الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1813

(2022/09)

السلسلة X: شبكات البيانات والاتصالات
بين الأنظمة المفتوحة ومسائل الأمن

أمن الاتصالات المتنقلة الدولية–2020

المتطلبات الأمنية والمراقبة من أجل تشغيل الخدمات الرأسية التي تدعم الاتصالات فائقة الموثوقية ومنخفضة الكمون (URLLC) في شبكات الاتصالات المتنقلة الدولية–2020 الخاصة

التوصية ITU-T X.1813

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
القياس الحيوي عن بُعد	X.1099–X.1080
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب (1)	X.1149–X.1140
بروتوكولات الأمن (1)	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1309–X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1319–X.1310
أمن شبكة الكهرباء الذكية	X.1339–X.1330
البريد المعتمد	X.1349–X.1340
أمن إنترنت الأشياء (IoT)	X.1369–X.1350
أمن أنظمة النقل الذكية (ITS)	X.1399–X.1370
أمن سجل الحسابات الموزع	X.1429–X.1400
أمن التطبيقات (2)	X.1459–X.1450
أمن شبكة الويب (2)	X.1489–X.1470
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
الدفاع السيبراني	X.1599–X.1590
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680
الاتصالات الكمومية	
المصطلحات	X.1701–X.1700
مولِّد الأعداد العشوائية الكمومية	X.1709–X.1702
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1711–X.1710
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1719–X.1712
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1729–X.1720
أمن البيانات	
أمن البيانات الضخمة	X.1759–X.1750
حماية البيانات	X.1789–X.1770
أمن شبكات الاتصالات المتنقلة الدولية–2020	**X.1819–X.1800**

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1813

المتطلبات الأمنية والمراقبة من أجل تشغيل الخدمات الرأسية التي تدعم الاتصالات فائقة الموثوقية ومنخفضة الكمون (URLLC) في شبكات الاتصالات المتنقلة الدولية–2020 الخاصة

ملخص

توصّف التوصية ITU-T X.1813 المتطلبات الأمنية لتشغيل الخدمات الرأسية التي تدعم الاتصالات فائقة الموثوقية ومنخفضة الكمون (URLLC) في شبكات الاتصالات المتنقلة الدولية–2020 الخاصة. وتحدد التهديدات والمخاطر التي تظهر عند تقديم الخدمات الرأسية التي تدعم الاتصالات URLLC في شبكة الاتصالات المتنقلة الدولية–2020 الخاصة، وتصف سيناريوهات نشر الأمن في شبكة الاتصالات المتنقلة الدولية–2020 الخاصة من أجل تشغيل الخدمات الرأسية التي تدعم الاتصالات URLLC. ولا يندرج رصد محتويات الاتصالات ضمن مجال تطبيق هذه التوصية.

ينحصر الهدف من شبكة الاتصالات المتنقلة الدولية–2020 الخاصة، التي يُنظر إليها أيضاً على أنها شبكة غير عمومية للاتصالات المتنقلة الدولية–2020 (NPN)، في استخدام كيان خاص مثل شركة، ويمكن نشر هذه الشبكة في مجموعة متنوعة من التشكيلات، باستخدام العنصرين الافتراضي والمادي على السواء. وستوفر هذه الشبكة السرعة والكمون المنخفض وغيرهما من المزايا التي تعد بها الاتصالات المتنقلة الدولية–2020 لدعم تطبيقات الجيل التالي.

وفي الخدمات الرأسية للمصانع الذكية والمدن الذكية التي تستخدم شبكة خاصة للاتصالات المتنقلة الدولية–2020، تستخدم العديد من أجهزة إنترنت الأشياء (IoT) الاتصالات الآلية الكثيفة (mMTC) والاتصالات فائقة الموثوقية ومنخفضة الكمون (URLLC). ويمكن أن تتعرض هذه الاتصالات لتهديدات أمنية وما يرتبط بها من مخاطر. وبالإضافة إلى ذلك، يمكن أن تتسبب هذه التهديدات في تدهور التشغيل المستقر للخدمات الرأسية التي تدعم الاتصالات URLLC. ولا يمكن ضمان معرفة الحالات التي يتدهور فيها أداء الخدمات الرأسية بسبب هذه المخاطر.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1813	2022-09-02	17	11.1002/1000/14991

مصطلحات أساسية

تفحص الرزم المعمق، كشف النقطة الطرفية والتصدي لها، حوسبة الحافة متعددة النفاذ، شبكة غير عمومية، مراقبة الشبكة، الأداء، شبكة الاتصالات المتنقلة الدولية–2020 الخاصة، الأمن، وظيفة مستوي المستعمل.

* للنفاذ إلى التوصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة الأمم المتحدة المتخصصة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

المتطلبات الأمنية والمراقبة من أجل تشغيل الخدمات الرأسية التي تدعم الاتصالات فائقة الموثوقية ومنخفضة الكمون (URLLC) في شبكات الاتصالات المتنقلة الدولية–2020 الخاصة

1 مجال التطبيق

توصّف هذه التوصية المتطلبات الأمنية لتشغيل الخدمات الرأسية التي تدعم الاتصالات فائقة الموثوقية ومنخفضة الكمون (URLLC) في شبكات الاتصالات المتنقلة الدولية–2020 الخاصة. وتحدد التوصية التهديدات والمخاطر التي تظهر عند تقديم الخدمات الرأسية التي تدعم الاتصالات URLLC في شبكات الاتصالات المتنقلة الدولية–2020 الخاصة، وتصف سيناريوهات نشر الأمن في شبكات الاتصالات المتنقلة الدولية–2020 الخاصة من أجل تشغيل الخدمات الرأسية التي تدعم الاتصالات URLLC.

