Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1813

(09/2022)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité des réseaux IMT-2020

Exigences de sécurité et de suivi applicables à l'exploitation des services verticaux prenant en charge les communications ultra-fiables à faible temps de latence (URLLC) dans les réseaux IMT-2020 privés

Recommandation UIT-T X.1813

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile (1)	X.1140–X.1149
Sécurité des applications (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1350–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1399
Sécurité de la technologie des registres distribués	X.1400–X.1429
Sécurité des applications (2)	X.1450–X.1459
Sécurité de la toile (2)	X.1470–X.1489
ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
Cyberdéfense	X.1590–X.1599
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
Protection des données	X.1770–X.1789
SÉCURITÉ DES IMT-2020	**X.1800–X.1819**

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1813

Exigences de sécurité et de suivi applicables à l'exploitation des services verticaux prenant en charge les communications ultra-fiables à faible temps de latence (URLLC) dans les réseaux IMT-2020 privés

Résumé

La Recommandation UIT-T X.1813 définit les exigences de sécurité applicables à l'exploitation des services verticaux prenant en charge les communications ultra-fiables à faible temps de latence (URLLC) dans un réseau IMT-2020 privé. Elle recense les menaces et les risques qui apparaissent lors de la fourniture de services verticaux prenant en charge les communications URLLC dans un réseau IMT-2020 privé et décrit des scénarios de déploiement de la sécurité des réseaux IMT-2020 privés, pour l'exploitation des services verticaux prenant en charge les communications URLLC. La surveillance des contenus des communications n'entre pas dans le cadre de cette Recommandation.

Un réseau IMT-2020 privé, également considéré comme un réseau IMT-2020 non public (NPN), est destiné à être réservé à l'usage d'une entité privée, par exemple une entreprise, et peut être déployé dans diverses configurations, au moyen d'éléments virtuels et physiques. Il présentera un débit élevé et un faible temps de latence et offrira d'autres avantages des IMT-2020 pour permettre les applications de prochaine génération.

Pour les services verticaux fournis dans les usines intelligentes et les villes intelligentes qui utilisent un réseau IMT-2020 privé, de nombreux dispositifs de l'Internet des objets (IoT) utilisent des communications massives de type machine (mMTC) et des communications ultra-fiables à faible temps de latence (URLLC). Ces communications peuvent être exposées à des menaces de sécurité et aux risques qui leur sont associés. En outre, ces menaces peuvent nuire à la stabilité de l'exploitation des services verticaux prenant en charge les communications URLLC. Cette stabilité ne peut être garantie lorsque la qualité de fonctionnement des services verticaux est détériorée en raison de ces risques.

Historique

Édition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1813	02-09-2022	17	11.1002/1000/14991

Mots clés

Inspection approfondie des paquets (DPI), détection et réponse du point d'extrémité, informatique en périphérie à accès multiples (MEC), réseau non public (NPN), surveillance du réseau, qualité de fonctionnement, réseau IMT-2020 privé, sécurité, fonction de plan d'utilisateur (UPF).

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (TIC). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

À la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1813

Exigences de sécurité et de suivi applicables à l'exploitation des services verticaux prenant en charge les communications ultra-fiables à faible temps de latence (URLLC) dans les réseaux IMT-2020 privés

1 Domaine d'application

La présente Recommandation définit les exigences de sécurité applicables à l'exploitation des services verticaux prenant en charge les communications ultra-fiables à faible temps de latence (URLLC) dans les réseaux IMT-2020 privés. Elle recense les menaces et les risques en matière de sécurité qui apparaissent lors de la fourniture de services verticaux prenant en charge les communications URLLC dans les réseaux IMT-2020 privés et décrit des scénarios de déploiement de la sécurité des réseaux IMT-2020 privés, pour l'exploitation des services verticaux prenant en charge les communications URLLC.

La surveillance du contenu des communications n'entre pas dans le cadre de la présente Recommandation, pour des raisons de protection de la vie privée.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute Recommandation ou autre référence est sujette à révision; les utilisateurs de la présente Recommandation sont donc invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références indiquées ci-après. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T Y.3102] Recommandation UIT-T Y.3102 (2018), *Cadre applicable aux réseaux IMT-2020*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation emploie les termes suivants définis ailleurs:

3.1.1 réseau 5G non public [b-3GPP TS 22.261]: réseau 5G destiné à une utilisation privée.

3.1.2 attaque [b-ISO 13491-1]: tentative d'obtention ou de modification d'informations sensibles ou d'un service sur un dispositif, par un adversaire qui n'y est pas autorisé.

NOTE 1 – Les fonctions de réseau (NF) incluent, sans s'y limiter, les fonctionnalités des nœuds de réseau, par exemple la gestion des sessions, la gestion de la mobilité et les fonctions de transport, dont on définit le comportement fonctionnel et les interfaces.

NOTE 2 – Les fonctions de réseau peuvent être mises en œuvre dans un équipement matériel dédié ou dans un logiciel, de manière virtuelle.

NOTE 3 – Les fonctions de réseau ne sont pas considérées comme des ressources, mais toute fonction de réseau peut être instanciée en utilisant les ressources.

3.1.3 déploiement [b-ISO/CEI/IEEE 24765]: phase d'un projet au cours de laquelle un système est mis en service et les problèmes de mise en service sont résolus.

3.1.4 domaine [b-ISO/CEI 14888-1]: ensemble d'entités qui fonctionnent selon une unique politique de sécurité.

Exemple – Des certificats de clés publiques créés par une seule autorité ou par plusieurs autorités appliquant la même politique de sécurité.

3.1.5 Internet des objets (IoT) [b-UIT-T Y.4000]: infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution.

3.1.6 surveillance du réseau [b-ISO/CEI 27033-1]: processus consistant à observer et examiner en permanence, d'une part, les données enregistrées concernant l'activité et les opérations sur un réseau, y compris les journaux d'audit et les alertes, et, d'autre part, les analyses connexes.

3.1.7 fonction de réseau [b-UIT-T Y.3100]: dans le contexte des IMT-2020, fonction de traitement au sein d'un réseau.

3.1.8 système [b-ISO/CEI 27000]: applications, services, actifs informatiques ou autres composants du traitement de l'information.

3.1.9 partie prenante [b-ISO/PAS 19450]: personne physique, organisation ou groupe de personnes ayant un intérêt, ou pouvant être affectées, lorsqu'un système est envisagé, conçu ou déployé.

3.1.10 confiance [b-ISO/CEI 25010]: mesure dans laquelle un utilisateur ou une autre partie prenante est convaincu(e) qu'un produit ou un système se comportera comme prévu.

3.1.11 service vertical [b-5G-PPP]: du point de vue de l'entreprise, un service vertical est un service axé sur un secteur spécifique ou sur un groupe de clients ayant des besoins particuliers (par exemple les services automobiles, les services de loisirs, les services de cybersanté et l'industrie 4.0).

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 système de communication IMT-2020: système destiné à gérer les processus de communication IMT-2020 pour les services des IMT-2020.

NOTE 1 – Dans le contexte de l'UIT-T, la 5G est désignée par l'expression "IMT-2020".

NOTE 2 – Dans la présente Recommandation, "système de communication IMT-2020" renvoie au même concept que "système IMT-2020".

3.2.2 écosystème des IMT-2020: ensemble de parties prenantes qui interagissent pour former un système IMT-2020 stable et opérationnel.

NOTE – Ce terme fait référence au développement de la technologie de communication 5G, au sein de laquelle une communauté de parties prenantes du secteur privé et des milieux universitaires met à disposition ses produits, ses technologies et ses compétences spécialisées, pour rendre des fonctionnalités possibles à différentes couches de la pile de valeurs de la 5G, comme l'infrastructure, le réseau, la plate-forme, le service et l'application.

3.2.3 réseau IMT-2020 privé: un réseau 5G non public (voir le paragraphe 3.1.1) qui utilise des éléments aussi bien virtuels que physiques d'un système de communication IMT-2020 et qui est destiné à être réservé à l'usage d'une entité privée, par exemple une entreprise.

3.2.4 service IMT-2020: avantage fourni par l'écosystème des IMT-2020.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

5GC réseau central 5G (*5G core)*

AMF	fonction de gestion d'accès et de mobilité (*access and mobility management function*)
DDoS	déni de service réparti (*distributed denial of service*)
DPI	inspection approfondie des paquets (*deep packet inspection*)
EC	informatique en périphérie (*edge computing*)
EDR	détection et réponse du point d'extrémité (*endpoint detection and response*)
GTP	protocole de tunnellisation GPRS (*GPRS tunnelling protocol*)
IoT	internet des objets (*Internet of things*)
MEC	informatique en périphérie à accès multiples (*multi-access edge computing*)
MEC DP	plan de données MEC (*MEC data plane*)
mMTC	communications massives de type machine (*massive machine type communications*)
NF	fonction de réseau (*network function*)
NMCF	fonction client de surveillance du réseau (*network monitoring client function*)
NMF	fonction de surveillance du réseau (*network monitoring function*)
NMSF	fonction de serveur de surveillance du réseau (*network monitoring server function*)
NPN	réseau non public (*non-public network*)
PLMN	réseau mobile terrestre public (*public land mobile network*)
RTT	temps de transmission aller-retour (*round-trip time*)
SBA	architecture fondée sur les services (*service-based architecture*)
SMF	fonction de gestion de session (*session management function*)
UDM	gestion de données unifiée (*unified data management*)
UE	équipement d'utilisateur (*user equipment*)
UID	identificateur d'utilisateur (*user ID*)
UPF	fonction de plan d'utilisateur (*user plane function*)
URLLC	communications ultra-fiables à faible temps de latence (*ultra-reliability and low latency communication*)

5 Conventions

La présente Recommandation utilise les conventions suivantes:

L'expression "**il est obligatoire**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "**il est recommandé**" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

L'expression "**il est interdit**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "**peut, à titre d'option**" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Ces mots n'impliquent pas que la mise en œuvre du vendeur doit incorporer l'option et que la caractéristique peut éventuellement être activée par l'opérateur du réseau/le fournisseur de service. Ils signifient plutôt que le fabricant peut incorporer la caractéristique à titre facultatif et revendiquer néanmoins la conformité avec la spécification.

