Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1813

(09/2022)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad de las IMT-2020

Requisitos de seguridad y control del funcionamiento de servicios verticales que soportan comunicaciones ultrafiables y de baja latencia (URLLC) en redes IMT-2020 privadas

Recomendación UIT-T X.1813

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web (1)	X.1140–X.1149
Seguridad de las aplicaciones	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1319
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Correo certificado	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1350–X.1369
Seguridad en los sistemas de transporte inteligente (STI)	X.1370–X.1399
Seguridad de tecnología de libro mayor distribuido (DLT)	X.1400–X.1429
Seguridad de las aplicaciones (2)	X.1450–X.1459
Seguridad de la web (2)	X.1470–X.1489
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
Ciberdefensa	X.1590–X.1599
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
Protección de los datos	X.1770–X.1789
SEGURIDAD DE IMT-2020	**X.1800–X.1819**

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1813

Requisitos de seguridad y control del funcionamiento de servicios verticales que soportan comunicaciones ultrafiables y de baja latencia (URLLC) en redes IMT-2020 privadas

Resumen

En la Recomendación UIT-T X.1813 se especifican los requisitos de seguridad para el funcionamiento de los servicios verticales que soportan comunicaciones ultrafiables y de baja latencia (URLLC) en las redes privadas IMT-2020. Se identifican las amenazas y los riesgos asociados a la prestación de dichos servicios y se describen escenarios de despliegue de seguridad de las redes privadas IMT-2020 para el funcionamiento de los servicios verticales que soportan URLLC. La supervisión de los contenidos de las comunicaciones queda fuera del alcance de esta Recomendación.

Una red privada IMT-2020, que también se conoce como una red no pública (NPN) IMT-2020, se ha diseñado para el uso exclusivo de una entidad privada, como una empresa, y puede desplegarse en distintas configuraciones utilizando elementos tanto virtuales como físicos. Proporcionará velocidad, baja latencia y otras ventajas previstas por las IMT-2020 para soportar las aplicaciones de la próxima generación.

En los servicios verticales para fábricas inteligentes y ciudades inteligentes que utilizan una red IMT-2020 privada, muchos dispositivos de Internet de las cosas (IoT) emplean comunicaciones masivas entre máquinas (mMTC) y comunicaciones ultrafiables y de baja latencia (URLLC). Estas comunicaciones pueden estar expuestas a amenazas de seguridad y a sus riesgos asociados, y esas amenazas pueden deteriorar la estabilidad del funcionamiento de los servicios verticales que soportan URLLC. Estas no pueden garantizarse cuando el rendimiento de los servicios verticales se ve degradado por estos riesgos.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1813	02-09-2022	17	11.1002/1000/14991

Palabras clave

Detección y respuesta de puntos extremos, DPI, MEC, NPN, red IMT-2020 privada, rendimiento, seguridad, supervisión de red, UPF.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente o derecho de autor, que pueda ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los implementadores que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT-T disponibles en el sitio web del UIT-T en http://www.itu.int/ITU-T/ipr/.

© UIT 2023

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

Página

1 Alcance 1

2 Referencias 1

3 Definiciones 1

3.1 Términos definidos en otros documentos 1

3.2 Términos definidos en esta Recomendación 2

4 Siglas y acrónimos 2

5 Convenios 3

6 Aspectos generales 3

7 Amenazas para los servicios verticales que soportan URLLC en las redes privadas IMT-2020 6

8 Riesgos para los servicios verticales que soportan URLLC en las redes privadas IMT-2020 7

9 Escenarios de despliegue de las funciones de seguridad para el funcionamiento de los servicios verticales que soportan URLLC en las redes privadas IMT-2020 7

10 Requisitos de seguridad y control para el funcionamiento de los servicios verticales que soportan URLLC en las redes privadas IMT-2020 10

10.1 Seguridad de la NMSF 10

10.2 Seguridad de la NMCF 12

Anexo A – Características de la NMSF 13

Anexo B – Características de la NMCF 15

Anexo C – Visualización de los resultados de la monitorización 16

Apéndice I – Casos de utilización de las redes privadas IMT-2020 para servicios verticales 18

Bibliografía 21

Recomendación UIT-T X.1813

Requisitos de seguridad y control del funcionamiento de servicios verticales que soportan comunicaciones ultrafiables y de baja latencia (URLLC) en redes IMT-2020 privadas

1 Alcance

En esta Recomendación se especifican los requisitos de seguridad para el funcionamiento de los servicios verticales que soportan comunicaciones ultrafiables y de baja latencia (URLLC) en las redes privadas IMT-2020. Se identifican las amenazas y los riesgos asociados a la prestación de dichos servicios y se describen escenarios de despliegue de seguridad de las redes privadas IMT-2020 para el funcionamiento de los servicios verticales que soportan URLLC.

La supervisión de los contenidos de las comunicaciones queda fuera del alcance de esta Recomendación para la protección de la privacidad.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación

[UIT-T Y.3102] Recomendación UIT-T Y.3102 (2018), *Marco de la red IMT-2020*.

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 red no pública 5G [b-3GPP TS 22.261]: Una red 5G destinada a una utilización privada.

3.1.2 ataque [b-ISO 13491-1]: Intento realizado por un atacante en el dispositivo para obtener o modificar información sensible o un servicio que no está autorizado a obtener o modificar.

NOTA 1 – Las funciones de red incluyen, entre otras, las funcionalidades de nodo de red como, por ejemplo, gestión de sesión, gestión de movilidad y funciones de transporte, cuyo comportamiento funcional e interfaces están definidos.

NOTA 2 – Las funciones de red pueden implementarse en un *hardware* dedicado o como funciones de *software* virtualizadas.

NOTA 3 – Las funciones de red no se consideran recursos, sino que cualquier función de red puede instanciarse utilizando los recursos.

3.1.3 despliegue [b-ISO/CEI/IEEE 24765]: Fase de un proyecto en la que el sistema se pone en marcha y se resuelven los problemas de la transición.

3.1.4 dominio [b-ISO/CEI 14888-1]: Conjunto de entidades que opera en el marco de una política de seguridad única.

Ejemplo – Certificados de clave pública creados por una única autoridad o por un conjunto de autoridades que utilizan la misma política de seguridad.

3.1.5 Internet de las cosas (IoT) [b-UIT-T Y.4000]: Infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperabilidad de tecnologías de la información y la comunicación presentes y futuras.

3.1.6 monitorización de red [b-ISO/CEI 27033-1]: Proceso de observar y revisar continuamente los datos registrados en operaciones y actividades de red, incluidos ficheros cronológico de auditoría y alertas, y su análisis correspondiente.

3.1.7 función de red [UIT-T Y.3100]: En el contexto de las IMT-2020 una función de procesamiento en una red.

3.1.8 sistema [b-ISO/CEI 27000]: Aplicaciones, servicios, bienes de tecnología de la información o demás componentes de tratamiento de la información.

3.1.9 parte interesada [b-ISO/PAS 19450]: Persona, organización o grupo de personas interesados en el sistema considerado, creado o desplegado, o que puede verse afectado por él.

3.1.10 confianza [b-ISO/CEI 25010]: Grado en que un usuario u otra parte interesada confía en que un producto o sistema se comportará como está previsto.

3.1.11 servicio vertical [b-5G-PPP]: Desde un punto de vista de negocio, un servicio vertical es un servicio orientado a una industria específica o a un grupo de clientes con necesidades especializadas (por ejemplo, servicios de automoción, servicios de entretenimiento, servicios de cibersalud, industria 4.0).

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los términos siguientes:

3.2.1 sistema de comunicaciones IMT-2020: Un sistema que gestiona los procesos de comunicación de las IMT-2020 para los servicios de las IMT-2020.

NOTA 1 – 5G corresponde a IMT-2020 en el contexto del UIT-T.

NOTA 2 – El sistema de comunicaciones IMT-2020 es idéntico al sistema IMT-2020 de esta Recomendación.

3.2.2 ecosistema IMT-2020: Conjunto de partes interesadas que interactúan para componer un sistema IMT-2020 que funciona de forma estable.

NOTA – El término hace referencia al desarrollo de la tecnología de las comunicaciones 5G, donde una comunidad de partes interesadas de la industria y el mundo académico contribuyen con sus productos, tecnologías y conocimientos, para habilitar la funcionalidad en diferentes capas de la pila de valores 5G, por ejemplo, infraestructuras, redes, plataformas, servicios y aplicaciones.

3.2.3 red privada IMT-2020: Red no pública 5G (véase la cláusula 3.1.1) que utiliza tanto elementos virtuales como físicos de los sistemas de comunicaciones IMT-2020 para el uso exclusivo de una entidad privada como una empresa.

3.2.4 servicio IMT-2020: Beneficio proporcionado por el ecosistema IMT-2020.