لأغراض حماية الخصوصية، تقع مراقبة محتويات الاتصالات خارج مجال تطبيق هذه التوصية.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T Y.3102] التوصية ITU-T Y.3102 (2018)، *إطار شبكة الاتصالات المتنقلة الدولية–2020*.

3 التعاريف

1.3 المصطلحات المعرَّفة في مراجع أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في مراجع أخرى:

1.1.3 شبكة غير عمومية من الجيل الخامس (5G non-public network) [b-3GPP TS 22.261]: شبكة من الجيل الخامس مخصصة للاستعمال الخاص.

2.1.3 هجوم (attack) [b-ISO13491-1]: محاولة الحصول على معلومات حساسة أو خدمة أو تعديلهما من جانب أحد الخصوم غير المرخص لهم بذلك.

الملاحظة 1 – تشمل وظائف الشبكة (NF) على سبيل المثال لا الحصر وظائف عقدة الشبكة، مثل إدارة الدورة وإدارة التنقلية ووظائف النقل التي يعرّف سلوكها الوظيفي وسطوحها البينية.

الملاحظة 2 – يمكن تنفيذ وظائف الشبكة على عتاد مخصص أو كوظائف برمجيات ممثَّلة افتراضياً.

الملاحظة 3 – لا تعتبر وظائف الشبكة موارد وإنما يمكن تمثيل حالة أي من وظائف الشبكة باستعمال الموارد.

3.1.3 النشر (deployment) [b-ISO/IEC/IEEE 24765]: مرحلة في مشروع يجري فيها تشغيل نظام وحل إشكالات الانتقال إلى المرحلة التالية.

4.1.3 الميدان (domain) [b-ISO/IEC 14888-1]: مجموعة من الكيانات تعمل بموجب سياسة أمنية واحدة.

مثال: شهادات المفتاح العمومي التي تنتجها سلطة واحدة أو مجموعة من السلطات تستعمل سياسة الأمن نفسها.

5.1.3 إنترنت الأشياء (IoT) [b-ITU-T Y.4000]: بنية تحتية عالمية لمجتمع المعلومات، تمكّن الخدمات المتطورة عن طريق التوصيل البيني للأشياء (المادية والافتراضية) استناداً إلى تكنولوجيات المعلومات والاتصالات القابلة للتشغيل البيني القائمة والمتطورة.

6.1.3 مراقبة الشبكة (network monitoring) [b-ISO/IEC 27033-1]: عملية المراقبة والاستعراض المستمرين للبيانات المسجلة بشأن نشاط الشبكة وعملياتها، بما في ذلك سجلات التدقيق والإنذارات والتحليلات ذات الصلة.

7.1.3 وظيفة الشبكة (network function) [ITU-T Y.3100]: في سياق الاتصالات المتنقلة الدولية–2020، هي وظيفة المعالجة في الشبكة.

8.1.3 النظام (system) [b-ISO/IEC 27000]: تطبيقات أو خدمات أو أصول تكنولوجيا المعلومات أو غيرها من مكونات تداول المعلومات.

9.1.3 صاحب المصلحة (stakeholder) [b-ISO/PAS 19450]: فرد أو منظمة أو مجموعة من الأشخاص لديهم مصلحة، أو قد يتأثرون، بالنظام الجاري التفكير فيه أو تطويره أو نشره.

10.1.3 الثقة (trust) [b-ISO/IEC 25010]: درجة ثقة المستعمل أو أي صاحب مصلحة آخر بأن المنتج أو النظام سيتصرف على النحو المقصود.

11.1.3 الخدمة الرأسية (vertical service) [b-5G-PPP]: من منظور الأعمال، هي خدمة تركز على صناعة محددة أو مجموعة من العملاء ذوي الاحتياجات المتخصصة (مثل خدمات السيارات وخدمات الترفيه وخدمات الصحة الإلكترونية والصناعة 4.0).

2.3 المصطلحات المعرفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 نظام الاتصال في الاتصالات المتنقلة الدولية–2020 (IMT-2020 communication system): نظام لإدارة عملية الاتصال في الاتصالات المتنقلة الدولية–2020 من أجل خدمات الاتصالات المتنقلة الدولية–2020.

الملاحظة 1 – تشير شبكات الجيل الخامس (5G) إلى الاتصالات المتنقلة الدولية–2020 في سياق قطاع تقييس الاتصالات.

الملاحظة 2 – نظام الاتصالات المتنقلة الدولية–2020 مطابق للنظام IMT-2020 في هذه التوصية.

2.2.3 النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020 (IMT-2020 ecosystem): مجموعة من أصحاب المصلحة تتفاعل لتشكيل نظام اتصالات متنقلة دولية–2020 يعمل بشكل مستقر.

ملاحظة – يتعلق المصطلح بتطوير تكنولوجيا الاتصالات من الجيل الخامس، حيث يساهم مجتمع أصحاب المصلحة من دوائر الصناعة والأوساط بالمنتجات والتكنولوجيا والخبرات الخاصة بهم لتمكين الوظائف في طبقات مختلفة من مكدس قيم النظام 5G مثل البنية التحتية والشبكة والمنصة والخدمة والتطبيق.