6 Considérations générales

L'architecture d'un système IMT-2020 est conçue de manière à permettre aux opérateurs de réseau d'assurer la connectivité des données et la fourniture des services fondés sur des technologies telles que la virtualisation des fonctions de réseau et les réseaux pilotés par logiciel. Le 3GPP donne une définition de l'architecture fondée sur les services (SBA) dans la spécification technique [b-3GPP TS 23.501], dans laquelle la fonctionnalité du plan de commande et les répertoires de données communs d'un réseau IMT-2020 sont fournis par le biais d'un ensemble de fonctions de réseau (NF) interconnectées, qui sont toutes autorisées à accéder aux services des autres fonctions de réseau. La Figure 1 montre l'architecture d'un système IMT-2020.

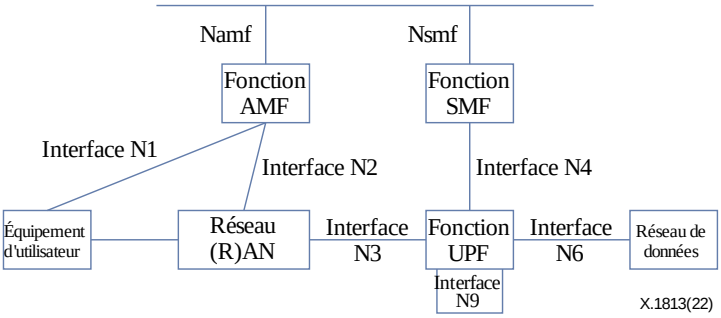

Figure 1 – Architecture d'un système IMT-2020

L'architecture d'un système IMT-2020, telle que définie dans [UIT-T Y.3102] et dans la spécification technique [b-3GPP TS 23.501], comporte les fonctions de réseau suivantes:

– La fonction de gestion d'accès et de mobilité (AMF), qui fournit une fonction de gestion d'enregistrement, une fonction de gestion des connexions, une fonction de gestion de mobilité, une fonction d'authentification de l'accès, une fonction d'autorisation de l'accès, une fonction de gestion des services de localisation, une fonction de notification des événements de mobilité de l'équipement d'utilisateur (UE), etc.

– Le réseau de données (DN), par exemple les services fournis par un opérateur, l'accès à l'Internet ou les services fournis par des tiers.

– La fonction de gestion de session (SMF), qui fournit des fonctions d'établissement, de modification et de libération, des fonctions d'attribution d'adresse IP d'équipement d'utilisateur et de gestion, une fonction de sélection et de commande du plan d'utilisateur, une fonction de rassemblement de données de taxation et une fonction de prise en charge des interfaces de taxation, une fonction de commande et de coordination du rassemblement de données de taxation au niveau de la fonction de plan d'utilisateur (UPF), une fonction de notification de données sur la liaison descendante, une fonction de prise en charge de la compression d'en-tête, etc.

– La fonction UPF permet de gérer le chemin du plan d'utilisateur des sessions de l'unité de données de protocole (PDU). La spécification technique du G3GPP prend en charge les déploiements avec une fonction UPF unique ou avec de multiples fonctions UPF pour une session PDU donnée. La sélection de la fonction UPF est effectuée par la fonction SMF. La fonction UPF prévoit l'attribution d'une adresse/d'un préfixe IP à l'équipement d'utilisateur, pour faire suite à la demande transmise par la fonction SMF, et fournit une fonction de routage et de retransmission des paquets, une fonction d'inspection des paquets, une fonction de traitement de la qualité de service pour le plan d'utilisateur, une fonction de mise en mémoire tampon des paquets sur la liaison descendante, une fonction de déclenchement de notifications pour les données sur la liaison descendante, etc.

– Namf: l'élément Namf identifie une interface fondée sur les services pour la fonction de gestion de l'accès et de la mobilité dans le réseau central.
– Nsmf: l'élément Nsmf identifie une interface fondée sur les services pour la fonction de gestion de session.
– UE: équipement d'utilisateur.
– (R)AN: réseau d'accès (radioélectrique).

L'architecture d'un système IMT-2020 contient les points de référence suivants:

– N1: Point de référence entre l'équipement d'utilisateur et la fonction AMF.
– N2: Point de référence entre le réseau (R)AN et la fonction AMF.
– N3: Point de référence entre le réseau (R)AN et la fonction UPF.
– N4: Point de référence entre la fonction SMF et la fonction UPF.
– N6: Point de référence entre la fonction UPF et un réseau de données.
– N9: Point de référence entre deux fonctions UPF.

Les réseaux IMT-2020 privés sont destinés à être réservés à l'usage d'une entité privée, par exemple une entreprise, et peuvent être déployés dans diverses configurations, au moyen des éléments virtuels et physiques des systèmes de communication IMT-2020. Un réseau IMT-2020 privé est établi sur la base des principes de l'architecture des systèmes IMT-2020définis dans la spécification technique [b-3GPP TS 23.501], y compris les principes de flexibilité et de modularité pour les fonctionnalités nouvellement introduites. L'architecture fonctionnelle d'un réseau IMT-2020 privé est illustrée à l'Appendice I.

Les spécifications du 3GPP [b-3GPP TS 23.501] prévoient différents scénarios pour le déploiement des réseaux privés. Au plus haut niveau, les réseaux privés peuvent être répartis en deux catégories:

– les réseaux IMT-2020 privés déployés en tant que réseaux autonomes totalement isolés;
– les réseaux IMT-2020 privés déployés en tant que tranches d'un réseau mobile terrestre public (RMTP), en lien avec un réseau public.

En outre, l'Internet des objets (IoT) est défini dans [b-UIT-T Y.4000] comme une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution. Dans cette Recommandation, le cas d'utilisation principal de ces services verticaux est le service IoT. Dans ce contexte, les dispositifs IoT pourraient être les dispositifs représentatifs des équipements d'utilisateur définis par le 3GPP dans la spécification technique [b-3GPP TS 22.261].

La technologie IMT-2020 étant entrée en phase de commercialisation, les réseaux IMT-2020 privés seront principalement utilisés pour mettre en place des services IMT-2020 verticaux avec des dispositifs IoT industriels, y compris des services pour les usines intelligentes et les villes intelligentes qui nécessitent des performances en temps réel, avec des communications ultra-fiables à faible temps de latence (URLLC). En conséquence, les réseaux IMT-2020 privés doivent répondre à diverses exigences en termes de sécurité et de qualité de fonctionnement, étant donné qu'ils traitent des données sensibles au facteur temps, conformément à [UIT-T Y.3102]. La Figure 2 montre l'architecture de sécurité globale des réseaux IMT-2020 privés, conformément à la spécification technique [b-3GPP TR 23.734].

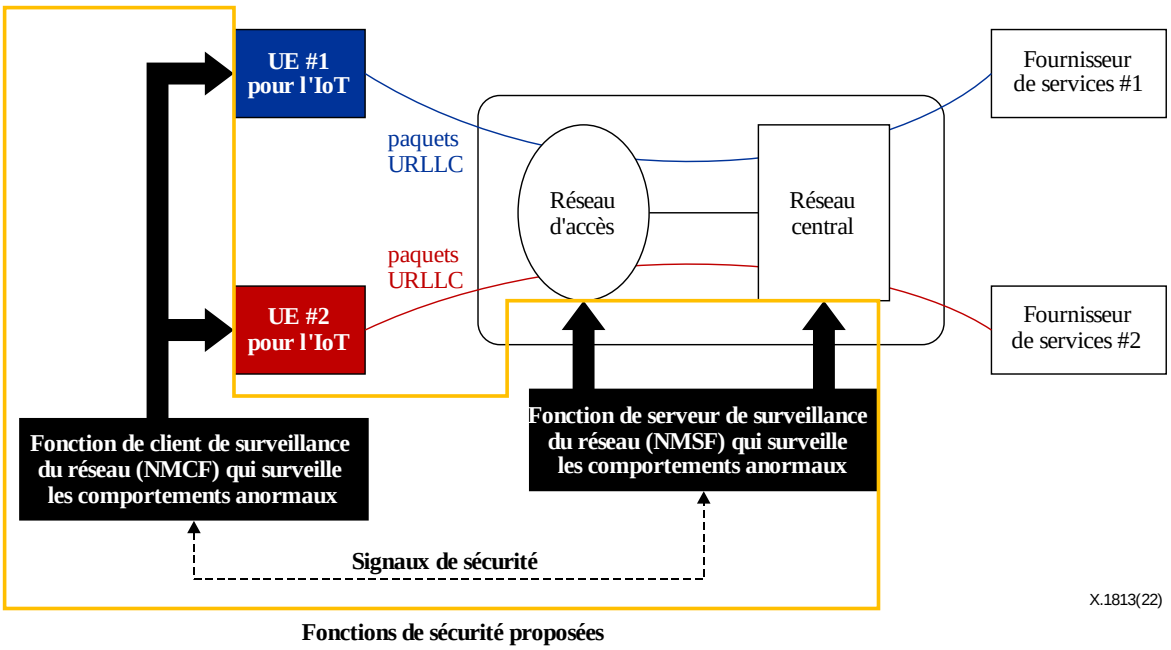

Figure 2 – Architecture de sécurité des réseaux IMT-2020 privés

Comme le montre la Figure 2, l'architecture de sécurité d'un réseau IMT-2020 privé permet aux opérateurs de surveiller la sécurité/la qualité de fonctionnement des communications entre les nœuds du réseau et les équipements d'utilisateur situés aux points d'extrémité d'un réseau IMT-2020 privé pour l'exploitation des services verticaux prenant en charge les communications URLLC.

7 Menaces pour les services verticaux prenant en charge les communications URLLC dans les réseaux IMT-2020 privés

L'IoT ouvre de nouvelles perspectives prometteuses très diverses, notamment les systèmes d'automatisation et de commande industriels (IACS), les communications dans les véhicules autonomes, les réseaux électriques intelligents, les capteurs installés sur les autoroutes et les capteurs de circulation, les communications des drones, les capteurs médicaux et la réalité augmentée/réalité virtuelle, qui fonctionnent en grande partie de manière automatisée. Il est possible que les services IoT doivent également posséder les caractéristiques des communications URLLC pour les services IMT-2020. D'après la spécification technique [b-3GPP TS 22.261], les réseaux privés sont destinés à être réservés à l'usage d'une entité privée, par exemple une entreprise, et seuls les équipements d'utilisateur autorisés ont le droit d'accéder à un réseau privé.