4 Siglas y acrónimos

En la presente Recomendación se utilizan las siglas y los acrónimos siguientes:

5GC Núcleo 5G (*5G core*)

AMF Función de gestión de acceso y movilidad (*access and mobility management function*)

DDoS Denegación de servicio distribuida (*distributed denial of service*)

DPI Inspección detallada de paquetes (*deep packet inspection*)

EC Computación periférica (*edge computing*)

EDR	Detección y respuesta de puntos extremos (*endpoint detection and response*)
GTP	Protocolo de tunelización de GPRS (*GPRS tunnelling protocol*)
IoT	Internet de las cosas (*Internet of things*)
MEC	Computación periférica multiacceso (*multi-access edge computing*)
MEC DP	Plano de datos de la MEC (*MEC data plane*)
mMTC	Comunicaciones masivas tipo máquina (*massive machine type communications*)
NF	Función de red (*network function*)
NMCF	Función de cliente de monitorización de red (*network monitoring client function)*
NMF	Función de monitorización de red (*network monitoring function*)
NMSF	Función de servidor de monitorización de red (*network monitoring server function*)
NPN	Red no pública (*non-public network*)
RMTP	Red móvil terrestre pública
RTT	Tiempo de ida y vuelta (*round trip time*)
SBA	Arquitectura basada en los servicios (*service-based architecture*)
SMF	Función de gestión de sesión (*session management function*)
UDM	Gestión de datos unificada (*unified data management*)
UE	Equipo de usuario (*user equipment*)
UID	Identidad de usuario (*user ID*)
UPF	Función del plano de usuario (*user plane function*)
URLLC	Comunicaciones ultrafiables y de baja latencia (*ultra-reliable and low latency communication*)

5 Convenios

En la presente Recomendación, se utilizan los siguientes convenios:

La expresión "**se requiere**" indica un requisito que debe cumplirse estrictamente, no permitiéndose desviación alguna si se quiere declarar la conformidad con la presente Recomendación.

La expresión "**se recomienda**" indica que se trata de un requisito recomendado pero que no es absolutamente obligatorio. El cumplimiento de ese requisito no es necesario para declarar la conformidad.

La expresión "**se prohíbe**" indica un requisito que debe cumplirse estrictamente, no permitiéndose desviación alguna si se quiere declarar la conformidad con la presente Recomendación.

La expresión "**se tiene la opción de**" o "**puede opcionalmente**" indica un requisito opcional que se permite, sin que ello signifique en modo alguno su recomendación. El uso de este término no implica que el fabricante deba ofrecer esta opción, y el operador de red/proveedor de servicio puede activar esta función opcionalmente. Significa más bien, que el fabricante tiene la opción de proporcionar esta función sin que ello afecte a la conformidad con la presente especificación.

6 Aspectos generales

El sistema IMT-2020 tiene una arquitectura que permite a los operadores de redes la conectividad y los servicios de datos en base a técnicas, por ejemplo, la virtualización de funciones de red y las redes definidas por *software*. El 3GPP ha definido una arquitectura basada en servicios (SBA) [b-3GPP

TS 23.501], según la cual la funcionalidad del plano de control y los repositorios de datos comunes de la red IMT-2020 se proporcionan mediante un conjunto de funciones de red (NF) interconectadas, cada una de las cuales tiene autorización para acceder a los servicios de las otras. La Figura 1 muestra la arquitectura del sistema IMT-2020.

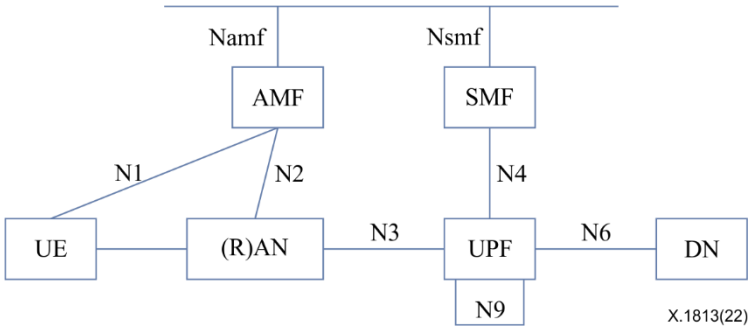

Figura 1 – Arquitectura del sistema IMT-2020

La arquitectura del sistema IMT-2020 definida en [UIT-T Y.3102] y también en [b-3GPP TS 23.501] está compuesta de las siguientes funciones de red:

– Función de gestión de acceso y movilidad (AMF) que proporciona la función de gestión de registro, la función de gestión de conexión, la función de gestión de movilidad, la función de autentificación del acceso, la función de autorización del acceso, la función de gestión de los servicios de ubicación, la función de notificación de los eventos de movilidad de los equipos de usuario (UE), entre otros.

– Red de datos (DN), como servicios de operador, acceso a Internet o servicios de terceros.

– Función de gestión de sesión (SMF) que proporciona las funciones de establecimiento, modificación y liberación de sesión, las funciones de atribución y gestión de la dirección IP de los UE, la función de selección y control del plano de usuario, las interfaces de recogida de datos de tarificación y de soporte de la tarificación, el control y la coordinación de la recogida de datos de tarificación en la función del plano de usuario, notificaciones de datos de enlaces descendentes, soporte de la compresión de encabezamientos, entre otros.

– Función del plano de usuario (UPF) que gestiona el trayecto del plano de usuario de las sesiones de las unidades de datos de protocolo (PDU). El 3GPP soporta tanto los despliegues con una única UPF o con múltiples UPF para una sesión concreta de DPU. La selección de la UPF la realiza la SMF. La UPF proporciona la atribución de la dirección/prefijo IP del UE en respuesta a una solicitud de la SMF, la función de encaminamiento y reenvió de paquetes, la función de inspección de paquetes, el tratamiento de la QoS para el plano de usuario, el almacenamiento en memoria intermedia del enlace descendente y la activación de notificación de datos del enlace descendente, entre otros.

– Namf: identifica una interfaz basada en servicios para la función principal de gestión de la movilidad y el acceso.

– Nsmf: identifica una interfaz basada en servicios para la función de gestión de sesión.

– UE: equipo de usuario.

– (R)AN: red de acceso (radioeléctrico).

La arquitectura del sistema IMT-2020 contiene los siguientes puntos de referencia:

– N1: punto de referencia entre el UE y la AMF.

– N2: punto de referencia entre la (R)AN y la AMF.

– N3: punto de referencia entre la (R)AN y la UPF.

– N4: punto de referencia entre la SMF y la UPF.

– N6: punto de referencia entre la UPF y una red de datos (DN).

– N9: punto de referencia entre dos UPF.

Las redes privadas IMT-2020 se han diseñado para el uso exclusivo de una entidad privada, como una empresa, y pueden desplegarse con distintas configuraciones que utilizan elementos tanto virtuales como físicos del sistema de comunicaciones IMT-2020. Una red privada IMT-2020 debe construirse según los principios de la arquitectura del sistema IMT-2020 definidos en [b-3GPP TS 23.501], que incluyen la flexibilidad y la modularidad de las funcionalidades recién introducidas. La arquitectura funcional de una red privada IMT-2020 se muestra en el Apéndice I.

Las especificaciones 3GPP [b-3GPP TS 23.501] prevén diferentes escenarios de despliegue de las redes privadas. En el nivel más alto, las redes privadas pueden dividirse en dos categorías:

– las redes privadas IMT-2020 desplegadas de manera completamente aislada, redes independientes;

– las redes privadas IMT-2020 desplegadas como segmento de una red pública móvil terrestre (RPMT) en combinación con una red pública.

Por otro lado, la Internet de las cosas (IoT) está definida en [b-UIT-T Y.4000] como una infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperabilidad de tecnologías de la información y la comunicación presentes y futuras. En la presente Recomendación, el principal caso de utilización de unos servicios verticales de este tipo es la IoT. En este contexto los dispositivos IoT pueden ser los dispositivos que representan los UE definidos por 3GPP [b-3GPP TS 22.261].

Ahora que la tecnología IMT-2020 ha entrado en una fase de comercialización, las redes privadas IMT-2020 se utilizarán principalmente para establecer servicios verticales IMT-2020 con dispositivos IoT industriales, como los servicios para las fábricas inteligentes y las ciudades inteligentes que requieren un funcionamiento en tiempo real con comunicaciones ultrafiables y de baja latencia (URLLC). Por lo tanto, las redes privadas IMT-2020 deben satisfacer diversos requisitos en cuanto a seguridad y rendimiento, ya que procesan datos que son sensibles al tiempo con arreglo a la norma [UIT-T Y.3102]. En la Figura 2 se muestra la arquitectura general de seguridad de las redes privadas IMT-2020 de acuerdo con [b-3GPP TR 23.734].

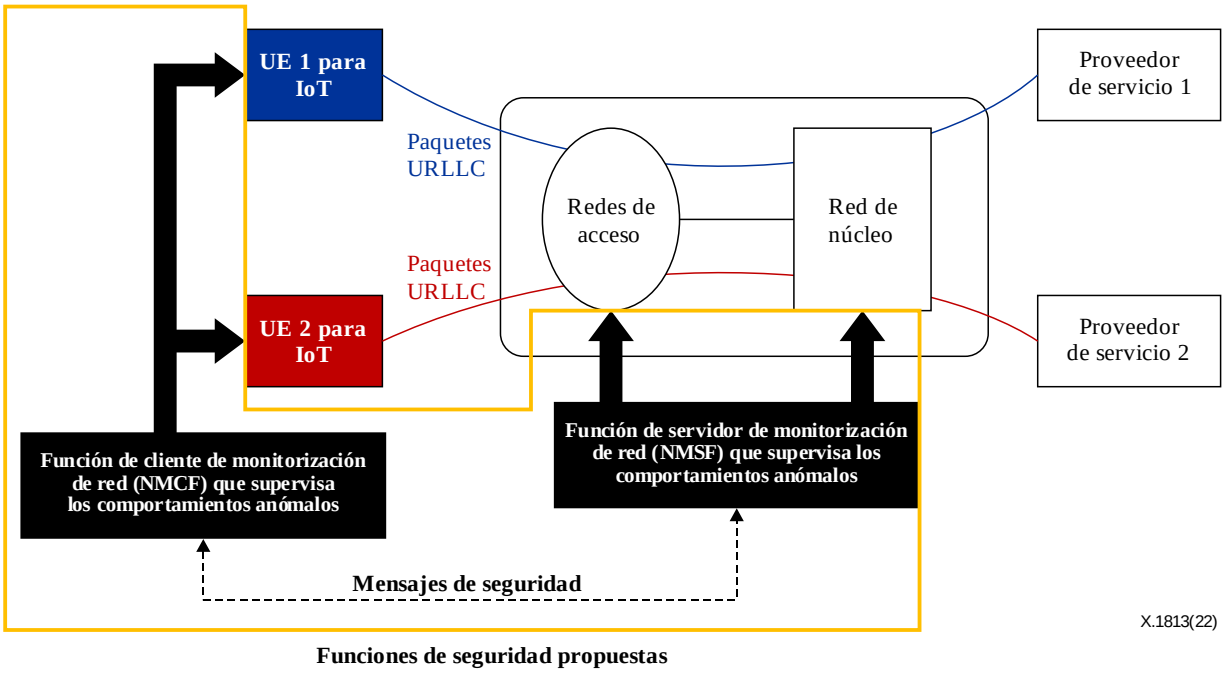

Figura 2 – Arquitectura de seguridad de las redes privadas IMT-2020

En la Figura 2, la arquitectura de seguridad de las redes privadas IMT-2020 permite a los operadores monitorizar la seguridad y el funcionamiento de las comunicaciones entre los nodos de la red y los equipos de usuario de los extremos de usuario de una red privada IMT-2020 para el funcionamiento de los servicios verticales que soportan comunicaciones URLLC.