3.2.3 شبكة الاتصالات المتنقلة الدولية–2020 الخاصة (IMT-2020 private network): شبكة غير عمومية من الجيل الخامس (انظر الفقرة 1.1.3) تستخدم العناصر الافتراضية والمادية لنظام الاتصالات المتنقلة الدولية–2020 وينحصر الهدف من هذه الشبكة في استخدام كيان خاص مثل شركة.

4.2.3 خدمة الاتصالات المتنقلة الدولية–2020 (IMT-2020 service): ميزة يوفرها النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

5GC شبكة الجيل الخامس الأساسية *(5G Core)*

AMF وظيفة إدارة النفاذ والتنقلية *(Access and Mobility Management Function)*

DDoS رفض الخدمة الموزع *(Distributed Denial of Service)*

DPI تفحص الرزم المعمق *(Deep Packet Inspection)*

EC حوسبة الحافة *(Edge Computing)*

EDR كشف النقطة الطرفية والتصدي لها *(Endpoint Detection and Response)*

GTP بروتوكول نفقي للخدمة الراديوية العامة بأسلوب الرزم *(GPRS Tunnelling Protocol)*

IoT إنترنت الأشياء *(Internet of Things)*

MEC حوسبة الحافة متعددة النفاذ *(Multi-access Edge Computing)*

MEC DP مستوي البيانات لحوسبة الحافة متعددة النفاذ *(MEC Data Plane)*

mMTC الاتصالات الآلية الكثيفة *(massive Machine Type Communications)*

NF وظيفة الشبكة *(Network Function)*

NMCF وظيفة عميل مراقبة الشبكة *(Network Monitoring Client Function)*

NMF وظيفة مراقبة الشبكة *(Network Monitoring Function)*

NMSF وظيفة مخدم مراقبة الشبكة *(Network Monitoring Server Function)*

NPN شبكة غير عمومية *(Non-Public Network)*

PLMN شبكة متنقلة برية عمومية *(Public Land Mobile Network)*

RTT مدة الذهاب والإياب *(Round Trip Time)*

SBA معمارية قائمة على الخدمة *(Service-Based Architecture)*

SMF وظيفة إدارة الدورة *(Session Management Function)*

UDM إدارة البيانات الموحدة *(Unified Data Management)*

UE معدات المستعمل *(User Equipment)*

UID هوية المستعمل *(User ID)*

UPF وظيفة مستوي المستعمل *(User Plane Function)*

URLLC اتصالات فائقة الموثوقية منخفضة الكمون *(Ultra-Reliable and Low-Latency Communication)*

5 الاصطلاحات

تستخدم هذه التوصية الاصطلاحات التالية:

كلمة "**يُشترط**" تدل على متطلب يجب التقيد به تماماً ولا يسمح بأي انحراف عنه في حال ادعاء الامتثال لهذه التوصية.

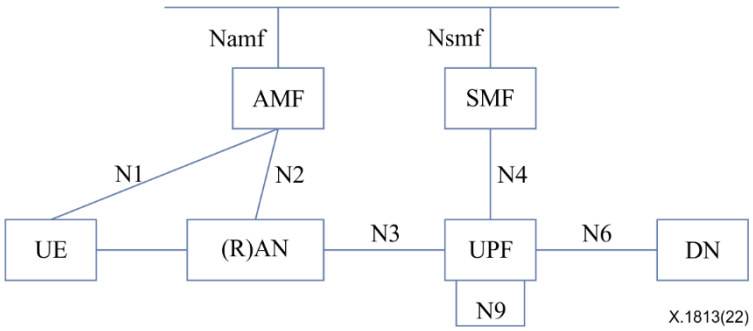
وتدل كلمة "**يُوصى**" على متطلب يُوصى به لكنه غير إلزامي في المطلق. وبالتالي لا يتعين توفر هذا المتطلب لزعم الامتثال.

وتدل كلمة "**يحظر**" على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم الامتثال لهذه التوصية.

وتدل عبارة "**من الجائز**" على متطلب اختياري مسموح به دون أن ينطوي على أي توصية به. ولا يرمي هذا المصطلح إلى إلزام تطبيق البائع بتقديم هذا الخيار الذي يمكن أن يقدمه مشغل الشبكة/مورد الخدمة اختيارياً. وبالأحرى، فإن البائع يمكنه إدراج هذه الخاصية اختيارياً ويدعى إلى الامتثال لهذه المواصفة في نفس الوقت.

6 نظرة عامة

صمم نظام الاتصالات المتنقلة الدولية–2020 خصيصاً لدعم مشغلي الشبكات من أجل توصيلية البيانات والخدمات استناداً إلى تقنيات مثل التمثيل الافتراضي لوظائف الشبكة والتوصيل الشبكي المعرَّف بالبرمجيات. ويعرّف مشروع شراكة الجيل الثالث (3GPP) المعمارية القائمة على الخدمة (SBA) في الوثيقة [b-3GPP TS 23.501] حيث تُقدم وظيفة مستوي التحكم ومستودعات البيانات المشتركة للشبكة IMT-2020 بواسطة مجموعة من وظائف الشبكة الموصولة بينياً (NF)، ولكل منها إذن بالنفاذ إلى خدمات بعضها البعض. ويعرض الشكل 1 معمارية النظام IMT-2020.



