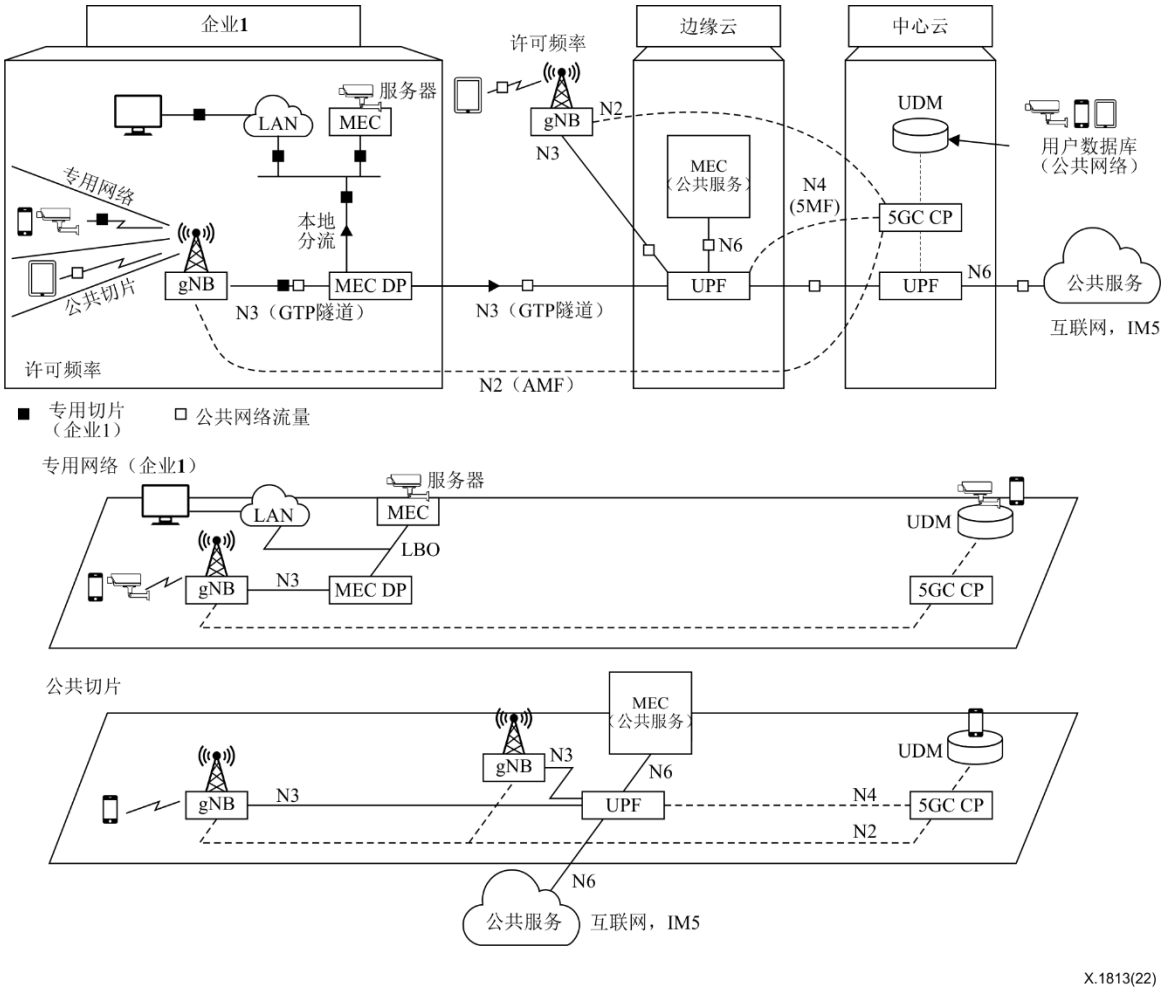
关于(c)，gNB、MEC数据平面（DP）和MEC部署在企业内部，UPF位于移动运营商的边缘云中，远离设备。MEC DP查看来自gNB（GTP decap）的数据包目的IP地址，这些地址属于所有GPRS隧道协议（GTP）的隧道，如果是本地流量，则将用户IP数据包路由至内部专用网。在此架构中，可以提供增强的安全性并减少延迟。

根据[b-Harrison]的观点，图I.1中的部署类型(b)可以在使用网络切片的垂直视图中将其作为图I.2。图I.2说明了图I.1所部署由IMT-2020专用和公共网络共享的类型(b)的详细功能架构。