7 Amenazas para los servicios verticales que soportan URLLC en las redes privadas IMT-2020

La IoT abarca una amplia variedad de posibilidades nuevas y apasionantes, como los sistemas de control y automatización industrial (SCAI), las comunicaciones de vehículos autónomos, las redes eléctricas inteligentes, los sensores de tráfico/autopistas, las comunicaciones con drones, los sensores médicos y la RA/RV, que funcionan en su mayoría de manera automatizada. Los servicios IoT también pueden tener que cumplir las características de las URLLC de los servicios IMT-2020. Según [b-3GPP TS 22.261], las redes privadas están destinadas al uso exclusivo de una entidad privada, como una empresa, y sólo los UE autorizados deberán disponer del derecho a acceder a una red privada.

En un entorno de este tipo, las amenazas para los servicios verticales se identifican, entre otras cosas, como cualquier ataque que pueda afectar a los componentes y los interfaces de la red privada IMT-2020 en lo que respecta a la latencia. Una red privada IMT-2020 puede desplegarse con o sin una UPF/computación periférica multiacceso (MEC). La UPF es accesible desde Internet a través de la interfaz N6 definida por el 3GPP. Por lo tanto, si una red privada IMT-2020 se despliega con UPF y MEC, la interfaz N6 tiene una exposición importante a los ataques, ya que los atacantes pueden acceder a ella desde cualquier punto de Internet. Dichos ataques se pueden producir de forma intencionada o no, desde fuera o desde dentro de una red privada IMT-2020.

Las amenazas contra la UPF, la MEC y la interfaz N6 pueden ser las siguientes:

– ataques de denegación de servicio distribuida (DDoS);
– espionaje del tráfico/datos de los enlaces de comunicación;
– aumento inesperado del tráfico o tráfico anómalo generado por los UE en una red privada IMT-2020.

Las redes privadas IMT-2020 se despliegan de manera privada con componentes e interfaces de red, y parte de ellos son nuevos y diferentes de los de las redes existentes en los aspectos relativos a la seguridad. La interfaz N3 que conecta las redes de acceso y de núcleo utiliza IPsec para la seguridad del transporte. La interfaz N4 conecta la UPF y la AMF. Esta interfaz N4 es cerrada en un núcleo de paquetes evolucionado (EPC) 4G, pero no en el vEPC IMT-2020. Contrariamente a la interfaz X6, las interfaces N3 y N4 no son accesibles desde Internet, pero existe la posibilidad de que se produzcan nuevos tipos de amenazas y de problemas no intencionados.

Las amenazas contra las interfaces N3 y N4 pueden ser las siguientes:

– métodos de control de acceso insuficiente implementados en una red privada IMT-2020;
– limitaciones de las medidas y los procedimientos de seguridad ejecutados por un operador de una red privada IMT-2020;
– un mal diseño o una configuración inadecuada de los componentes de la red privada IMT-2020 que no tienen en cuenta un incremento inesperado de los accesos.

El hecho de que los expertos no estén acostumbrados a muchas de las nuevas características de la red IMT-2020 también pueden suponer unas amenazas y unos obstáculos involuntarios.

8 Riesgos para los servicios verticales que soportan URLLC en las redes privadas IMT-2020

Las redes privadas IMT-2020 proporcionan esencialmente una red de gran confianza dentro de la infraestructura de la IoT, ya que el 3GPP ha normalizado las redes privadas IMT-2020 con el propósito de garantizar la seguridad de los servicios verticales emergentes de las IMT-2020.

A pesar de los métodos de seguridad convencionales como la autentificación, la autorización y la confidencialidad de los datos que proporcionan las normas de seguridad, entre otras las del 3GPP, las redes privadas IMT-2020 pueden quedar expuestas a numerosos riesgos. Los métodos de seguridad existentes no pueden, por ejemplo, acabar con las amenazas provocadas por el comportamiento irregular de los equipos de usuario que operan en la red privada IMT-2020.

Como las redes IMT-2020 poseen unas características basadas en el *software* más importantes, pueden estar expuestas a un número mayor de riesgos relacionados con el *software*, como los errores en los procedimientos de actualización, los fallos de desarrollo y los errores de configuración de *software*. Como resultado, una red IMT-2020 puede experimentar degradación del rendimiento debido a los diferentes riesgos indicados.

En este contexto, estos riesgos pueden tener los efectos siguientes:

– Funcionamiento inestable y peligroso de los servicios verticales. Los comportamientos anómalos de los dispositivos IoT que operan en la red IMT-2020 pueden suponer una amenaza para el funcionamiento normal de una infraestructura de ciudad inteligente.

– Destrucción, modificación o alteración de información almacenada dentro de la infraestructura de una red IMT-2020, o que se comunica por ella.

– Degradación del funcionamiento del servicio URLLC de las IMT-2020: si una red IMT-2020 no puede garantizar los requisitos de servicio de baja latencia de las URLLC de las IMT-2020, la red puede experimentar degradación del rendimiento, lo que repercutiría negativamente en los servicios verticales cronosensibles. Así, por ejemplo, dado que las fábricas inteligentes están diseñadas de acuerdo con los requisitos de las URLLC, la calidad y la velocidad de la producción pueden verse reducidas si no se satisfacen los requisitos de baja latencia. Esto no solo puede provocar enormes pérdidas económicas, sino que también puede causar accidentes de seguridad. Otro ejemplo sería la calidad de imagen de las cámaras de seguridad, que puede degradarse significativamente debido al retraso de la conexión de varios sensores.

Por lo tanto, es necesario desarrollar requisitos de seguridad para el funcionamiento de los servicios verticales que soportan URLLC en las redes privadas IMT-2020, con el fin de hacer frente a las amenazas y los riesgos señalados.

9 Escenarios de despliegue de las funciones de seguridad para el funcionamiento de los servicios verticales que soportan URLLC en las redes privadas IMT-2020

En este apartado se definen los escenarios de despliegue de las funciones de seguridad para el funcionamiento de los servicios verticales que soportan URLLC en una red privada IMT-2020. La arquitectura de seguridad de las redes privadas IMT-2020 está constituida por las funciones de monitorización de la red (NMF). Las NMF constan de una función de servidor de monitorización de red (NMSF) y una función de cliente de monitorización de red (NMCF). Las NMF pueden implementarse mediante una función de inspección detallada de paquetes (DPI) instalada en un nodo de red o mediante un nodo de red DPI dedicado.

Las NMSF pueden configurarse como nodos de red independientes separados de la UPF o la MEC. En concreto, las NMSF deberán colocarse en la entrada o la salida de una UPF o MEC para que puedan monitorizar los paquetes de las mismas.

Existen tres escenarios de despliegue de las NMSF, que son los siguientes:

a) La NMSF se integra como un nodo en la MEC.

b) La NMSF se implementa como un nodo independiente para monitorizar los paquetes de salida de la UPF.

c) Múltiples NMSF están configuradas de tal manera que una primera NMSF está integrada como un nodo en la MEC y una segunda NMSF está implementada como nodo independiente para monitorizar los paquetes de salida de la UPF.

En estos tres escenarios de despliegue, el hecho de que se asigne a las NMSF, la o las IP designadas, es una cuestión de implementación. En estos tres escenarios de despliegue, la NMCF está integrada en los UE.

En la Figura 3 se muestra el escenario de despliegue A de la arquitectura de seguridad de las redes privadas IMT-2020 en el que se configuran múltiples NMCF y las NMSF.