الشكل 1 – معمارية نظام الاتصالات المتنقلة الدولية–2020

تتألف معمارية نظام الاتصالات المتنقلة الدولية–2020 المعرّفة في التوصية [ITU-T Y.3102] وفي الوثيقة [b-3GPP TS 23.501] من وظائف الشبكة التالية:

- وظيفة إدارة النفاذ والتنقلية (AMF) التي توفر وظيفة إدارة التسجيل ووظيفة إدارة التوصيل ووظيفة إدارة التنقلية ووظيفة استيقان النفاذ ووظيفة تخويل النفاذ ووظيفة إدارة خدمات الموقع ووظيفة التبليغ بتنقلية معدات المستعمل (UE) وما إلى ذلك.
- شبكة البيانات (DN)، مثل خدمات المشغل، أو النفاذ إلى الإنترنت أو خدمات الطرف الثالث.
- وظيفة إدارة الدورة (SMF) التي توفر إنشاء الدورة ووظائف التعديل والتحرير ووظائف توزيع وإدارة عناوين بروتوكول الإنترنت لمعدات المستعمل (UE) واختيار وظيفة مستوى المستعمل والتحكم فيها وجمع بيانات الترسيم ودعم السطوح البينية للترسيم والتحكم في جمع بيانات الترسيم وتنسيقها في وظيفة مستوي المستعمل (UPF)، والإخطار ببيانات الوصلة الهابطة، ودعم ضغط الرأسية وغيرها من الوظائف.
- تعالج وظيفة مستوي المستعمل (UPF) مسير مستوي مستعمل دورات وحدة بيانات البروتوكول (PDU). ويدعم مشروع 3GPP عمليات النشر باستخدام وظيفة UPF واحدة أو وظائف UPF متعددة لدورة PDU معينة. ويُنفذ اختيار مستوي المستعمل بواسطة وظيفة إدارة الدورة. وتوفر وظيفة UPF توزيع عنوان/سابقة عنوان بروتوكول الإنترنت لمعدات

المستعمل (UE) استجابة لطلب وظيفة إدارة الدورة، ووظيفة تسيير الحزم وإعادة تسييرها، ووظيفة فحص الرزم، ومعالجة جودة الخدمة لمستوي المستعمل، والتخزين المؤقت لحزم الوصلة الهابطة، وإثارة الإخطار ببيانات الوصلة الهابطة وما إلى ذلك.

- Namf: يحدد Namf سطحاً بينياً قائماً على الخدمة لوظيفة النفاذ وإدارة التنقلية الأساسية.
- Nsmf: يحدد Nsmf سطحاً بينياً قائماً على الخدمة لوظيفة إدارة الدورة.
- UE: معدات المستعمل.
- (R)AN: شبكة النفاذ الراديوي.

تتضمن معمارية النظام IMT-2020 النطاق المرجعية التالية:

- N1: نقطة مرجعية بين معدات المستعمل ووظيفة إدارة النفاذ والتنقلية.
- N2: نقطة مرجعية بين (R)AN ووظيفة إدارة النفاذ والتنقلية.
- N3: نقطة مرجعية بين (R)AN ووظيفة مستوي المستعمل.
- N4: نقطة مرجعية بين وظيفة إدارة الدورة ووظيفة مستوي المستعمل.
- N6: نقطة مرجعية بين وظيفة مستوي المستعمل وشبكة بيانات (DN).
- N9: نقطة مرجعية بين وظيفتين من وظائف مستوي المستعمل.

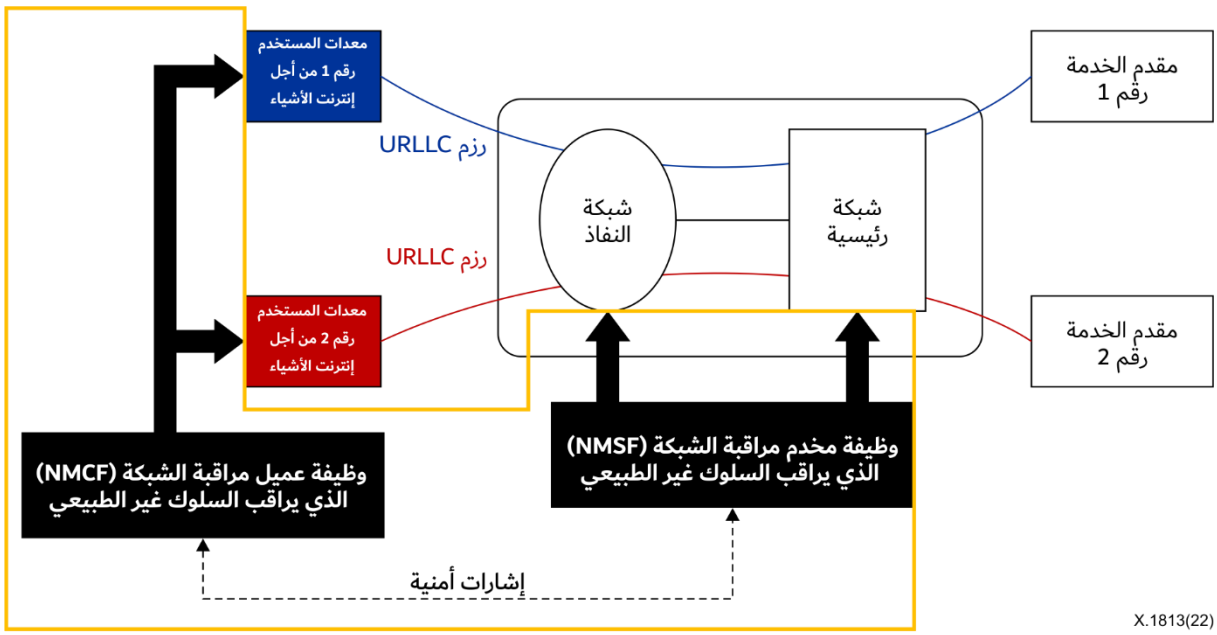
ينحصر الهدف من شبكة الاتصالات المتنقلة الدولية–2020 الخاصة في استخدام كيان خاص مثل شركة، ويمكن نشر هذه الشبكة في مجموعة متنوعة من التشكيلات، باستخدام العنصرين الافتراضي والمادي لأنظمة الاتصالات IMT-2020. وتستند الشبكة الخاصة IMT-2020 إلى المبادئ المعمارية للنظام IMT-2020 المعرّفة في المرجع [b-3GPP TS 23.501]، والتي تشمل مرونة ونمطية الوظائف المستحدثة حديثاً. ويوضح التذييل I المعمارية الوظيفية للشبكة الخاصة IMT-2020.