Dans ce type d'environnement, les menaces aux services verticaux, entre autres, sont identifiées comme tout type d'attaques susceptibles de nuire aux éléments et aux interfaces des réseaux IMT-2020 privés en créant de la latence. Un réseau IMT-2020 privé peut être déployé en utilisant ou non une fonction UPF ou l'informatique en périphérie à accès multiples (MEC). Une fonction UPF est accessible, sur l'Internet, via l'interface N6 définie par le 3GPP. Par conséquent, si un réseau IMT-2020 privé est déployé en utilisant une fonction UPF ou l'informatique en périphérie à accès multiples, l'interface N6 est fortement exposée aux attaques, étant donné que les attaquants peuvent y accéder de partout sur l'Internet. Les attaques de ce type peuvent se produire volontairement ou involontairement, depuis l'extérieur ou l'intérieur d'un réseau IMT-2020 privé.

Les menaces à la fonction UPF, à l'informatique en périphérie à accès multiples et à l'interface N6 sont les suivantes:

– Les attaques par déni de service réparti (DDoS).

– L'espionnage du trafic/des données sur les liaisons de communication.

– Une augmentation inattendue du trafic ou un trafic anormal généré par les équipements d'utilisateur situés dans un réseau IMT-2020 privé.

Un réseau IMT-2020 privé est déployé à titre privé avec des éléments et des interfaces de réseau, qui comportent des parties nouvelles ou différentes par rapport aux réseaux existants, en ce qui concerne la sécurité. L'interface N3 qui connecte le réseau d'accès et le réseau central utilise le protocole IPsec pour garantir la sécurité de transport. L'interface N4 connecte la fonction UPF et la fonction AMF. Cette interface est fermée dans un réseau central évolué en mode paquet (EPC) 4G, mais pas dans un réseau central évolué en mode paquet virtualisé (vEPC) IMT-2020. Par rapport à l'interface X6, les interfaces N3 et N4 ne sont pas accessibles via l'Internet, mais il est possible que de nouveaux types de menaces et d'obstacles apparaissent de manière involontaire.

Les menaces aux interfaces N3 et N4 apparaissent dans les cas suivants:

– Les méthodes de commande d'accès mises en œuvre dans un réseau IMT-2020 privé sont insuffisantes.
– Les mesures et procédures de sécurité appliquées par l'opérateur d'un réseau IMT-2020 privé présentent des limites.
– Les éléments du réseau IMT-2020 privé sont mal conçus ou mal configurés, et ne permettent pas de gérer une augmentation soudaine des accès.

L'absence de spécialistes familiarisés avec le grand nombre de nouvelles fonctionnalités des réseaux IMT-2020 peut également constituer une menace et un obstacle involontaires.

8 Risques associés aux services verticaux prenant en charge les communications URLLC dans les réseaux IMT-2020 privés

Un réseau IMT-2020 privé constitue pour l'essentiel un réseau très fiable dans l'infrastructure de l'IoT, étant donné que les réseaux IMT-2020 ont été normalisés par le 3GPP, afin de garantir la sécurité des nouveaux services IMT-2020 verticaux.

Malgré l'utilisation des méthodes de sécurité classiques pour l'authentification, l'autorisation et la confidentialité des données qui sont fournies dans les normes du 3GPP et dans d'autres normes relatives à la sécurité, un réseau IMT-2020 privé demeure exposé à de nombreux risques. Par exemple, les méthodes de sécurité existantes ne permettent pas d'éliminer les menaces liées au comportement anormal des équipements d'utilisateur situés dans un réseau IMT-2020 privé.

Les réseaux IMT-2020 étant dotés de caractéristiques plus robustes orientées vers les logiciels, ils peuvent être exposés à un plus grand nombre de risques associés aux logiciels, comme des défauts en matière d'élaboration de logiciels, des procédures de mise à jour incorrectes et des erreurs de configuration. Par conséquent, dans un réseau IMT-2020, la qualité de fonctionnement peut se dégrader en raison des risques susmentionnés.

Dans ce contexte, ces risques peuvent avoir les conséquences suivantes:

– Exploitation instable et dangereuse de services verticaux: le comportement anormal des dispositifs IoT situés dans un réseau IMT-2020 peut menacer le fonctionnement normal d'une infrastructure de ville intelligente.
– Destruction, modification ou altération des informations stockées dans l'infrastructure d'un réseau IMT-2020 ou communiquées par ce biais.
– Dégradation de la qualité de fonctionnement d'un service IMT-2020 fondé sur les communications URLLC: si un réseau IMT-2020 ne peut satisfaire aux exigences de faible latence d'un service IMT-2020 fondé sur les communications URLLC, le réseau peut voir sa qualité de fonctionnement se dégrader, ce qui nuirait aux services verticaux sensibles au facteur temps associés. Par exemple, les usines intelligentes étant conçues pour répondre aux exigences des communications URLLC, la qualité ou la vitesse de production risquent d'être

dégradées si les exigences en matière de faible temps de latence ne sont pas respectées. Ceci peut entraîner non seulement des pertes financières considérables, mais également des accidents. La dégradation potentiellement significative de la qualité d'image des caméras de sécurité du fait du temps de connexion des différents capteurs constitue un autre exemple.

Par conséquent, il est nécessaire de définir des exigences de sécurité applicables à l'exploitation des services verticaux prenant en charge les communications URLLC dans les réseaux IMT-2020 privés, afin de remédier aux menaces et aux risques mentionnés ci-dessus.

9 Scénarios de déploiement des fonctions de sécurité pour l'exploitation des services verticaux prenant en charge les communications ultra-fiables à faible temps de latence (URLLC) sur les réseaux IMT-2020 privés

Ce paragraphe présente des scénarios de déploiement des fonctions de sécurité destinées à l'exploitation des services verticaux prenant en charge les communications ultra-fiables à faible temps de latence (URLLC) sur le réseau IMT-2020 privé. L'architecture de sécurité du réseau IMT-2020 privé est configurée à l'aide de fonctions de surveillance du réseau (NMF). Les fonctions NMF sont composées d'une fonction de surveillance du réseau côté serveur (NMSF) et d'une autre côté client (NMCF). Les fonctions NMF peuvent être mises en œuvre en déployant une fonction d'inspection approfondie des paquets (DPI) dans un nœud de réseau ou en déployant un nœud de réseau DPI dédié.

Les fonctions NMSF peuvent être configurées en tant que nœuds de réseau indépendants séparés des fonctions UPF ou des systèmes MEC. Plus précisément, elles doivent être associées à l'entrée ou à la sortie d'une fonction UPF ou d'un système MEC afin qu'elles puissent en surveiller les paquets.

Il existe trois scénarios de déploiement des fonctions NMSF:

a) Intégration de la fonction NMSF en tant que nœud dans le système MEC.

b) Mise en œuvre de la fonction NMSF en tant que nœud séparé pour surveiller le paquet créé par la fonction UPF.

c) Configuration de plusieurs fonctions NMSF de sorte qu'une première est intégrée en tant que nœud dans le système MEC et qu'une deuxième est mise en œuvre en tant que nœud séparé afin d'assurer la surveillance du paquet créé par la fonction UPF.

Dans ces scénarios de déploiement, l'attribution ou non d'adresses IP aux fonctions NMSF ne pose aucun problème pour leur mise en œuvre. La fonction NMCF est intégrée aux équipements d'utilisateurs dans ces trois scénarios.

La Figure 3 illustre le scénario de déploiement A dans une architecture de sécurité du réseau IMT-2020 privé, lors duquel plusieurs fonctions NMCF et NMSF sont configurées.

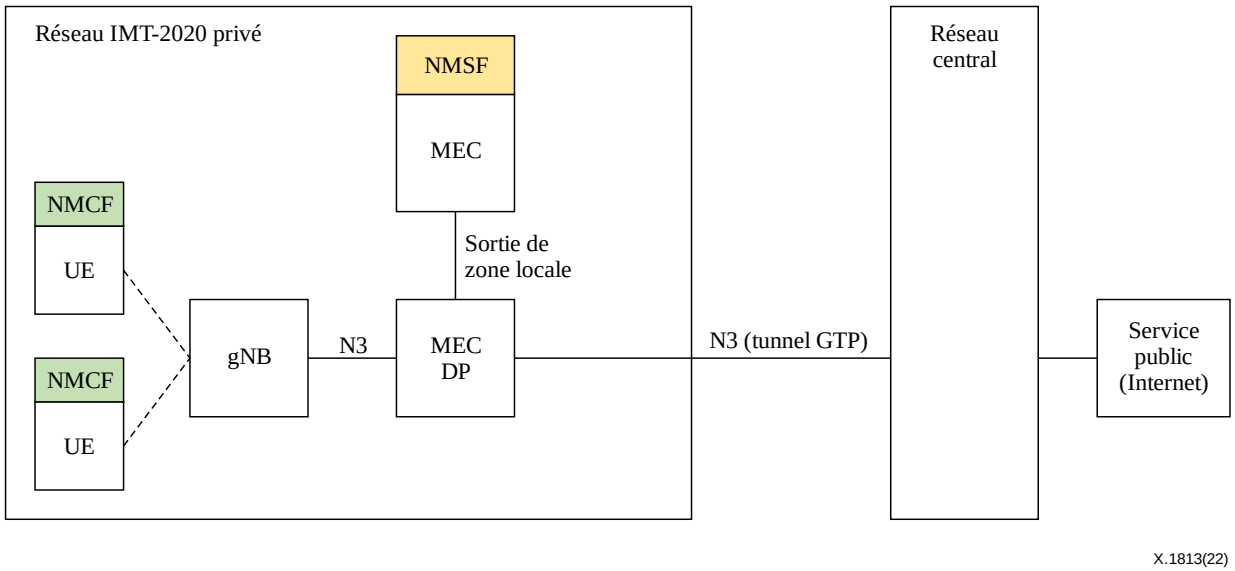

Figure 3 – Scénario de déploiement A

En ce qui concerne la Figure 3, les fonctions NMCF peuvent être intégrées à leurs équipements d'utilisateurs respectifs, notamment des dispositifs IoT, qui communiquent avec un nœud gNB. L'intégration de fonctions NMCF à des dispositifs IoT est l'une des solutions les plus efficaces pour garantir la sécurité et les performances des communications URLLC sur le réseau IMT-2020 privé. La fonction NMCF peut être mise en œuvre dans des logiciels et désignée comme une entité de détection et de réponse du point d'extrémité (EDR) ou comme un micromoteur (ME). Le serveur de la fonction NMCF peut être situé sur le réseau IMT-2020 privé, dans un domaine d'informatique en nuage périphérique ou un domaine de réseau public (Internet). Les équipements d'utilisateurs sont connectés sans câbles au nœud gNB. Chaque équipement d'utilisateur transmet des paquets au nœud gNB ou en reçoit de la part de ce dernier. Le nœud gNB est connecté au réseau central IMT-2020 ou à un réseau local par l'intermédiaire des interfaces N3 et N4. Les paquets transitent à travers les interfaces N3 et N4.