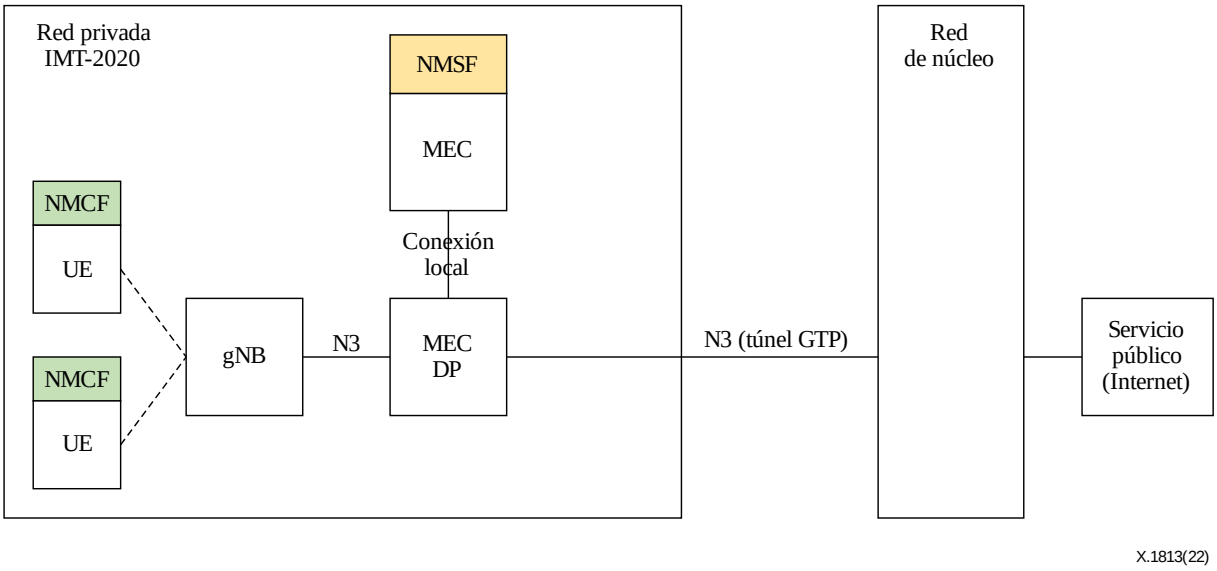

Figura 3 – Escenario de despliegue A

En el escenario de la Figura 3, las NMCF pueden estar integradas en cada UE, en particular en los dispositivos IoT, que se comunican con un gNB. La integración de las NMCF en los dispositivos IoT es una de las soluciones efectivas para garantizar la seguridad y el funcionamiento de las URLLC en las redes privadas IMT-2020. Las NMCF pueden implementarse mediante *software* y también pueden denominarse entidades de detección y respuesta de puntos extremos (EDR) o micromotores (ME). El servidor de las NMCF puede estar ubicado en la red privada IMT-2020, en una nube periférica o en un dominio público de red (Internet). Los UE están conectados al gNB de forma inalámbrica. Cada UE envía paquetes al gNB o recibe paquetes del gNB. El gNB está conectado a la red de núcleo IMT-2020 o a una red local a través de las interfaces N3 y N4. Los paquetes fluyen a través de las interfaces N3 y N4.

Si se asigna una dirección IP a la NMSF, entonces la NMCF y la NMSF se comunican entre sí a través de N3 y N4 para intercambiar mensajes de seguridad entre ellas, como puede ser el resultado de la monitorización en la NMCF.

En el caso del escenario A, aunque no se muestra en la Figura 3, también puede integrarse una NMSF adicional en el plano de datos de la MEC (MEC DP), de modo que las dos NMSF puedan supervisar tanto el tráfico de la red privada como el de la red pública hacia o desde los UE. La NMSF también puede configurarse como una entidad independiente separada de la MEC.

En la Figura 4, se muestra el escenario de despliegue B de la arquitectura de seguridad de las redes privadas IMT-2020 en el que se configuran múltiples NMCF y las NMSF.

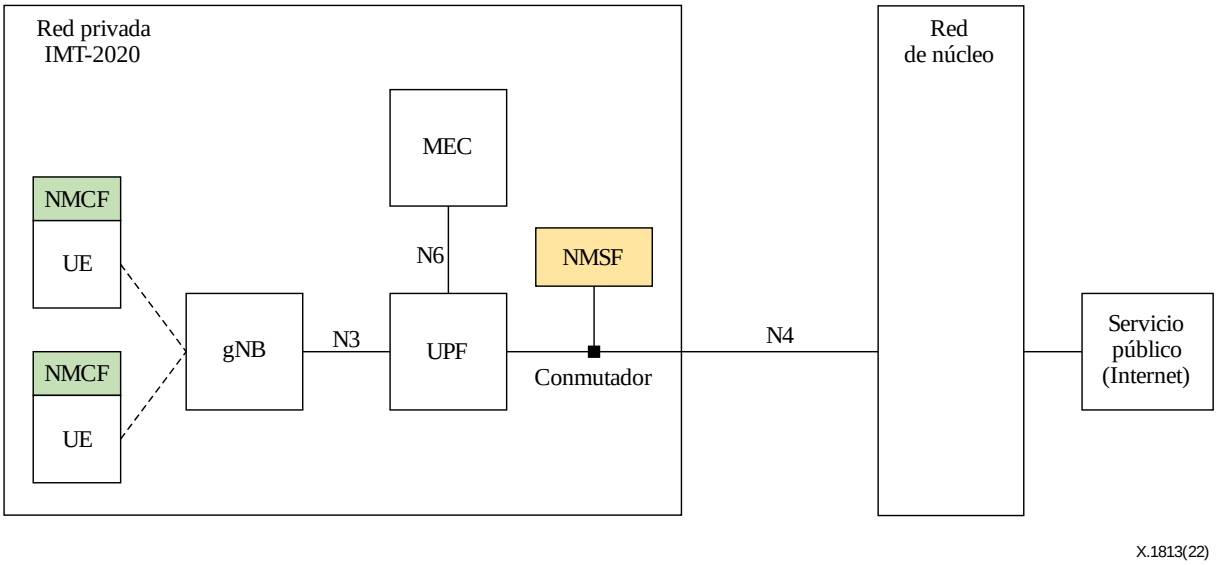

Figura 4 – Escenario de despliegue B

En el escenario de la Figura 4, la NMSF se implementa como nodo independiente fuera de la UPF para monitorizar los paquetes de salida de dicha UPF. Puede utilizarse un conmutador para replicar los paquetes de la UPF. Si se asigna una dirección IP a la NMSF, entonces las NMCF y la NMSF se comunican entre sí a través de N3 y N4 para intercambiar mensajes de seguridad entre ellas, como puede ser el resultado de la monitorización generado en un UE (nodo de cliente). Si la red privada IMT-2020 utiliza una función de encriptación de nodo a nodo como IPsec, las NMSF pueden configurarse en un punto donde los paquetes desencriptados salen del nodo.

En la Figura 5 se muestra el escenario de despliegue C de la arquitectura de seguridad de las redes privadas IMT-2020 en el que se configuran múltiples NMF.

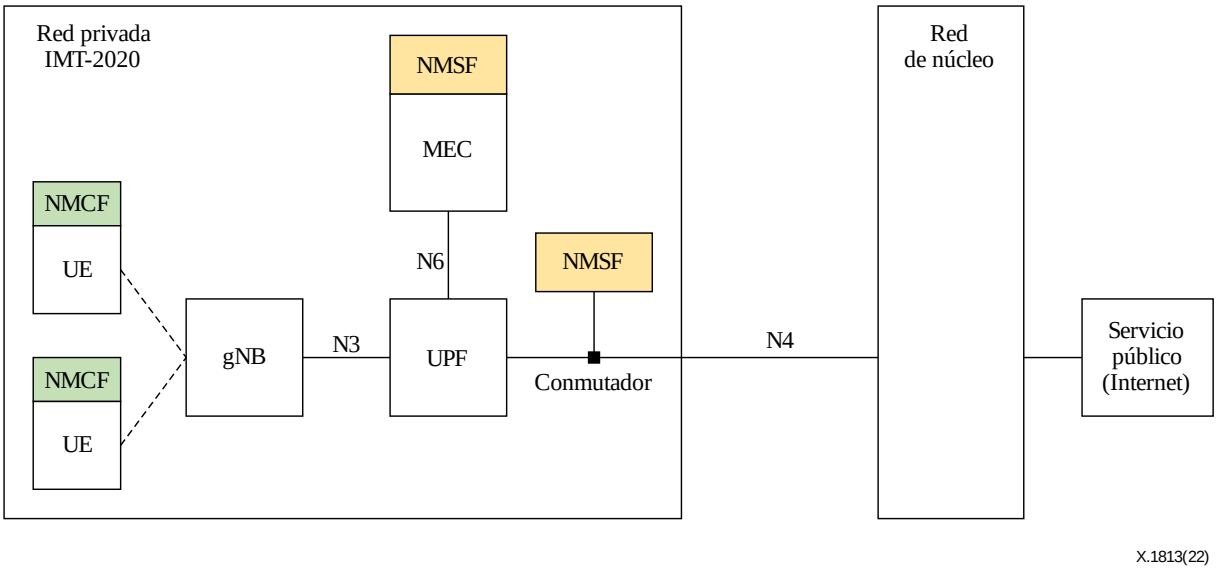

Figura 5 – Escenario de despliegue C

En el escenario de la Figura 5, no solo se integra la NMSF en la MEC, sino que también se implementa como nodo independiente fuera de la UPF para monitorizar la salida de paquetes de la UPF. Si se asignan direcciones IP a las NMSF, entonces las NMCF y las NMSF se comunican entre sí a través de N3 y N4 para intercambiar mensajes de seguridad entre ellas, como puede ser el resultado de la monitorización generado en un UE (nodo de cliente). Si la red privada IMT-2020 utiliza una función de encriptación de nodo a nodo como IPsec, las NMSF pueden configurarse en un punto donde los paquetes desencriptados salen del nodo.

Los tres escenarios descritos no son excluyentes entre sí, y la utilización de un modo u otro depende del coste o de las características de la red, entre otros. También son posibles otros despliegues diferentes de las NMSF y las NMCF. Por ejemplo, las NMSF se pueden integrar en cualquiera de los nodos de red junto con la UPF y/o la MEC.

Por tanto, desde la perspectiva de la arquitectura funcional de la red, la monitorización de la seguridad y el funcionamiento puede realizarse utilizando la NMSF instalada en la MEC y/o la UPF y las NMCF instaladas en los dispositivos IoT, y un protocolo de señalización entre las NMSF y las NMCF.