图I.2 – 图I.1中部署类型(b)的详细功能架构

根据[b-Harrison]的观点，图I.1中的部署类型(c)可以在使用网络切片的垂直视图中将其作为图I.3。图I.3说明了图I.1所部署由IMT-2020专用和公共网络共享的类型(c)的详细功能架构。



图I.3 – 图I.1中部署类型(c)的详细功能架构

上文提到的IMT-2020专网的所有功能架构均是网络运营商为安全和增强URLLC性能而部署的。在IMT-2020专用网络中维护网络性能和安全性是支持URLLC垂直业务最重要的因素之一。其中一种候选方法称为深度数据包检测（DPI），此方法亦在[b-ITU-T Y.2774]建议书和[b-ITU-T Y.2775]建议书中有所描述。然而，这些建议书的范围仅局限于一般移动网络，因此不能应用于IMT-2020专用网络，更具体而言，不能应用于支持URLLC的垂直业务。

参考文献

[b-ITU-T Y.2774] Recommendation ITU-T Y.2774 (2019), *Functional requirements of deep packet inspection for future networks*.

[b-ITU-T Y.2775] Recommendation ITU-T Y.2775 (2019), *Functional architecture of deep packet inspection for future networks*.

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network.*

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

[b-ISO13491-1] ISO-13491-1:2016, *Financial services – Secure cryptographic devices (retail) – Part 1: Concepts, requirements and evaluation methods*. <https://www.iso.org/standard/61137.html>

[b-ISO/IEC 14888-1] ISO/IEC 14888-1:2008, *Information technology – Security techniques – Digital signatures with appendix – Part 1: General*. <https://www.iso.org/standard/44226.html>

[b-ISO/IEC/IEEE 24765] ISO/IEC/IEEE 24765:2017, *Systems and software engineering – Vocabulary*. <https://www.iso.org/standard/71952.html>

[b-ISO/IEC 25010] ISO/IEC 25010:2011, *Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models*. <https://www.iso.org/standard/35733.html>

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. <https://www.iso.org/standard/66435.html>

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*. <https://www.iso.org/standard/63461.html>

[b-ISO/PAS 19450] ISO/PAS 19450:2015, *Automation systems and integration – Object-Process Methodology*. <https://www.iso.org/standard/62274.html>

[b-3GPP TS 22.261] 3GPP TS 22.261 v17.2.0 (2020), *Service requirements for the 5G system (Stage 1, Release 17).* <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3107>

[b-3GPP TS 23.501] 3GPP TS 23.501 v17.0.0 (2021), *System architecture for the 5G System (5GS); Stage 2 (Release 17).* <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144>

[b-3GPP TR 23.734] 3GPP TR 23.734 v16.2.0 (2019), *Study on enhancement of 5G System (5GS) for vertical and Local Area Network (LAN) services*. <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3487>

[b-5G-PPP] 5G PPP Architecture Working Group (2019), *View on 5G Architecture, Version 3.0*. <https://5g-ppp.eu/wp-content/uploads/2019/07/5G-PPP-5G-Architecture-White-Paper_v3.0_PublicConsultation.pdf>

[b-Harrison] Harrison J. Son, (2020), *Private 5G network strategies of Mobile operators and None-mobile operators*. <https://www.netmanias.com/en/?m=view&id=reports&no=14585>

ITU-T系列建议书

系列A	ITU-T工作的组织
系列D	资费及结算原则和国际电信/ICT的经济和政策问题
系列E	综合网络运行、电话业务、业务运行和人为因素
系列F	非话电信业务
系列G	传输系统和媒介、数字系统和网络
系列H	视听及多媒体系统
系列I	综合业务数字网
系列J	有线网络和电视、声音节目及其他多媒体信号的传输
系列K	干扰的防护
系列L	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列M	电信管理，包括TMN和网络维护
系列N	维护：国际声音节目和电视传输电路
系列O	测量设备的技术规范
系列P	电话传输质量、电话设施及本地线路网络
系列Q	交换和信令，以及相关的测量和测试
系列R	电报传输
系列S	电报业务终端设备
系列T	远程信息处理业务的终端设备
系列U	电报交换
系列V	电话网上的数据通信
系列X	**数据网、开放系统通信和安全性**
系列Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列Z	用于电信系统的语言和一般软件问题

瑞士印刷
2022年，日内瓦