Si une adresse IP est attribuée à la fonction NMSF, les fonctions NMCF et NMSF communiquent entre elles à l'aide d'une interface N3 et N4 pour échanger des signaux de sécurité, tels que le résultat du contrôle de la fonction NMCF.

Bien que cela ne soit pas illustré sur la Figure 3, dans le scénario A, une fonction NMSF supplémentaire peut aussi être intégrée au plan de données MEC, afin que deux fonctions NMSF puissent surveiller le trafic des réseaux privé et public circulant par l'équipement d'utilisateur. La fonction NMSF peut également être configurée en tant qu'entité indépendante séparée du système MEC.

La Figure 4 illustre le scénario de déploiement B dans l'architecture de sécurité du réseau IMT-2020 privé, dans lequel plusieurs fonctions NMCF et NMSF sont configurées.

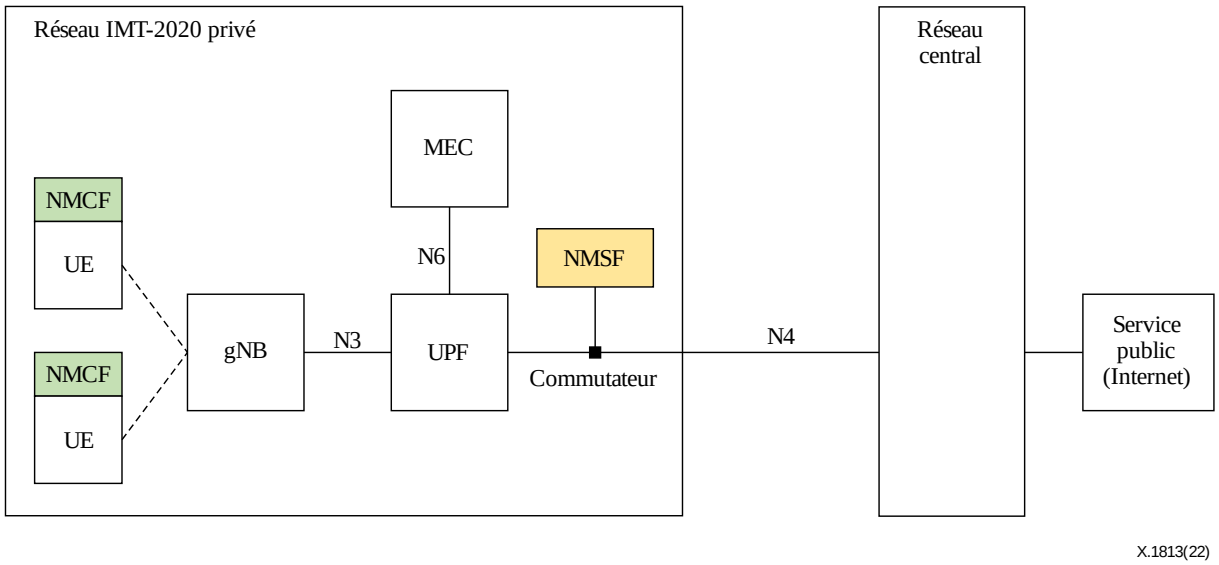

Figure 4 – Scénario de déploiement B

En ce qui concerne la Figure 4, la fonction NMSF est mise en œuvre en tant que nœud séparé en dehors de la fonction UPF afin de surveiller les paquets créés par cette dernière. Un commutateur peut être utilisé pour mettre en miroir les paquets créés par la fonction UPF. Si une adresse IP est attribuée à la fonction NMSF, les fonctions NMCF et NMSF communiquent entre elles par l'intermédiaire d'une interface N3 et N4 pour échanger des signaux de sécurité, tels que le résultat du contrôle généré par l'équipement d'utilisateur (nœud client). Si le réseau IMT-2020 privé utilise une fonction de chiffrement de nœud à nœud (par exemple, le protocole IPSec), les fonctions NMSF peuvent être configurées à un point où les paquets déchiffrés sont créés par le nœud.

La Figure 5 illustre le scénario de déploiement C dans l'architecture de sécurité du réseau IMT-2020 privé, dans lequel plusieurs fonctions NMF sont configurées.

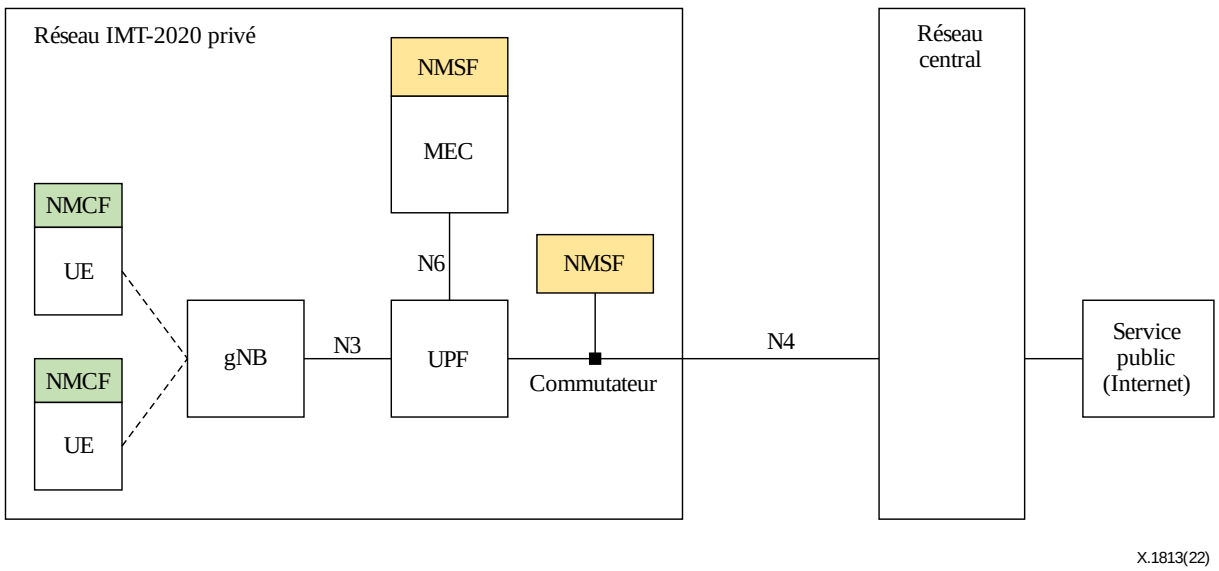

Figure 5 – Scénario de déploiement C

En ce qui concerne la Figure 5, la fonction est mise en œuvre non seulement dans le système MEC, mais aussi en tant que nœud séparé en dehors de la fonction UPF afin de surveiller les paquets créés par cette dernière. Si des adresses IP sont attribuées aux fonctions NMSF, les fonctions NMCF et NMSF communiquent entre elles par l'intermédiaire d'une interface N3 et N4 pour échanger des

signaux de sécurité, tels que le résultat du contrôle généré par l'équipement d'utilisateur (nœud client). Si le réseau IMT-2020 privé utilise une fonction de chiffrement de nœud à nœud (par exemple, le protocole IPsec), les fonctions NMSF peuvent être configurées à un point où les paquets déchiffrés sont créés par le nœud.

Les trois scénarios décrits ci-dessus ne s'excluent pas mutuellement et le mode à utiliser dépend, entre autres, du coût et des caractéristiques du réseau. Il existe aussi plusieurs autres méthodes de déploiements des fonctions NMSF et NMCF. Par exemple, les fonctions NMSF peuvent être intégrées à n'importe quel nœud du réseau avec les fonctions UPF ou MEC.

Par conséquent, en ce qui concerne l'architecture fonctionnelle d'un réseau, il est possible de surveiller la sécurité et les performances à l'aide d'une fonction NMSF intégrée aux fonctions MEC ou UPF, et les fonctions NMCF intégrées aux dispositifs IoT, ainsi qu'en utilisant un protocole de signalisation entre les fonctions NMSF et NMCF.

10 Exigences de sécurité et de suivi applicables à l'exploitation des services verticaux prenant en charge les communications URLLC sur les réseaux IMT-2020 privés

Ce paragraphe identifie les exigences de sécurité et de suivi applicables à l'exploitation des services verticaux prenant en charge les communications URLLC sur un réseau IMT-2020 privé. Un réseau IMT-2020 privé requiert un niveau de sécurité et de performances plus élevé que les réseaux classiques en raison du volume de données important échangé entre les nombreux dispositifs clients/capteurs et les serveurs centraux qui les contrôlent. En outre, les exigences applicables aux communications URLLC du réseau IMT-2020 doivent être mises en œuvre en périphérie en vertu du document [UIT-T Y.3102].

Dans les scénarios de déploiement des fonctions NMSF et NMCF sur le réseau IMT-2020 privé, l'exploitation des services verticaux prenant en charge les communications URLLC est régie, entre autres, par les exigences générales de sécurité et de suivi suivantes:

a) Il est obligatoire de surveiller et de détecter tout comportement anormal des équipements d'utilisateurs et du réseau IMT-2020 privé afin d'atténuer tout risque en matière de sécurité.

b) Il est obligatoire de surveiller les performances des services verticaux prenant en charge les communications URLLC.

c) Il est obligatoire de signaler à l'administrateur du réseau tout comportement anormal des équipements d'utilisateurs et des réseaux IMT-2020 privés afin que les problèmes puissent être résolus et que les capacités de communication URLLC puissent être rétablies à temps.