10 Requisitos de seguridad y control para el funcionamiento de los servicios verticales que soportan URLLC en las redes privadas IMT-2020

En este apartado se identifican los requisitos de seguridad y control para el funcionamiento de los servicios verticales que soportan URLLC en una red privada IMT-2020. Una red privada IMT-2020 requiere un nivel de seguridad y rendimiento más alto que las redes convencionales debido al gran volumen de datos intercambiados entre los numerosos dispositivos de cliente/sensores y los servidores centrales que los controlan. Además, los requisitos de las URLLC de las IMT-2020 también deben cumplirse en la zona periférica, de acuerdo con la [UIT-T Y.3102].

Para los escenarios de despliegue de redes privadas IMT-2020 con NMSF y NMCF, los requisitos generales de seguridad y control para el funcionamiento de los servicios verticales que soportan URLLC son los siguientes:

a) Se requiere la monitorización y la detección del comportamiento anómalo de los UE y de las redes privadas IMT-2020 para mitigar los riesgos de seguridad.

b) Se requiere la monitorización del funcionamiento de los servicios verticales que soportan URLLC.

c) Se requiere alertar al administrador de la red sobre el comportamiento anómalo de los UE y de las redes privadas IMT-2020 para que se puedan resolver los problemas y restaurar las capacidades de las URLLC a tiempo.

Opcionalmente, se recomienda visualizar los comportamientos anómalos de los UE y de las redes privadas IMT-2020 para solucionarlos de una forma más eficaz. En el Anexo C se describe la visualización de los resultados de la monitorización.

10.1 Seguridad de la NMSF

La seguridad requerida para la NMSF es la siguiente:

a) Se requiere que la NMSF proporcione al menos una función de replicación de los paquetes transmitidos y recibidos entre un nodo cliente y un nodo servidor, obteniendo así al menos un paquete replicado. El nodo de cliente es un UE o un dispositivo IoT. La replicación de paquetes es una técnica que recoge y analiza en tiempo real los paquetes intercambiados en un nodo específico. La NMSF puede disponer de una función de conmutación para la replicación de paquetes.

b) Se requiere que la NMSF determine los comportamientos anómalos o los problemas de seguridad que ponen en peligro la seguridad y el funcionamiento de una red privada IMT-2020, a partir de la información incluida en los paquetes replicados.

c) Si se asigna una dirección IP a una NMSF, se requiere que la NMSF reciba un paquete de comprobación de seguridad de la NMCF, utilizando el formato de paquete TCP, y calcule el tiempo de ida y vuelta (RTT) basándose en el paquete de comprobación de seguridad recibido.

En la Figura 6 se muestra el paquete de comprobación de seguridad con el formato de paquete TCP.

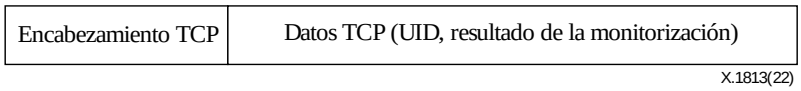

Figura 6 – Paquete de comprobación de seguridad con el formato de paquete TCP

Cuadro 1 – Campos del paquete de comprobación de seguridad

Campo	Longitud en bytes	Descripción
ID de usuario (UID)	4	Este campo contiene un identificador de usuario (UID) de un equipo de usuario (UE)
Longitud	2	Este campo contiene la longitud en bytes del campo resultado de la monitorización
Resultado de la monitorización	Variable	Este campo contiene la información de actividad, la utilización de CPU y la utilización de memoria de un UE

d) Si no se asigna una dirección IP a la NMSF, se requiere que la NMSF replique un paquete de comprobación de seguridad transmitido por la NMCF, utilizando el formato de paquete de protocolo de datagrama de usuario (UDP), a un nodo servidor y calcule el tiempo de ida y vuelta (RTT) basándose en el paquete de comprobación de seguridad replicado.

En la Figura 7 se muestra el paquete de comprobación de seguridad con el formato de paquete UDP.

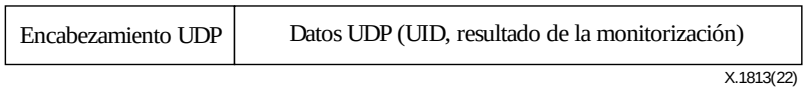

Figura 7 – Paquete de comprobación de seguridad con el formato de paquete UDP

Cuadro 2 – Campos del paquete de comprobación de seguridad

Campo	Longitud en bytes	Descripción
UID	4	Este campo contiene un identificador de usuario (UID) de un equipo de usuario (UE)
Longitud	2	Este campo contiene la longitud en bytes del campo resultado de la monitorización
Resultado de la monitorización	Variable	Este campo contiene la información de actividad, la utilización de CPU y la utilización de memoria de un UE

e) Se recomienda que la NMSF proporcione alarmas de los comportamientos anómalos que dificultan el cumplimiento de los requisitos de las URLLC, en base al estado de la seguridad y el funcionamiento. Cuando se detecta un comportamiento anómalo que pone en peligro la seguridad y el funcionamiento, la NMSF envía una alarma al usuario para que éste pueda responder adecuadamente al comportamiento anómalo. A continuación, la NMSF envía la información de alarma a un controlador de seguridad que le encarga tomar las medidas oportunas ante el comportamiento anómalo, es decir, el apagado de la red. Las informaciones de alarma se envían a través de las interfaces N3 y N4, proporcionadas por el protocolo de señalización 3GPP.

El algoritmo normativo del Anexo A permite realizar las funciones detalladas de la NMSF para la monitorización del rendimiento y la seguridad basada en la replicación.

10.2 Seguridad de la NMCF

La seguridad requerida para la NMCF es la siguiente:

a) La NMCF debe funcionar con los recursos de computación de los diferentes nodos de cliente o de los sensores IoT y se recomienda que utilice el mínimo número de recursos necesarios para que las funciones se realicen de forma adecuada.

b) Se requiere que la NMCF recoja los paquetes o información interna transmitida o recibida por los nodos de cliente a través de la red.

c) Se requiere que la NMCF monitorice y determine si existe una amenaza de seguridad en la red asociada con el nodo de cliente, incluida la propia NMCF, en base a los paquetes recogidos o a la información interna. Si la información interna indica un valor igual o mayor que un umbral, la NMCF determina que existe una amenaza de seguridad en la red. Ejemplos de información interna pueden ser la utilización de la CPU de un nodo de cliente, la utilización de la memoria de un nodo de cliente, etc.

d) Si se asigna una dirección IP a la NMSF, se requiere que la NMCF genere un paquete de comprobación de seguridad utilizando el formato de paquete TCP con el resultado de la monitorización que se muestra en la Figura 6 y envíe el paquete de comprobación de seguridad a la NMSF.

e) Si no se asigna una dirección IP a la NMSF, se requiere que la NMCF genere un paquete de comprobación de seguridad utilizando el formato de paquete UDP con el resultado de la monitorización que se muestra en la Figura 7 y envíe el paquete de comprobación de seguridad a un nodo servidor para que la NMSF pueda replicar el paquete de comprobación de seguridad.

f) Se recomienda que la NMCF muestre una alarma por cualquier funcionamiento anómalo del UE a un usuario de los dispositivos IoT.

En el caso de la NMCF, es más probable que recoja unos datos más precisos; por otra parte, la NMCF puede dejar de funcionar en caso de que se produzca un problema en el que, por ejemplo, se desconecte la alimentación de un equipo en funcionamiento normal. En consecuencia, la supervisión de la seguridad y del funcionamiento por parte de la NMSF es esencial.

Sin embargo, la supervisión de todos los flujos de datos de una gran cantidad de UE conectados a la red privada IMT-2020 puede suponer una gran carga para la NMSF y, en este caso, es necesaria la colaboración con la NMCF para supervisar de forma efectiva las amenazas a la red.

El algoritmo normativo del Anexo B permite realizar las funciones detalladas que implementan los requisitos de la NMCF.

Anexo A

Características de la NMSF

(Este anexo forma parte integrante de la presente Recomendación.)

De acuerdo con la presente Recomendación, la NMSF determina la existencia de comportamientos anómalos que suponen una amenaza para la seguridad y el funcionamiento en base a los paquetes replicados o a la información relacionada con los paquetes replicados. La NMSF determina la existencia de comportamientos anómalos calculando unos índices o parámetros relacionados con el funcionamiento y la seguridad de la red privada IMT-2020 y comparando los resultados obtenidos con los valores de referencia de los requisitos de los servicios de comunicaciones (IMT-2020 o LTE). En este caso, los requisitos del servicio de comunicación pueden obtenerse a partir de la información de acceso de un dispositivo IoT.

La Figura A.1 muestra un método para la medición del tiempo de ida y vuelta (RTT), que utiliza un paquete replicado, como indicador relacionado con el funcionamiento y la seguridad de la red privada IMT-2020 y para la determinación de los comportamientos anómalos que suponen una amenaza para la seguridad y el funcionamiento de la red privada IMT-2020 en base al RTT.