وتتوقع مواصفات مشروع الشراكة 3GPP [b-3GPP TS 23.501] مجموعة متنوعة من سيناريوهات نشر الشبكة الخاصة. وعلى أعلى مستوى، يمكن تقسيم الشبكات الخاصة إلى فئتين:

- شبكات خاصة IMT-2020 تُنشر كشبكات معزولة ومستقلة تماماً؛
- شبكات خاصة IMT-2020 تُنشر كشريحة من شبكة متنقلة برية عمومية (PLMN) بالاقتران مع شبكة عامة.

ومن ناحية أخرى، تعرّف إنترنت الأشياء (IoT) [b-ITU-T Y.4000] بأنها بنية تحتية عالمية لمجتمع المعلومات، تمكّن الخدمات المتقدمة عن طريق التوصيل البيني للأشياء (المادية والافتراضية) استناداً إلى تكنولوجيات المعلومات والاتصالات القابلة للتشغيل البيني القائمة والمتطورة. وفي هذه التوصية، تكون حالة الاستخدام الرئيسية لهذه الخدمات الرأسية هي خدمة إنترنت الأشياء. وفي هذا السياق، يمكن أن تكون أجهزة إنترنت الأشياء هي الأجهزة التمثيلية لمعدات المستعمل المحددة في المعيار [b-3GPP TS 22.261] للشراكة 3GPP.

ومع دخول تكنولوجيا الاتصالات المتنقلة الدولية–2020 مرحلة التسويق، ستُستخدم الشبكة الخاصة IMT-2020 بشكل رئيسي لبناء الخدمات الرأسية للاتصالات المتنقلة الدولية–2020 باستخدام أجهزة إنترنت الأشياء الصناعية، مثل خدمات المصانع الذكية والمدن الذكية التي تتطلب أداء في الوقت الفعلي مع اتصالات فائقة الموثوقية ومنخفضة الكمون (URLLC). ولذلك، يجب أن تستوفي الشبكات الخاصة IMT-2020 مختلف المتطلبات من حيث الأمن والأداء لأنها تعالج بيانات حساسة زمنياً وفقاً للتوصية [ITU-T Y.3102]. ويوضح الشكل 2 المعمارية الأمنية الشاملة للشبكات الخاصة IMT-2020 وفقاً للمعيار [b-3GPP TR 23.734].



الشكل 2 – معمارية الشبكة الخاصة IMT-2020

إشارة إلى الشكل 2، تمكّن المعمارية الأمنية للشبكة الخاصة IMT-2020 المشغلين من مراقبة أمن/أداء الاتصالات بين عقد الشبكة ومعدات مستعمل النقطة الطرفية في الشبكة الخاصة IMT-2020 لتشغيل الخدمات الرأسية التي تدعم الاتصالات فائقة الموثوقية ومنخفضة الكمون.

7 التهديدات التي تتعرض لها الخدمات الرأسية التي تدعم الاتصالات فائقة الموثوقية ومنخفضة الكمون في الشبكات الخاصة IMT-2020

تغطي إنترنت الأشياء مجموعة واسعة من الفرص الجديدة والمثيرة، مثل أنظمة الأتمتة والتحكم الصناعية (IACS)، والاتصالات في المركبات ذاتية القيادة، والشبكات الذكية، وأجهزة استشعار الطرق السريعة/حركة المرور، والاتصالات في الطائرات بدون طيار، وأجهزة الاستشعار الطبية، والواقع المعزز/الواقع الافتراضي، التي تعمل غالباً بطريقة آلية. وقد يتعين أيضاً أن تفي خدمات إنترنت الأشياء بخصائص الاتصالات URLLC [b-3GPP TS 22.261]، ينحصر الهدف من الشبكات الخاصة في استخدام كيان خاص مثل شركة، ولا يحق إلا لمعدات المستعمل المصرح لها النفاذ إلى شبكة خاصة.