Il est éventuellement recommandé de visualiser les comportements anormaux des équipements d'utilisateurs et des réseaux IMT-2020 privés afin de les régler plus efficacement. La visualisation du résultat du contrôle est décrite dans l'Annexe C.

10.1 Exigences de sécurité applicables à la fonction NMSF

Les exigences de sécurité applicables à la fonction NMSF comprennent notamment les suivantes:

a) La fonction NMSF doit fournir au moins une fonction de mise en miroir des paquets circulant entre le nœud client et le nœud serveur, afin de récupérer un paquet mis en miroir. Le nœud client est un équipement d'utilisateur ou un dispositif IoT. La mise en miroir des paquets est une technique permettant de collecter et d'analyser en temps réel des paquets échangés dans un nœud spécifique. La fonction NMSF peut agir comme commutateur pour la mise en miroir des paquets.

b) La fonction NMSF doit déterminer quels comportements anormaux ou problèmes menacent la sécurité et les performances du réseau IMT-2020 privé en fonction des informations que contiennent les paquets mis en miroir.

c) Si une adresse IP est attribuée à une fonction NMSF, cette dernière doit recevoir un paquet de vérification de la sécurité transmis par la fonction NMCF à travers le protocole TCP et calculer le temps de transmission aller-retour (RTT) en fonction du paquet de vérification de la sécurité reçu.

Le paquet de vérification de la sécurité est transmis selon le protocole TCP et au format illustré dans la Figure 6.

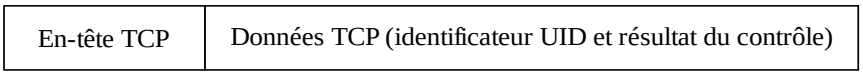

Figure 6 – Paquet de vérification de la sécurité transmis à l'aide du protocole TCP

Tableau 1 – Champs du paquet de vérification de la sécurité

Champ	Longueur en octets	Description
Identifiant d'utilisateur (UID)	4	Ce champ indique l'identifiant d'un équipement d'utilisateur.
Longueur	2	Ce champ indique la longueur en octets du champ correspondant au résultat du contrôle.
Résultat du contrôle	Variable	Ce champ indique les informations en service, l'utilisation de l'unité centrale de traitement et l'utilisation de la mémoire d'un équipement d'utilisateur.

d) Si aucune adresse IP n'a été attribuée à la fonction NMSF, cette dernière doit mettre en miroir un paquet de vérification de la sécurité transmis par la fonction NMCF au nœud serveur à l'aide du protocole de datagramme utilisateur (UDP) et calculer le temps de transmission aller-retour (RTT) en fonction du paquet de vérification de la sécurité mis en miroir.

Le paquet de vérification de la sécurité est transmis selon le protocole UDP et au format illustré dans la Figure 7.

Figure 7 – Paquet de vérification de la sécurité transmis à l'aide du protocole UDP

Tableau 2 – Champs du paquet de vérification de la sécurité

Champ	Longueur en octets	Description
Identifiant UID	4	Ce champ indique l'identifiant d'un équipement d'utilisateur.
Longueur	2	Ce champ indique la longueur en octets du champ correspondant au résultat du contrôle.
Résultat du contrôle	Variable	Ce champ indique les informations en service, l'utilisation de l'unité centrale de traitement et l'utilisation de la mémoire d'un équipement d'utilisateur.

e) Il est recommandé que la fonction NMSF signale les comportements anormaux qui enfreignent les exigences applicables aux communications URLLC en fonction de l'état de sécurité et des performances. Lorsqu'un comportement anormal menaçant la sécurité et les performances est détecté, la fonction NMSF alerte l'utilisateur afin qu'il puisse régler de manière adéquate le comportement anormal. Ensuite, la fonction NMSF envoie une alerte au contrôleur de la sécurité lui indiquant de prendre les mesures nécessaires pour régler le comportement anormal, c'est-à-dire de fermer le réseau. L'alerte est envoyée à travers l'interface N3 et N4 fournie par le protocole de signalisation.

Les fonctionnalités détaillées de la fonction NMSF en matière de surveillance des performances et de la sécurité fondée sur la mise en miroir peuvent être utilisées selon l'algorithme normatif décrit à l'Annexe A.

10.2 Exigences de sécurité applicables à la fonction NMCF

Les exigences de sécurité applicables à la fonction NMCF comprennent notamment les suivantes:

a) La fonction NMCF doit utiliser les ressources de calcul de chaque nœud client ou capteur IoT. De plus, il est recommandé qu'elle utilise le moins de ressources possible de sorte que les fonctions effectuent correctement leurs opérations.

b) La fonction NMCF doit collecter des paquets ou des informations internes transmis ou reçus par les nœuds clients du réseau.

c) La fonction NMCF doit surveiller et identifier la menace pour la sécurité du réseau associée au nœud client, y compris à la fonction NMCF elle-même, en se reposant sur les paquets et les informations internes collectés. Si une valeur indiquée par les informations internes est supérieure ou égale à un seuil donné, la fonction NMCF détermine qu'il existe une menace pour la sécurité du réseau. Les informations internes répertorient notamment l'utilisation de l'unité centrale de traitement ou de la mémoire d'un nœud client.

d) Si une adresse IP est attribuée à la fonction NMSF, la fonction NMCF doit générer un paquet de vérification de sécurité selon le protocole TCP, y compris le résultat du contrôle illustré sur la Figure 6, et l'envoyer à la fonction NMSF.

e) Si aucune adresse IP n'est attribuée à la fonction NMSF, la fonction NMCF doit générer un paquet de vérification de sécurité selon le protocole UDP contenant le résultat; comme illustré à la Figure 7, et l'envoyer au nœud serveur pour que la fonction NMSF puisse le mettre en miroir.

f) Il est recommandé que la fonction NMCF affiche une alerte destinée à l'utilisateur de dispositifs IoT afin de l'avertir de tout fonctionnement anormal d'un équipement d'utilisateur.

La fonction NMCF est plus susceptible de recueillir des données plus précises. De plus, elle peut s'arrêter en cas de problème, notamment si l'alimentation d'un équipement en état de marche normal est coupée. Par conséquent, il est essentiel que la fonction NMSF effectue la surveillance de la sécurité et des performances.

Cependant, surveiller chaque flux de données d'un grand nombre d'équipements d'utilisateurs connectés au réseau IMT-2020 privé peut surcharger la fonction NMSF. Dans ce cas, il est nécessaire de recourir également à la fonction NMCF pour surveiller efficacement les menaces visant le réseau.

Les fonctionnalités qui mettent en œuvre les exigences applicables à la fonction NMCF peuvent être utilisées selon l'algorithme normatif décrit à l'Annexe B.

Annexe A

Caractéristiques de la fonction NMSF

(Cette Annexe fait partie intégrante de la présente Recommandation.)

Conformément à la présente recommandation, la fonction NMSF détermine quels comportements anormaux menacent la sécurité et les performances en fonction des paquets mis en miroir ou des informations liées à ceux-ci. La fonction NMSF identifie les comportements anormaux en calculant des indices ou des paramètres liés aux performances ou à la sécurité du réseau IMT-2020 privé et en comparant le résultat des calculs à des valeurs de référence conformément aux exigences applicables aux services de communication (IMT-2020 ou LTE). Ces exigences peuvent être connues grâce aux informations d'accès d'un dispositif IoT.

La Figure A.1 illustre une méthode permettant de mesurer le temps de transmission aller-retour (RTT) en utilisant un paquet mis en miroir qui indique les performances ou le niveau de sécurité du réseau IMT-2020 privé et en déterminant quels comportements anormaux menacent la sécurité et les performances dudit réseau en fonction du RTT.

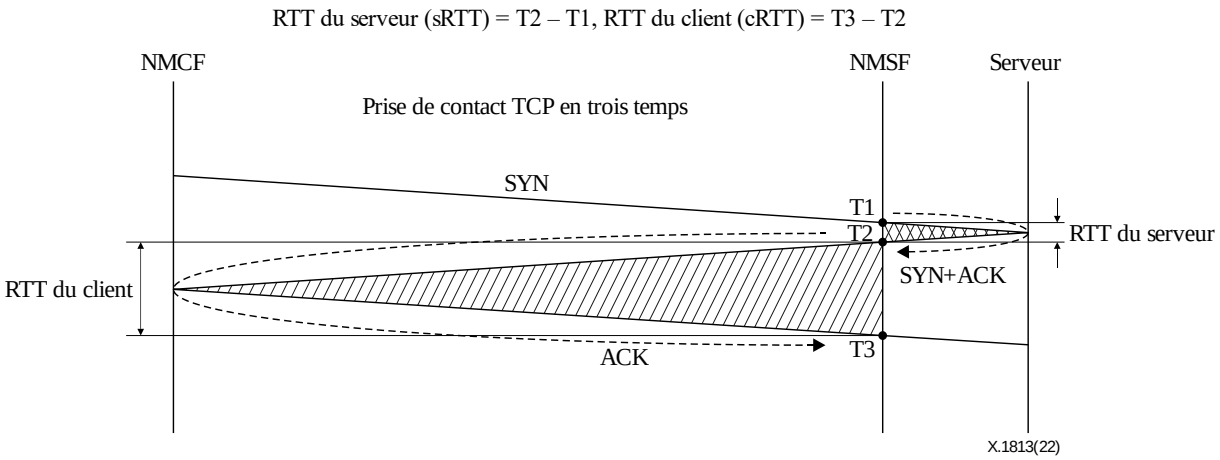

Figure A.1 – Mesure du RTT

En ce qui concerne la Figure A.1, dans le cas d'une prise de contact en trois temps s'inscrivant dans le cadre de la transmission et de la réception d'un signal de synchronisation (SYN), la fonction NMSF calcule le RTT d'un réseau à l'aide de paquets mis en miroir transmis sur celui-ci entre un utilisateur et un serveur. Par exemple, après avoir extrait et enregistré les repères temporels de transmission et de réception de trois paquets (SYN, SYN + ACK et ACK) échangés entre la fonction NMCF (c'est-à-dire le client) et le serveur de la fonction NMSF (ou MEC), la fonction NMSF conserve au moins l'une des informations de temps, soit T1, T2 ou T3. La fonction NMSF calcule le RTT du serveur de la fonction NMCF (sRTT) en soustrayant T1 de T2 (T2 – T1), le RTT du client (cRTT) en soustrayant T2 de T3 (T3 – T2), et le RTT total du réseau en ajoutant sRTT et cRTT (sRTT + cRTT) ou bien en soustrayant T1 de T3 (T3 – T1). En effectuant ce calcul pour chaque transaction, la fonction NMSF calcule le RTT de tout le réseau.