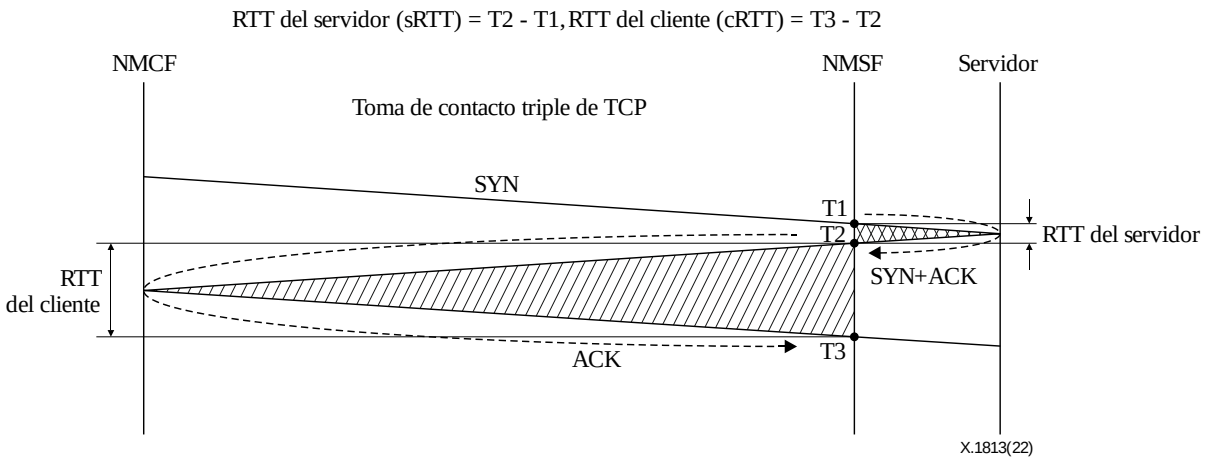

Figura A.1 – Medición del RTT

En la Figura A.1, en el escenario de toma de contacto triple relacionado con la transmisión y recepción de una señal de sincronización (SYN), la NMSF calcula el RTT de una red utilizando paquetes replicados entre un usuario y un servidor a través de la red. En el ejemplo, después de extraer y almacenar los tiempos de los tres paquetes (SYN, SYN+ACK y ACK) intercambiados entre la NMCF (es decir un cliente) y el servidor de la NMSF (o MEC), la NMSF garantiza al menos una de las tres informaciones de tiempos, T1, T2 o T3. La NMSF calcula el RTT debido al servidor (sRTT) restando T1 a T2 (T2 – T1), el RTT debido al cliente (cRTT) a partir de T3 – T2 y el RTT total de la red a partir de cRTT + sRTT, es decir T3 – T1. Al realizar el cálculo de cada transacción, la NMSF realiza el cálculo de toda la red.

La NMSF analiza la existencia de amenazas para el funcionamiento y la seguridad de la red privada IMT-2020 determinando si el sRTT, el cRTT y el RTT de la red cumplen los requisitos de las URLLC de las redes privadas IMT-2020. La Figura A.2 muestra la forma de identificar las zonas en donde se producen problemas de funcionamiento utilizando el sRTT y el cRTT en las redes privadas IMT-2020.

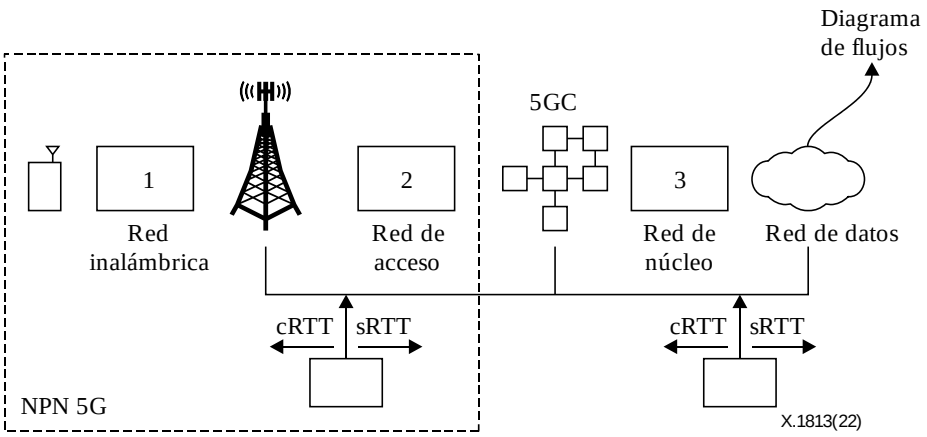

Figura A.2 – Identificación de las zonas con problemas de funcionamiento en una red privada IMT-2020

Además de la RTT, pueden utilizarse otros índices diferentes como indicadores para determinar una amenaza para el funcionamiento o la seguridad. Ejemplos típicos de índices pueden ser la información relativa al tiempo de espera de una respuesta, que representa el tiempo de latencia para que el servidor de la NMSF (o MEC) reciba los primeros datos asociados al contenido de una URL, en respuesta a la solicitud de contenido por parte de un cliente; el número de sesiones en espera de respuesta, que representa el número de sesiones que están en un estado en el cual no se ha recibido todavía la respuesta a una solicitud enviada por el cliente; los BPS (bloques por segundo), las CPS (confirmaciones por segundo), las TPS (transacciones por segundo), los errores HTTP 40x o 50x; la información sobre la transmisión y recepción de datos obtenida a partir de un paquete replicado; las informaciones estadísticas obtenidas a partir de un conjunto de paquetes replicados; y la información de actividad que representa la posibilidad de conectarse a un dispositivo IoT o a un servidor NMCF.

Utilizando estos índices, se puede implementar un algoritmo para determinar las amenazas para el funcionamiento y la seguridad de varias maneras. Por ejemplo, el NMSF puede determinar la existencia de una amenaza para la seguridad de la red en base a la información sobre el tráfico (capas OSI 3 y 4), incluyendo información sobre un flujo de paquetes e información sobre un protocolo (capa OSI 7).

Además de lo anterior, pueden utilizarse otras técnicas para detectar una amenaza de seguridad en la red, como la detección de las amenazas de seguridad en base a la información de los paquetes (por ejemplo, si el número de conexiones en una sección desde una IP de origen predeterminada hasta una IP de destino, o el BPS de un servidor, o las solicitudes de una URL, superan un valor umbral predeterminado, se determina que se trata de una amenaza de seguridad), la detección de las amenazas de seguridad en base a la información de tráfico (utilizando, por ejemplo, una técnica de agrupación basada en un gráfico de distribución del tráfico que determina que se ha producido un volumen de tráfico que excede el valor de un umbral predeterminado, se determina entonces que se ha producido un problema de seguridad en una red privada IMT-2020), la detección de amenazas de seguridad en base a la información de los protocolos, la detección basada en las anomalías, la detección basada en las firmas o en el uso indebido, la detección basado en el análisis de los protocolos basados en estados, y la detección basada en las especificaciones. El contenido de las comunicaciones entre las NMCF y los servidores de las NMCF también puede incluirse en el análisis de la NMSF.

Anexo B

Características de la NMCF

(Este anexo forma parte integrante de la presente Recomendación.)

Para la integración del servidor de la NMCF y la NMSF, se requiere un protocolo para el intercambio de información relacionada con la seguridad entre la NMCF (o el servidor de la NMCF) y la NMSF.

En primer lugar, la NMCF determina si existe una amenaza para la seguridad de la red utilizando los estados de los dispositivos IoT necesarios para su propio servicio, información del estado del sistema o de los registros, y el RTT. El estado de un dispositivo IoT necesario para el servicio incluye la carga de la CPU, la utilización de la memoria, la utilización del almacenamiento y la información de actividad. Por ejemplo, cuando la utilización de la memoria es igual o mayor que un valor umbral definido o el RTT es mayor que un valor umbral definido, la NMCF determina que se ha producido un comportamiento anómalo que supone una amenaza para la seguridad y el funcionamiento. Otro ejemplo es cuando la información de los registros indica que una entidad con una IP no autorizada ha intentado iniciar una sesión en un nodo de cliente, o que se ha llevado a cabo un proceso desconocido, la NMCF determina que se ha producido un comportamiento anómalo que supone una amenaza para la seguridad y el funcionamiento.

La NMCF transmite entonces el valor del resultado de la monitorización que determina la existencia de una amenaza para la seguridad al servidor de la NMCF o a la NMSF. En otras palabras, la NMSF recibe en tiempo real un resultado de monitorización correspondiente a una amenaza para la seguridad de la red determinado por un punto terminal. En este momento, debe identificarse el dispositivo IoT a partir de la información recogida por el servidor en relación con la NMCF y el contenido del análisis de la NMSF, de modo que el contenido generado por dicho dispositivo IoT pueda diferenciarse de los demás.

El método descrito puede reducir la carga de la NMSF central al realizar la monitorización de las amenazas en los puntos terminales, como la NMCF, y, en consecuencia, puede mejorar el rendimiento de la monitorización en relación con las amenazas para el funcionamiento y la seguridad de la red.

Anexo C

Visualización de los resultados de la monitorización

(Este anexo forma parte integrante de la presente Recomendación.)

La Figura C.1 muestra un ejemplo de visualización de la monitorización del funcionamiento y la seguridad de la red y el sistema utilizando la NMSF.