وفي مثل هذه البيئة، تُحدد التهديدات التي تتعرض لها الخدمات الرأسية من بين أمور أخرى، بوصفها أي هجمات يمكن أن تضر بالمكونات والسطوح البينية للشبكة الخاصة IMT-2020 في جوانب الكمون. ويمكن نشر الشبكة الخاصة IMT-2020 مع وظيفة مستوي المستعمل/حوسبة الحافة متعددة النفاذ (MEC) أو بدونها. ويمكن النفاذ إلى وظيفة مستوي المستعمل عبر الإنترنت عن طريق السطح البيني N6 الذي يحدده مشروع الشراكة 3GPP. ولذلك، في حال نشر شبكة خاصة IMT-2020 مع وظيفة مستوي المستعمل وحوسبة الحافة متعددة النفاذ، يكون السطح البيني N6 معرضاً لهجوم كبير نظراً لإمكانية نفاذ المهاجمين إلى الإنترنت في أي مكان. وتحدث هذه الهجمات عن قصد أو عن غير قصد من خارج الشبكة الخاصة IMT-2020 وداخلها.

ويمكن سرد التهديدات التي تتعرض لها وظيفة مستوي المستعمل وحوسبة الحافة متعددة النفاذ والسطح البيني N6 على النحو التالي:

- هجمات رفض الخدمة الموزع (DDoS)؛
- التجسس على حركة/بيانات وصلات الاتصالات؛
- زيادة غير متوقعة في الحركة أو حركة غير عادية يتم إنشاؤها بواسطة معدات المستعمل في شبكة خاصة IMT-2020.

تُنشر الشبكة الخاصة IMT-2020 بشكل خاص باستخدام مكونات الشبكة والسطوح البينية وأجزاء منها جديدة ومختلفة عن تلك الموجودة في الشبكات القائمة في الجانب الأمني. ويستخدم السطح البيني N3 الذي يصل بين شبكة النفاذ والشبكة الأساسية أمن بروتوكول الإنترنت من أجل أمن النقل. ويصل السطح البيني N4 بين وظيفة مستوي المستعمل ووظيفة إدارة النفاذ والتنقلية. ويُغلق السطح البيني N4 هذا في شبكة رزم أساسية متطورة (EPC) من الجيل الرابع ولكن ليس في شبكة IMT-2020 vEPC. وبالمقارنة مع السطح البيني X6، لا يمكن النفاذ إلى الإنترنت عبر N3 وN4، ومع ذلك، هناك احتمال حدوث أنواع جديدة من التهديدات والعقبات غير المقصودة.

ويمكن سرد التهديدات التي يتعرض لها السطحان البينيان N3 وN4 على النحو التالي:

- عدم كفاية أساليب التحكم المنفذة في الشبكة الخاصة IMT-2020
- القيود المفروضة على التدابير والإجراءات الأمنية التي ينفذها مشغل الشبكة الخاصة IMT-2020؛
- مكونات شبكية سيئة التصميم أو مشكّلة بشكل خاطئ في الشبكة الخاصة IMT-2020 لا تمثل زيادة مفاجئة في النفاذ.

كما أن نقص الخبراء غير المعتادين على العديد من الميزات الجديدة لشبكة الاتصالات المتنقلة الدولية–2020 يمكن أن يشكل تهديداً وحاجزاً غير مقصودين.

8 المخاطر بالنسبة للخدمات الرأسية التي تدعم الاتصالات فائقة الموثوقية ومنخفضة الكمون في الشبكات الخاصة IMT-2020

توفر الشبكة الخاصة IMT-2020 أساساً شبكة عالية الثقة في البنية التحتية لإنترنت الأشياء لأن الشبكة الخاصة IMT-2020 قد قام بتقييمها مشروع الشراكة 3GPP لأغراض أمنية للخدمات الرأسية IMT-2020 الناشئة.

وعلى الرغم من الأساليب الأمنية التقليدية للاستيقان والتخويل وسرية البيانات التي يوفرها مشروع الشراكة 3GPP والمعايير الأمنية الأخرى، لا يزال من الممكن أن تتعرض الشبكات الخاصة IMT-2020 لمخاطر عديدة. فعلى سبيل المثال، لا يمكن للأساليب الأمنية القائمة أن تتخلص من التهديدات الناجمة عن السلوك غير الطبيعي لمعدات المستعمل في الشبكة الخاصة IMT-2020.

وبما أن شبكات الاتصالات المتنقلة الدولية–2020 تتمتع بخصائص أقوى تتمحور حول البرمجيات، فقد تتعرض لعدد أكبر من البرمجيات المتعلقة بالبرمجيات مثل عيوب تطوير البرمجيات وإجراءات التحديث غير الصحيحة وأخطاء التشكيل. ونتيجة لذلك، قد تعاني شبكة IMT-2020 من تدهور الأداء بسبب المخاطر المختلفة المذكورة أعلاه.