La fonction NMSF analyse l'existence de menaces pouvant nuire aux performances ou à la sécurité du réseau IMT-2020 privé en déterminant si sRTT, cRTT et le RTT du réseau répondent aux exigences applicables aux communications URLLC dudit réseau. La Figure A.2 illustre comment sont identifiés les éléments du réseau IMT-2020 privé qui subissent des pertes de performances à l'aide des temps sRTT et cRTT.

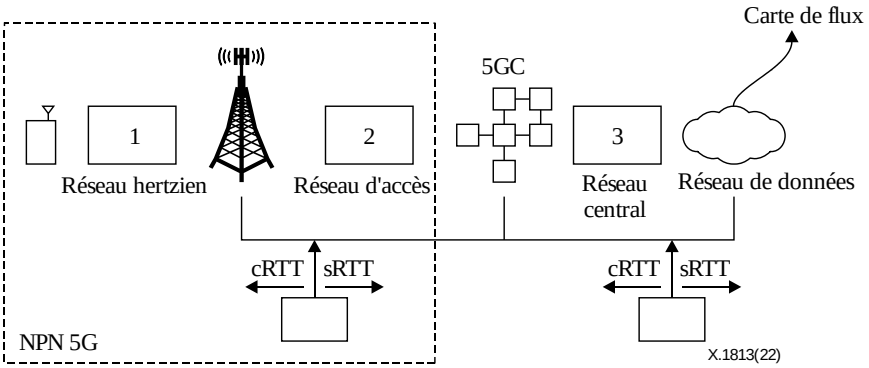

Figure A.2 – Identification des éléments d'un réseau IMT-2020 privé qui subissent des pertes de performances

En plus du RTT, plusieurs autres indicateurs peuvent permettre d'identifier une menace susceptible de nuire aux performances ou à la sécurité. On peut notamment citer: le délai d'attente de réponse, qui représente le temps qui s'écoule avant que le serveur de la fonction NMSF (ou MEC) ne reçoive les premières données associées au contenu provenant d'une adresse URL liée à la demande d'un client; le nombre de sessions en attente de réponse, qui représente le nombre de sessions pour lesquelles une demande du client n'a pas reçu de réponse; le BPS, CPS, TPS et code d'erreur HTTP compris dans l'intervalle 40x ou 50x; les informations contenues dans un paquet mis en miroir concernant la transmission et la réception de données; les informations statistiques obtenues à partir de plusieurs paquets mis en miroir; et des informations en service qui indiquent la possibilité de se connecter à un dispositif IoT ou au serveur de la fonction NMCF.

À l'aide de ces indicateurs, il est possible de mettre en œuvre, de différentes manières, un algorithme permettant d'identifier les menaces pouvant nuire aux performances et à la sécurité. Par exemple, la fonction NMSF détermine l'existence d'une menace pour la sécurité du réseau à l'aide des informations sur le trafic (couches 3 et 4 du modèle OSI), y compris des informations sur un flux de paquets et sur un protocole (couche 7 du modèle OSI).

Outre ce qui précède, diverses techniques peuvent être adoptées, notamment la détection de menaces pour la sécurité du réseau en fonction des informations contenues dans les paquets (par exemple, quand le nombre de connexions sur l'ensemble d'une section d'une adresse IP source prédéterminée à une adresse IP de destination, le BPS d'un serveur, ou la demande d'une URL, dépasse un seuil prédéterminé, on considère qu'il s'agit d'une menace de sécurité), la détection de menaces de sécurité en fonction des informations sur le trafic (par exemple, à l'aide d'une technique de regroupement reposant sur un graphique de distribution du trafic permettant de déterminer si le trafic dépasse un seuil prédéterminé, auquel cas on considère qu'un problème menace la sécurité du réseau IMT-2020 privé), ainsi que la détection de menaces de sécurité fondée sur les informations sur le protocole, les anomalies, les signatures ou les utilisations abusives, l'analyse des protocoles à états, et les spécifications. Le contenu des communications entre les serveurs des fonctions NMCF et NMCF peut aussi être inclus dans l'analyse de la fonction NMSF.

Annexe B

Caractéristiques de la fonction NMCF

(Cette Annexe fait partie intégrante de la présente Recommandation.)

En ce qui concerne l'intégration du serveur NMCF et de la fonction NMSF, un protocole d'échange d'informations de sécurité entre la fonction NMCF (ou serveur NMCF) et la fonction NMSF est nécessaire.

Premièrement, la fonction NMCF détermine s'il existe une menace pour la sécurité du réseau en utilisant les états des dispositifs IoT requis pour son propre fonctionnement, les informations d'état du système ou de journalisation et le RTT. L'état d'un dispositif IoT requis pour le fonctionnement comprend la charge de la CPU, l'utilisation de la mémoire, l'utilisation du stockage et les informations en service. Par exemple, lorsque l'utilisation de la mémoire est égale ou supérieure à une valeur de seuil préconfigurée ou lorsque le RTT est supérieur à une valeur de seuil préconfigurée, la fonction NMCF détermine qu'un comportement anormal menaçant la sécurité et la qualité de fonctionnement s'est produit. Un autre exemple porte sur le fait que, lorsque les informations de journalisation indiquent qu'une entité dont l'adresse IP est interdite a essayé de se connecter à un nœud client, ou qu'un processus inconnu a eu lieu, la fonction NMCF détermine qu'un comportement anormal menaçant la sécurité et la qualité de fonctionnement s'est produit.

La fonction NMCF transmet ensuite la valeur du résultat de contrôle déterminé pour évaluer s'il existe une menace pour la sécurité du serveur NMCF ou de la fonction NMSF. En d'autres termes, la fonction NMSF reçoit un résultat de contrôle concernant une menace pour la sécurité du réseau telle qu'elle est perçue par un point d'extrémité en temps réel. À ce stade, il convient d'identifier un dispositif IoT d'après les informations recueillies par le serveur NMCF par rapport à la fonction NMCF et d'après le contenu de l'analyse de la fonction NMSF, afin que le contenu généré par le dispositif IoT en question puisse être distingué des autres contenus.

La méthode décrite ci-dessus peut réduire la charge sur la fonction NMSF centrale en exécutant un contrôle des menaces aux points d'extrémité, comme la fonction NMCF, ce qui peut, par conséquent, améliorer le contrôle de la qualité de fonctionnement du réseau et des menaces pour la sécurité.

Annexe C

Visualisation des résultats de contrôle

(Cette Annexe fait partie intégrante de la présente Recommandation.)

La Figure C.1 illustre un exemple de visualisation du contrôle de la sécurité et de la qualité de fonctionnement du réseau/système en utilisant la fonction NMSF.

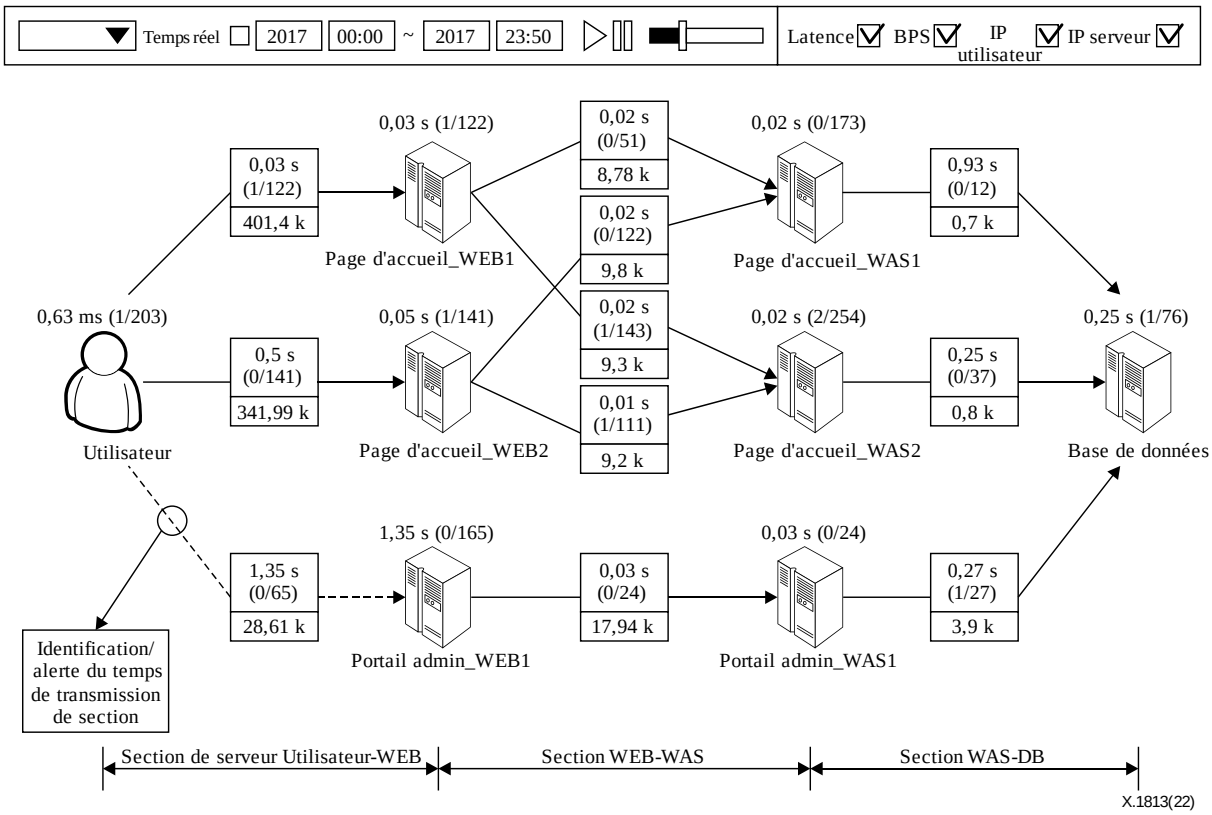

Figure C.1 – Exemple de visualisation du contrôle de la sécurité et de la qualité de fonctionnement du réseau/système

En se reportant à la Figure C.1, les résultats analysés basés sur des indicateurs de qualité de fonctionnement ou des indicateurs de sécurité sont visualisés en temps réel puis transmis aux utilisateurs sous la forme d'une alarme. Les gestionnaires de réseau sont en mesure de faire face immédiatement aux menaces en utilisant ces résultats. Autrement dit, les résultats analysés sont interprétés du point de vue de la qualité de fonctionnement et de la sécurité. Dès que des comportements anormaux sont détectés, le signal d'avertissement est envoyé aux gestionnaires de réseau.