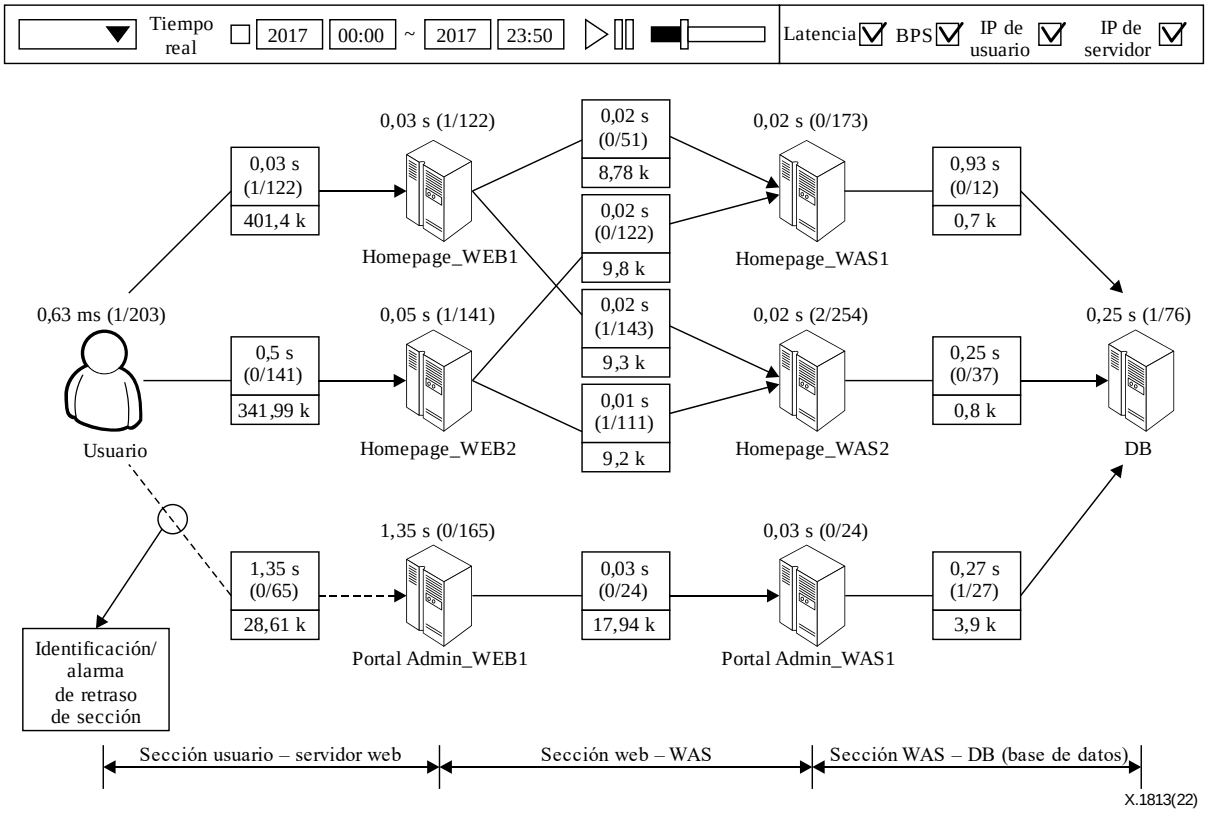

Figura C.1 – Ejemplo de visualización de la monitorización del funcionamiento y la seguridad de la red y el sistema

En el esquema que se muestra en la Figura C.1, los resultados de los análisis en base a los indicadores de funcionamiento o de seguridad se visualizan en tiempo real y se comunican a los usuarios en forma de alarma. Los gestores de la red pueden hacer frente a las amenazas de forma inmediata gracias a estos resultados. Es decir, los resultados analizados se interpretan en términos de funcionamiento y desde la perspectiva de la seguridad. En cuanto se detectan comportamientos anómalos, un mensaje de alarma llega a los gestores de la red.

Es deseable que la visualización muestre de forma intuitiva y clara los enlaces entre las entidades de una red. La visualización se implementa de manera que la NMSF genera los indicadores relacionados con el rendimiento y la seguridad como objetos, representa los objetos generados en un espacio visualizado y genera un diagrama de flujos que representa los flujos de tráfico de la red. Para ello, los objetos provienen de la generación de indicadores relacionados con el funcionamiento y la seguridad asociados a una primera entidad, de indicadores relacionados con el funcionamiento y la seguridad asociados a una segunda entidad, y de indicadores relacionados con el funcionamiento y la seguridad asociados a un enlace que conecta la primera entidad y la segunda.

Para una mayor claridad, se representa una línea entre la primera entidad y la segunda entidad en el diagrama de flujos basada en el objeto generado a partir de los indicadores relacionados con el

funcionamiento o la seguridad de los enlaces. Se pueden añadir elementos de color para diferenciarlos. Dicho de otra manera, al menos uno de los elementos de color, forma y grosor se visualiza de forma diferenciada en función de los indicadores de funcionamiento o seguridad asociados a los enlaces.

Al utilizar esta función de visualización, se puede conseguir una visibilidad y una claridad de todas las secciones del servicio. No solo mejora la prevención de los problemas de los servicios de la red gestionándolos, sino que da a la red la capacidad de hacer frente con facilidad a las amenazas en una gran infraestructura de IoT, como pueden ser las fábricas y las ciudades inteligentes.

Apéndice I

Casos de utilización de las redes privadas IMT-2020 para servicios verticales

(Este apéndice no forma parte integrante de la presente Recomendación.)

Esta Recomendación se basa en tres tipos de arquitectura de red privada IMT-2020, como se muestra en la Figura I.1.

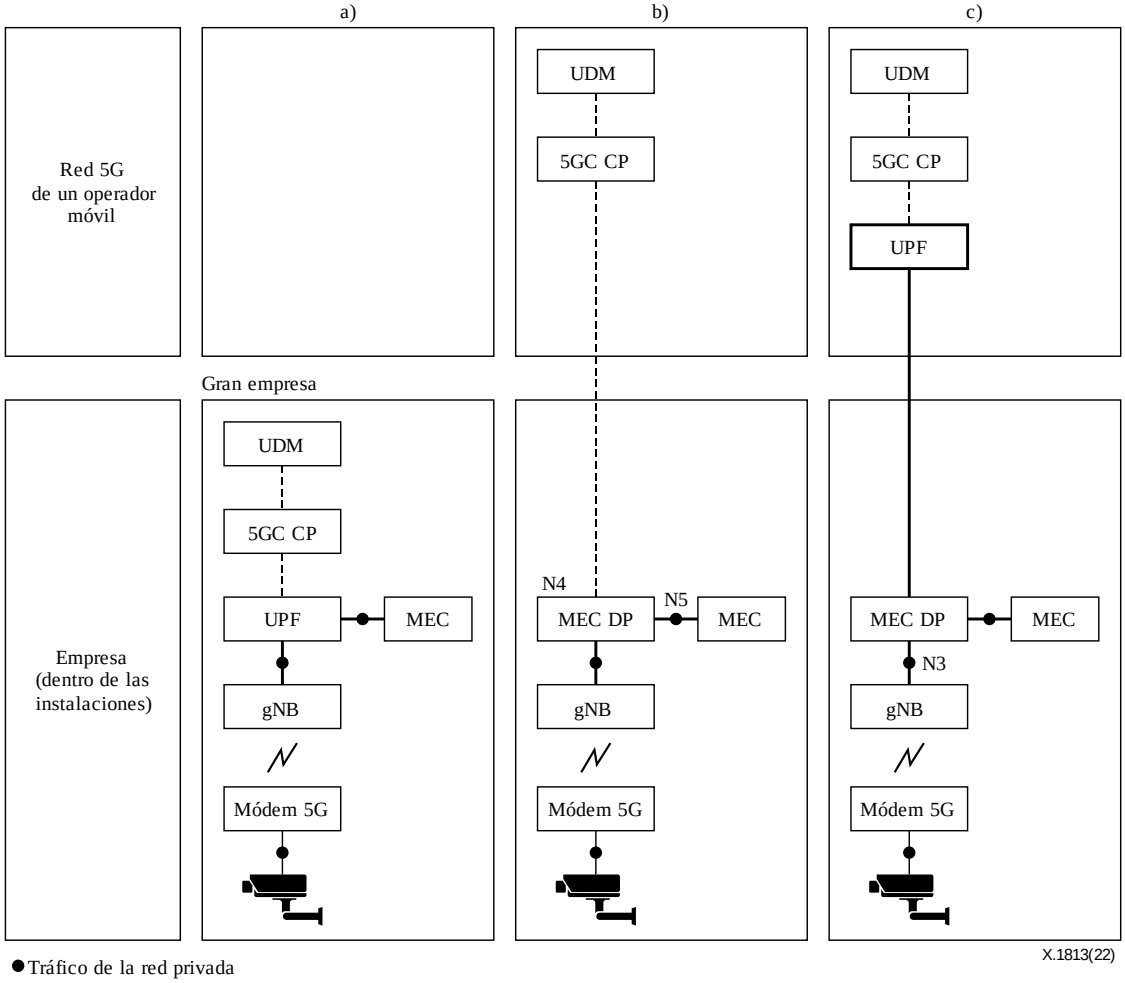

Figura I.1 – Tres tipos de despliegue de una red privada IMT-2020

De acuerdo con [b-Harrison], las redes privadas IMT-2020 pueden desplegarse como redes completamente aisladas a), independientes, o pueden desplegarse como un segmento de una RMTP junto con una red pública (b o c), como se muestra en la Figura I.1.

En el caso a), la red privada está físicamente separada de la red pública, lo que proporciona una seguridad total de los datos. Dado que el retardo de la red entre el dispositivo y el servidor de aplicaciones es de varios ms, se pueden implementar servicios de aplicaciones URLLC.

En el caso b), se despliega el gNB, la UPF y la MEC dentro de la empresa. En esta arquitectura, la RAN y el plano de control se comparten entre la red privada y la red pública, y se puede proporcionar una mayor seguridad y reducción de los retrasos.

En el caso c), el gNB, el plano de datos (DP) de la MEC y la MEC se despliegan dentro de la empresa, y la UPF se encuentra en la nube periférica del operador móvil, lejos de los dispositivos. El DP de la MEC examina las direcciones IP de destino de los paquetes provenientes de todos los túneles del

protocolo de tunelización GPRS (GTP) procedentes del gNB (GTP decap) y encamina los paquetes IP de usuario hacia la red privada interna si se trata de tráfico local. En esta arquitectura, se puede proporcionar una mayor seguridad y reducción de los retrasos.

De acuerdo con [b-Harrison], el tipo de despliegue b) de la Figura I.1 puede representarse como en la Figura I.2 con una vista vertical utilizando la segmentación de red. La Figura I.2 muestra una arquitectura funcional detallada para el tipo de despliegue b) de la Figura I.1, que comparten una red privada y otra pública IMT-2020.