وفي هذا السياق، قد يشمل تأثير هذه المخاطر ما يلي:

- تشغيل غير مستمر وخطير للخدمات الرأسية. قد يشكل السلوك غير الطبيعي لأجهزة إنترنت الأشياء في شبكة IMT-2020 تهديداً للتشغيل العادي للبنية التحتية للمدن الذكية.
- تدمير أو تعديل أو تغيير المعلومات المخزنة أو المرسلة داخل البنى التحتية في شبكة الاتصالات المتنقلة الدولية–2020.
- تدهور أداء خدمة IMT-2020 URLLC: إذا لم تتمكن الشبكة IMT-2020 من ضمان متطلبات الخدمة IMT-2020 URLLC ذات الكمون المنخفض، فقد تعاني الشبكة من تدهور الأداء، مما قد يؤدي إلى تأثير سلبي على الخدمات الرأسية المرتبطة بها الحساسة زمنياً. وعلى سبيل المثال، بما أن المصانع الذكية مصممة وفقاً لمتطلبات URLLC، فقد تتدهور جودة الإنتاج أو سرعته إذا لم تُستوف متطلبات الكمون المنخفض. وقد يؤدي ذلك ليس فقط إلى خسارة اقتصادية ضخمة، بل يمكن أن يسبب أيضاً حوادث السلامة. ومن الأمثلة الأخرى جودة الصورة للكاميرات الأمنية التي يمكن أن تتدهور بشكل كبير بسبب تأخر توصيل أجهزة الاستشعار المختلفة.

وبالتالي، يتعين وضع متطلبات أمنية لتشغيل الخدمات الرأسية الداعمة للاتصالات URLLC في شبكات خاصة IMT-2020 للتصدي للتهديدات والمخاطر المذكورة أعلاه.

9 سيناريوهات نشر الوظائف الأمنية لتشغيل الخدمات الرأسية التي تدعم الاتصالات URLLC في شبكات خاصة IMT-2020

تحدد هذه الفقرة سيناريوهات نشر الوظائف الأمنية لتشغيل الخدمات الرأسية التي تدعم الاتصالات URLLC في شبكة خاصة IMT-2020. وتُشكَّل معمارية أمن الشبكة الخاصة IMT-2020 بواسطة وظائف مراقبة الشبكة (NMF). وتتكون وظيفة مراقبة الشبكة من وظيفة مخدم مراقبة الشبكة (NMSF) ووظيفة عميل مراقبة الشبكة (NMCF). ويمكن تنفيذ وظيفة مراقبة الشبكة بوظيفة تفحص الحزم المتعمق (DPI) المنشورة في عقدة الشبكة أو بواسطة عقدة شبكة DPI مخصصة.

ويمكن تشكيل الوظائف NMSF كعقد شبكة مستقلة بمعزل عن وظيفة مستوي المستعمل أو حوسبة الحافة متعددة النفاذ. ويجب أن تقترن وظائف NMSF إما بدخل أو خرج وظيفة مستوي المستعمل أو حوسبة الحافة متعددة النفاذ حتى تتمكن من مراقبة الرزم الخاصة بها.

وهناك ثلاثة سيناريوهات لنشر الوظائف NMSF على النحو التالي:

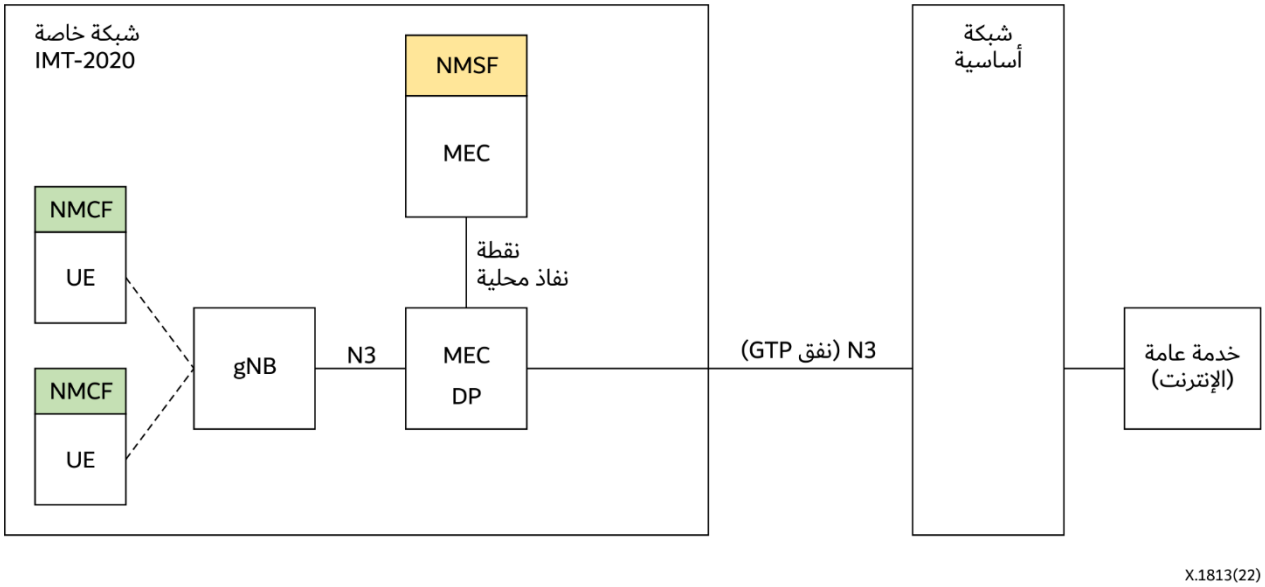
أ) إدماج وظيفة NMSF كعقدة في حوسبة الحافة متعددة النفاذ

ب) تنفيذ وظيفة مخدم مراقبة الشبكة كعقدة منفصلة لمراقبة خرج الرزم من وظيفة مستوي المستعمل.