Il est souhaitable que la visualisation exprime de manière intuitive et claire les liens entre les entités d'un réseau. La visualisation est mise en place de telle sorte que la fonction NMSF génère un indicateur de qualité de fonctionnement/sécurité en tant qu'objet, met en œuvre l'objet généré dans un espace visualisé et génère un graphique de flux qui représente le flux de trafic du réseau. Pour cela, les objets doivent être obtenus en générant des indicateurs de qualité de fonctionnement/sécurité en association avec une première entité, des indicateurs de qualité de fonctionnement/sécurité en association avec une seconde entité et des indicateurs de qualité de fonctionnement/sécurité en association avec un lien reliant la première entité et la seconde entité.

Dans un souci de clarté, une ligne reliant la première entité à la seconde entité est représentée sur le graphique de flux, en fonction de la création d'objets relatifs aux indicateurs de qualité de fonctionnement/sécurité associés aux liens. Il est possible d'ajouter des éléments de couleur pour mieux les distinguer. En d'autres termes, au moins une des couleurs, formes et épaisseurs est clairement visualisée en fonction des indicateurs de qualité de fonctionnement/sécurité associés aux liens.

En utilisant cette fonction de visualisation, il est possible d'obtenir une visibilité et une clarté en ce qui concerne toutes les sections de service. Cela améliore non seulement la prévention des problèmes liés aux services de réseau en les gérant, mais permet aussi au réseau de faire face facilement aux menaces qui pèsent sur les vastes infrastructures IoT, telles que les usines intelligentes et les villes intelligentes.

Appendice I

Cas d'utilisation des réseaux privés IMT-2020 pour les services verticaux

(Le présent Appendice ne fait pas partie intégrante de la Recommandation.)

La présente Recommandation est fondée sur trois types d'architectures de réseaux privés IMT-2020, comme indiqué dans la Figure I.1.

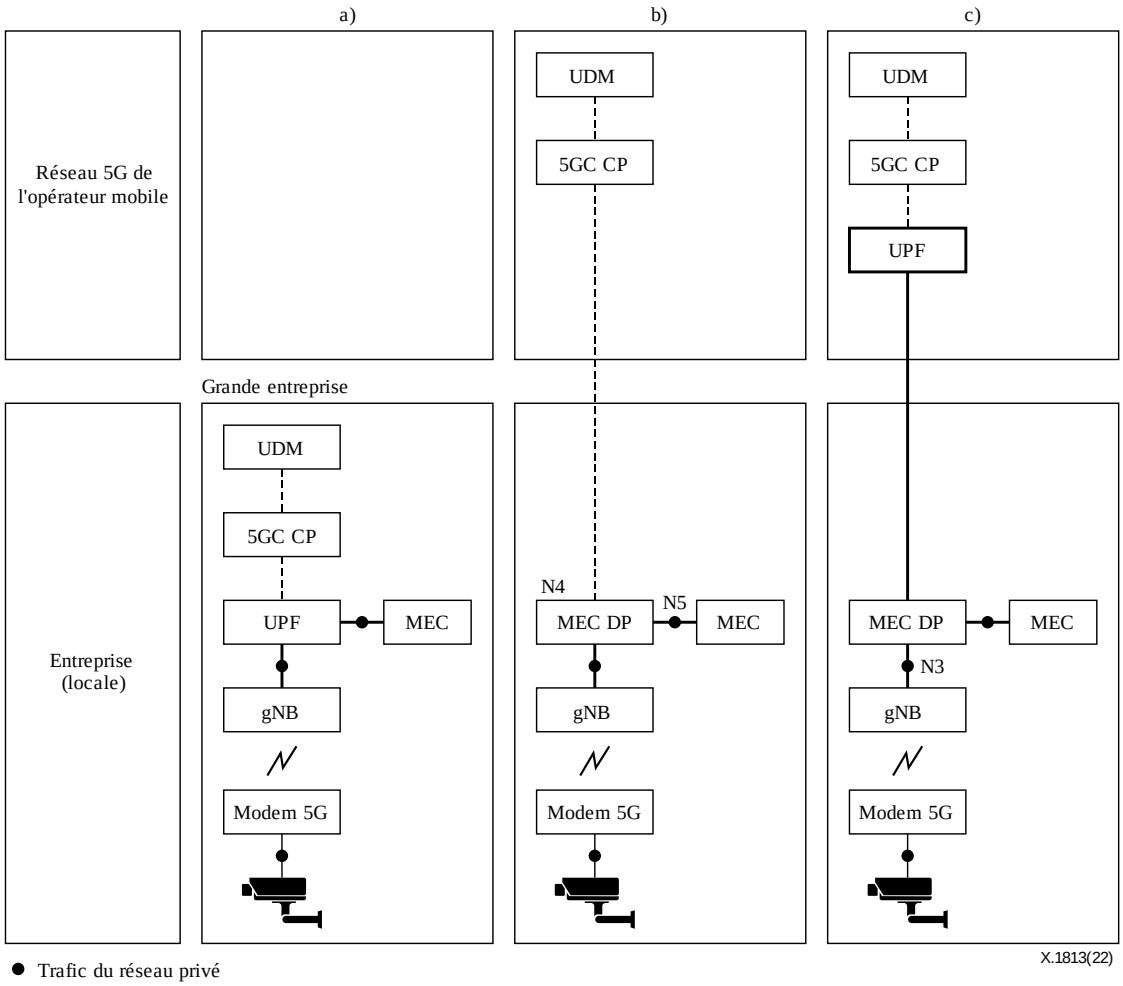

Figure I.1 – Trois types de déploiement d'un réseau privé IMT-2020

Selon [b-Harrison], les réseaux privés IMT-2020 peuvent être déployés comme des réseaux autonomes entièrement isolés (a) ou comme une tranche d'un RMTP conjointement avec un réseau public (b ou c), comme le montre la Figure I.1.

Concernant le type (a), le réseau privé est physiquement séparé du réseau public pour assurer la sécurité complète des données. Étant donné que le temps de transmission du réseau entre le dispositif et le serveur d'applications se compte en quelques millisecondes, il est possible de mettre en place des services d'applications URLLC.

Concernant le type (b), les éléments gNB, UPF et MEC sont déployés au sein de l'entreprise. Dans cette architecture, le réseau d'accès radioélectrique (RAN) et le plan de commande sont partagés entre les réseaux privé et public, ce qui permet d'assurer une sécurité renforcée et une réduction du temps de transmission.

Concernant le type (c), les éléments gNB, MEC et le plan de données MEC (MEC DP) sont déployés au sein de l'entreprise, et la fonction UPF est située dans le nuage périphérique de l'opérateur mobile, loin des dispositifs. Le MEC DP examine les adresses IP de destination des paquets appartenant à tous les tunnels du protocole de tunnellisation GPRS (GTP) provenant du nœud gNB (désencapsulation GTP) et achemine le paquet IP d'utilisateur vers le réseau privé interne s'il s'agit d'un trafic local. Dans cette architecture, une sécurité renforcée et une réduction du temps de transmission peuvent être assurées.

Selon [b-Harrison], le type de déploiement (b) de la Figure I.1 peut être illustré comme la Figure I.2 du point de vue vertical en utilisant le découpage de réseau. La Figure I.2 illustre une architecture fonctionnelle détaillée pour le type de déploiement (b) de la Figure I.1, qui est partagée entre les réseaux privé et public IMT-2020.