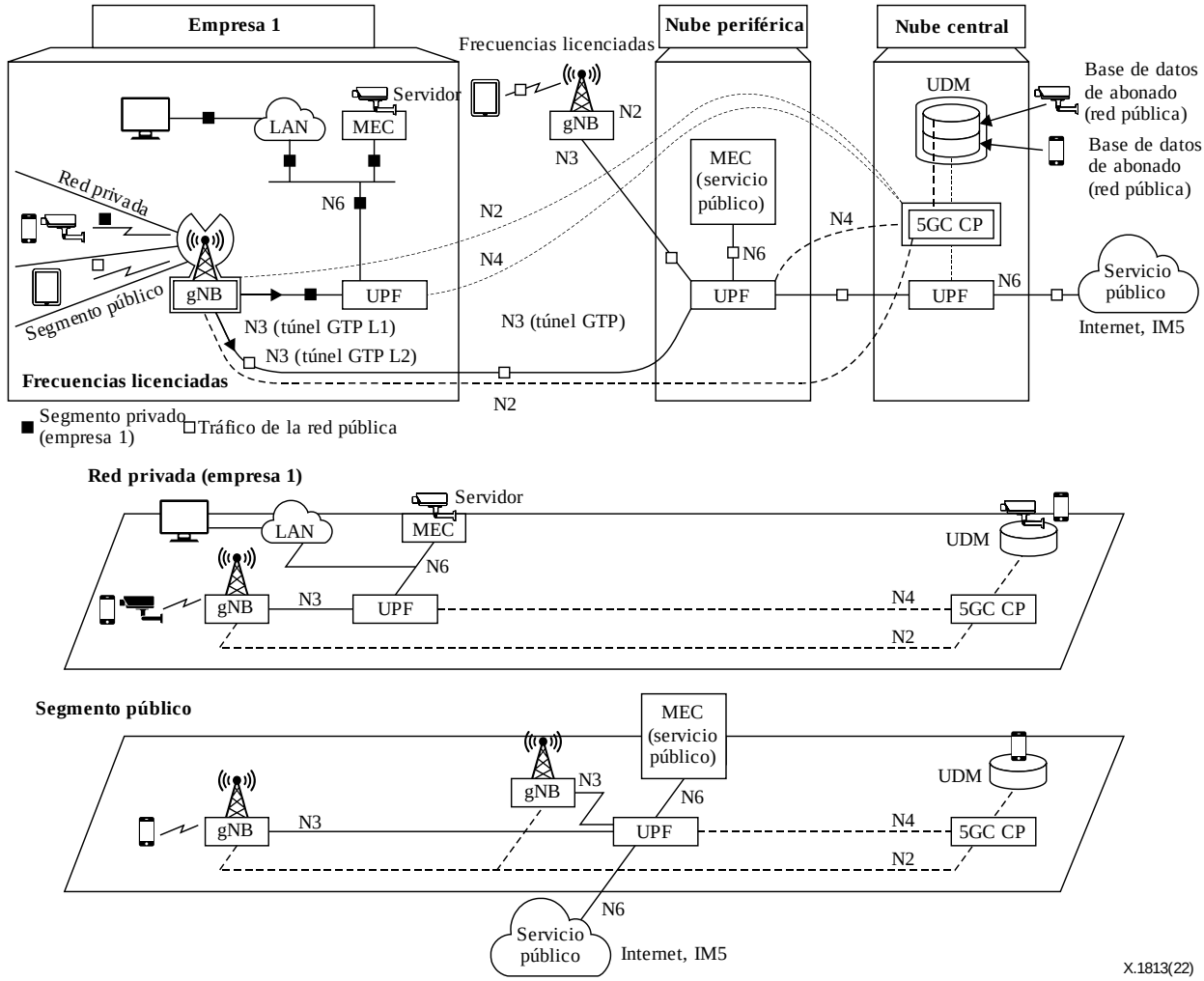

Figura I.2 – Arquitectura funcional detallada para el tipo de despliegue b) de la Figura I.1

De acuerdo con [b-Harrison], el tipo de despliegue c) de la Figura I.1 puede representarse como en la Figura I.3 con una vista vertical utilizando la segmentación de red. La Figura I.3 muestra una arquitectura funcional detallada para el tipo de despliegue c) de la Figura I.1, que comparten redes privadas y públicas IMT-2020.

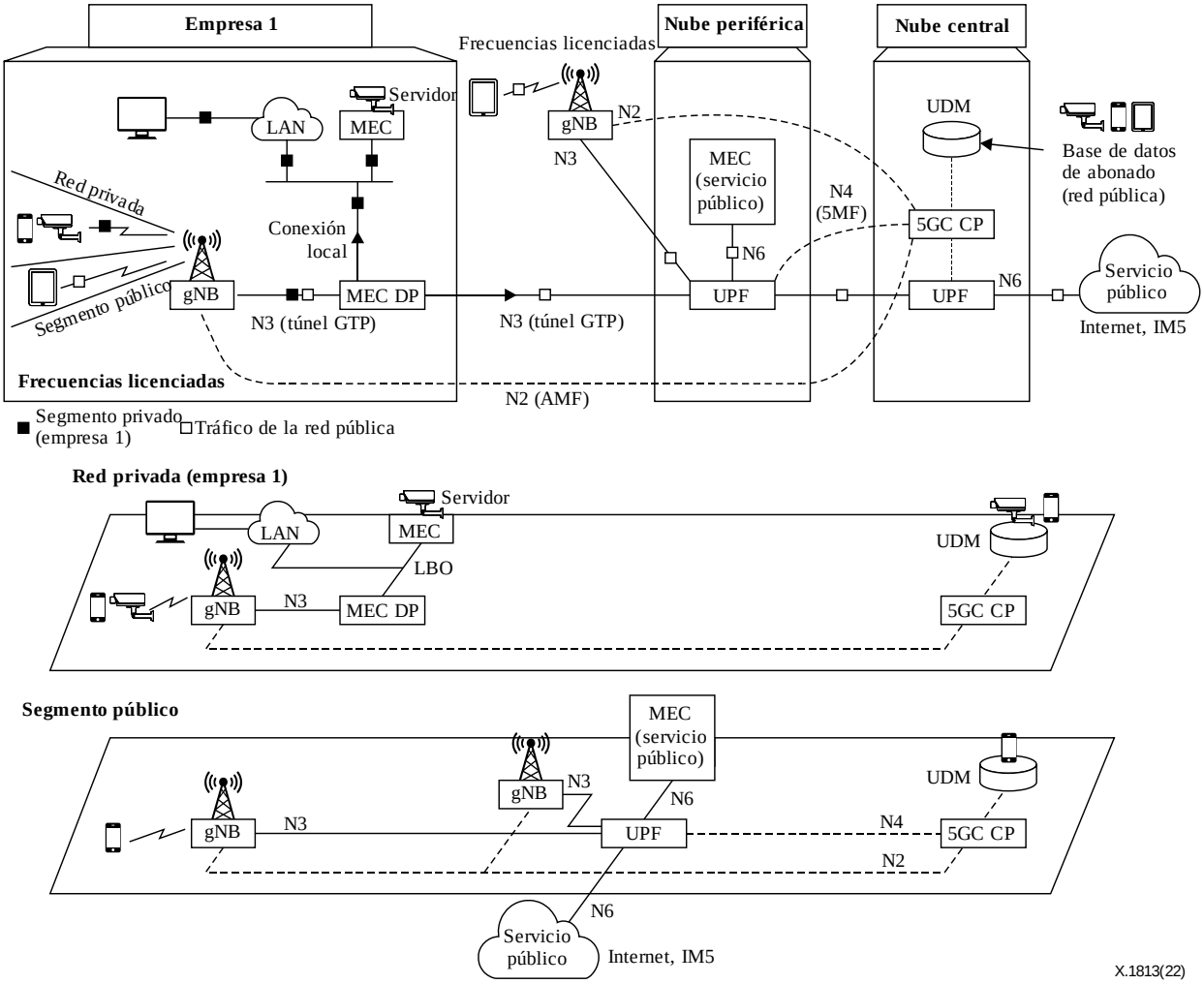

Figura I.3 – Arquitectura funcional detallada para el tipo de despliegue (c) de la Figura I.1

Los operadores de red han desplegado todas las arquitecturas funcionales de las redes privadas IMT-2020 mencionadas anteriormente para mejorar la seguridad y el funcionamiento de las URLLC. Mantener las prestaciones y la seguridad de las redes privadas IMT-2020 es uno de los factores más importantes para los servicios verticales que soportan URLLC. Una de las metodologías posibles es la denominada inspección detallada de paquetes (DPI), que también se describe en [b-UIT-T Y.2774] y [b-UIT-T Y.2775]. Sin embargo, el ámbito de aplicación de estas Recomendaciones se limita únicamente a las redes móviles generales y, por tanto, no puede aplicarse a las redes privadas IMT-2020 y, más concretamente, a los servicios verticales que soportan URLLC.

Bibliografía

[b-UIT-T Y.2774] Recomendación UIT-T Y.2774 (2019), *Requisitos funcionales de la inspección detallada de paquetes en las redes futuras*.

[b-UIT-T Y.2775] Recomendación UIT-T Y.2775 (2019), *Arquitectura funcional de la inspección detallada de paquetes en las redes futuras*.

[b-UIT-T Y.3100] Recomendación UIT-T Y.3100 (2017), *Términos y definiciones relativas a las redes IMT-2020*.

[b-UIT-T Y.4000] Recomendación UIT-T Y.4000/Y.2060 (2012), *Visión general de la Internet de las cosas*.

[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>

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2023