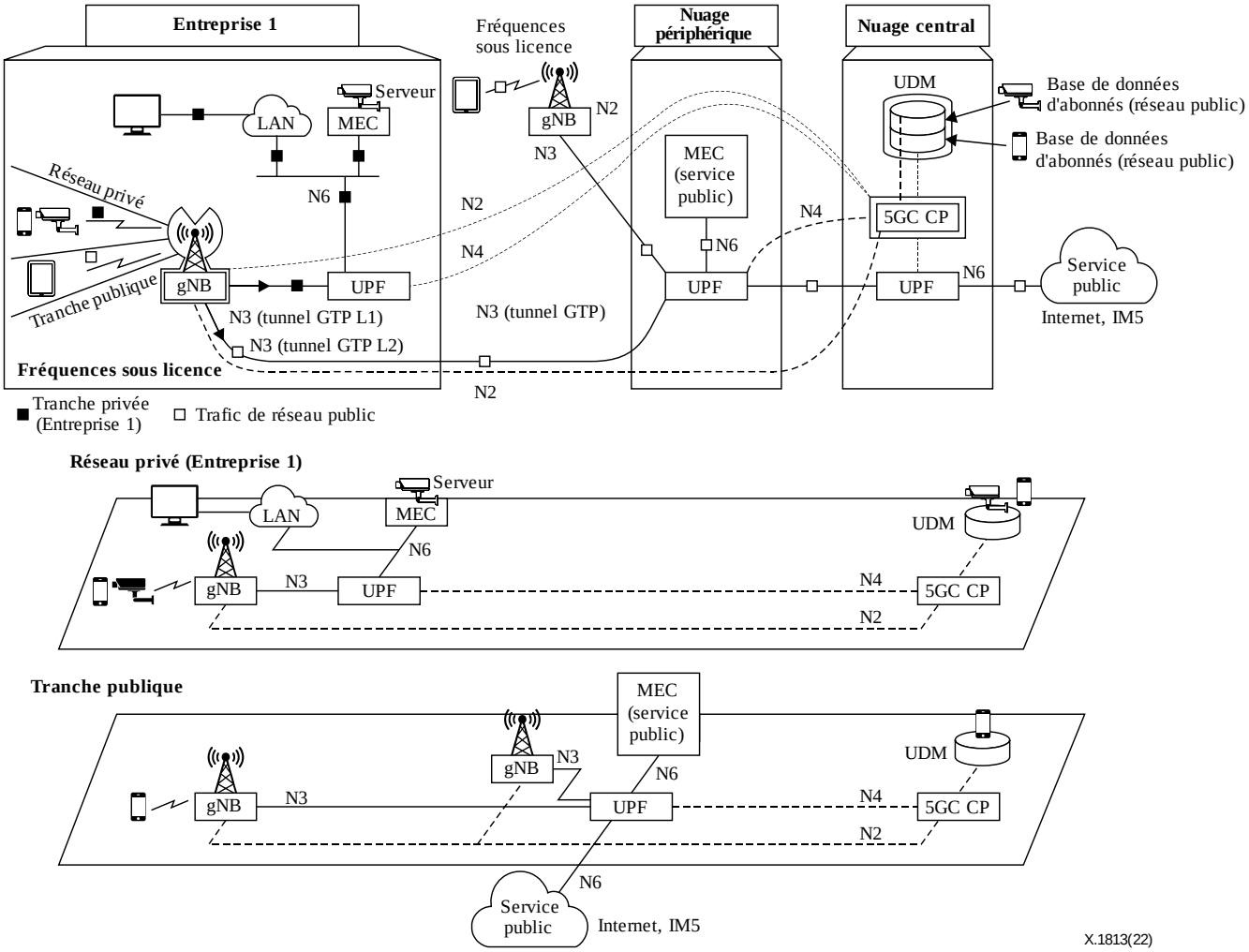

Figure I.2 – Architecture fonctionnelle détaillée pour le type de déploiement (b) de la Figure I.1

Selon [b-Harrison], le type de déploiement (c) de la Figure I.1 peut être illustré comme la Figure I.3 du point de vue vertical en utilisant le découpage de réseau. La Figure I.3 illustre une architecture fonctionnelle détaillée pour le type de déploiement (c) de la Figure I.1, qui est partagée entre les réseaux privé et public IMT-2020.

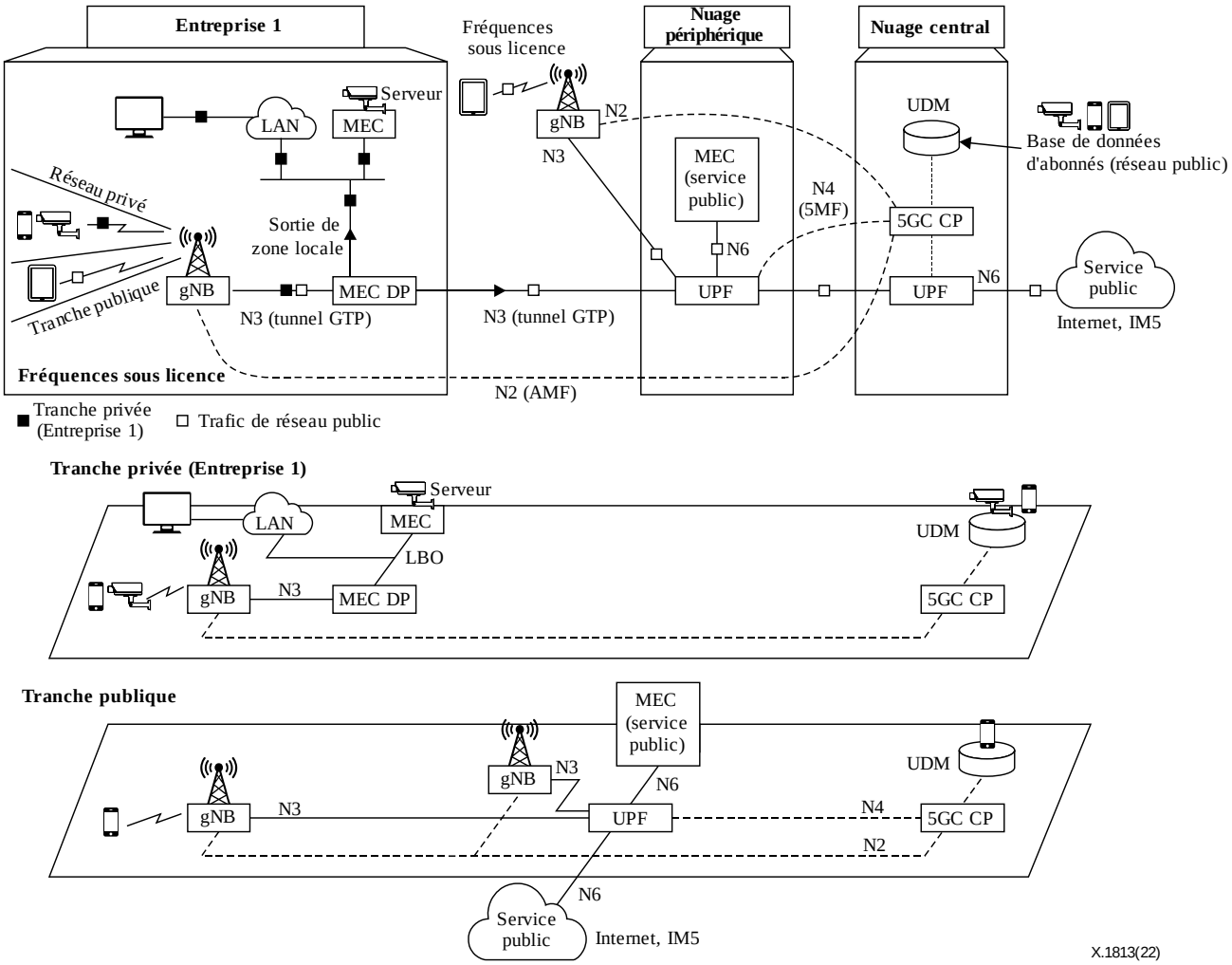

Figure I.3 – Architecture fonctionnelle détaillée pour le type de déploiement (c) de la Figure I.1

Toutes les architectures fonctionnelles des réseaux privés IMT-2020 mentionnées ci-dessus sont déployées par les opérateurs de réseau pour renforcer la sécurité et améliorer la qualité de fonctionnement des communications URLLC. Le maintien de la qualité de fonctionnement et de la sécurité d'un réseau privé IMT-2020 est l'un des facteurs les plus importants dont il faut tenir compte pour garantir que les services verticaux prennent en charge les communications URLLC. L'une des méthodes qu'il est envisageable de mettre en place consiste en une inspection approfondie des paquets (DPI), qui est également décrite dans [b-UIT-T Y.2774] et [b-UIT-T Y.2775]. Toutefois, le champ d'application de ces Recommandations ne concerne que les réseaux mobiles généraux et ne peut donc pas être appliqué aux réseaux privés IMT-2020, et plus particulièrement aux services verticaux prenant en charge les communications URLLC.

Bibliographie

[b-UIT-T Y.2774] Recommandation UIT-T Y.2774 (2019), *Exigences fonctionnelles de l'inspection approfondie des paquets dans les réseaux futurs*.

[b-UIT-T Y.2775] Recommandation UIT-T Y.2775 (2019), *Architecture fonctionnelle de l'inspection approfondie des paquets pour les réseaux futurs*.

[b-UIT-T Y.3100] Recommandation UIT-T Y.3100 (2017), *Réseaux IMT-2020: termes et définitions*.

[b-UIT-T Y.4000] Recommandation UIT-T Y.4000/Y.2060 (2012), *Présentation générale de l'Internet des objets*.

[b-ISO13491-1] ISO-13491-1:2016, Services financiers – *Dispositifs cryptographiques de sécurité (services aux particuliers) – Partie 1: Concepts, exigences et méthodes d'évaluation*.
<https://www.iso.org/standard/61137.html>

[b-ISO/CEI 14888-1] ISO/CEI 14888-1:2008, *Technologies de l'information – Techniques de sécurité – Signatures digitales avec appendice – Partie 1: Généralités*.
<https://www.iso.org/standard/44226.html>

[b-ISO/CEI/IEEE 24765] ISO/CEI/IEEE 24765:2017, *Ingénierie des systèmes et du logiciel – Vocabulaire*.
<https://www.iso.org/standard/71952.html>

[b-ISO/CEI 25010] ISO/CEI 25010:2011, *Ingénierie des systèmes et du logiciel – Exigences de qualité et évaluation des systèmes et du logiciel (SQuaRE) – Modèles de qualité du système et du logiciel*.
<https://www.iso.org/standard/35733.html>

[b-ISO/CEI 27000] ISO/CEI 27000:2016, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*.
<https://www.iso.org/standard/66435.html>

[b-ISO/CEI 27033-1] ISO/CEI 27033-1:2015, *Technologies de l'information – Techniques de sécurité – Sécurité de réseau – Partie 1: Vue d'ensemble et concepts*.
<https://www.iso.org/standard/63461.html>

[b-ISO/PAS 19450] ISO/PAS 19450:2015, *Systèmes d'automatisation et intégration – 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) (Exigences applicables aux services du système 5G (étape 1, version 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) (Architecture de système du système 5G (étape 2, version 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 (Étude relative à l'amélioration du système 5G pour les services verticaux et de réseau local (LAN))*.
<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3487>

[b-5G-PPP] 5G PPP Architecture Working Group (*Groupe de travail sur l'architecture du partenariat public-privé pour la 5G*) (2019), *View on 5G Architecture, Version 3.0 (Vue d'ensemble de l'architecture 5G, 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 (Stratégies de réseau 5G privé des opérateurs mobiles et des opérateurs non mobiles)*.
<https://www.netmanias.com/en/?m=view&id=reports&no=14585>

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2023