ج) تشكيل وظائف NMSF متعددة بحيث تُدمج وظيفة NMSF أولى كعقدة في حوسبة الحافة متعددة النفاذ وتُنفّذ وظيفة NMSF ثانية كعقدة منفصلة لمراقبة خرج الرزم من وظيفة مستوي المستعمل.

في سيناريوهات النشر الثلاثة هذه، هناك مشكلة في التنفيذ، سواء وُزعت بروتوكولات IP معينة لوظائف NMSF أم لا. وتُدمج وظيفة عميل مراقبة الشبكة (NMCF) في معدات المستعمل في جميع سيناريوهات النشر الثلاثة هذه.

ويصف الشكل 3 سيناريو النشر A في معمارية أمنية للشبكة الخاصة IMT-2020 حيث تُشكّل العديد من وظائف NMCF وNMSF.



الشكل 3 – سيناريو النشر A

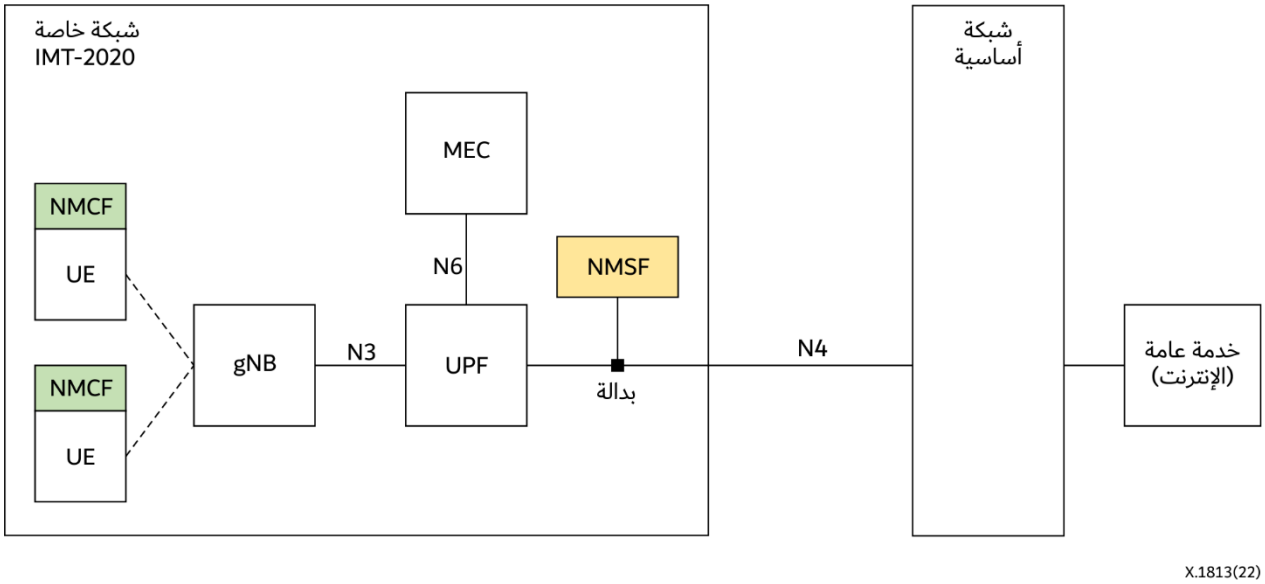
بالإشارة إلى الشكل 3، يمكن دمج وظائف عميل مراقبة الشبكة في معدات المستعمل الخاصة بها، لا سيما أجهزة إنترنت الأشياء التي تتواصل مع العقدة gNB. ويعد تثبيت وظائف NMCF على أجهزة إنترنت الأشياء أحد الحلول الفعالة التي تضمن أمن الاتصالات URLLC وأدائها في شبكة خاصة IMT-2020. ويمكن تنفيذ وظيفة عميل مراقبة الشبكة في البرمجيات ويمكن الإشارة إليها أيضاً باسم كيان الكشف عن النقطة الطرفية والتصدي لها (EDR) أو محرك صغير (ME). وقد يكون المخدم NMCF موجوداً داخل شبكة خاصة IMT-2020 أو حوسبة حافة أو ميدان شبكة عامة (الإنترنت). وتُوصّل معدات المستعمل لا سلكياً

بالعقدة gNB. وترسل كل معدَّة مستعمل رزماً إلى العقدة gNB أو تتلقى رزماً منها. وتُوصّل العقدة gNB بشبكة خاصة IMT-2020 أو بشبكة محلية عبر السطحين البينيين N3 وN4. وتتدفق الرزم عبر هذين السطحين البينيين.

وإذا خُصص عنوان IP للوظيفة NMSF، تتواصل الوظيفتان NMCF وNMSF مع بعضهما البعض عبر السطحين البينيين N3 وN4 لتبادل الإشارات الأمنية بينهما مثل نتيجة المراقبة عند NMCF.

وفي حالة السيناريو A، يمكن دمج وظيفة NMSF إضافية في مستوي البيانات MEC DP أيضاً، وإن لم يُبيّن ذلك في الشكل 3، بحيث يمكن لوظيفتين NMSF مراقبة حركة الشبكة الخاصة وحركة الشبكة العامة على السواء من أو إلى معدات المستعمل. ويمكن أيضاً تشكيل وظيفة NMSF ككيان مستقل بمعزل عن حوسبة الحافة متعددة النفاذ.

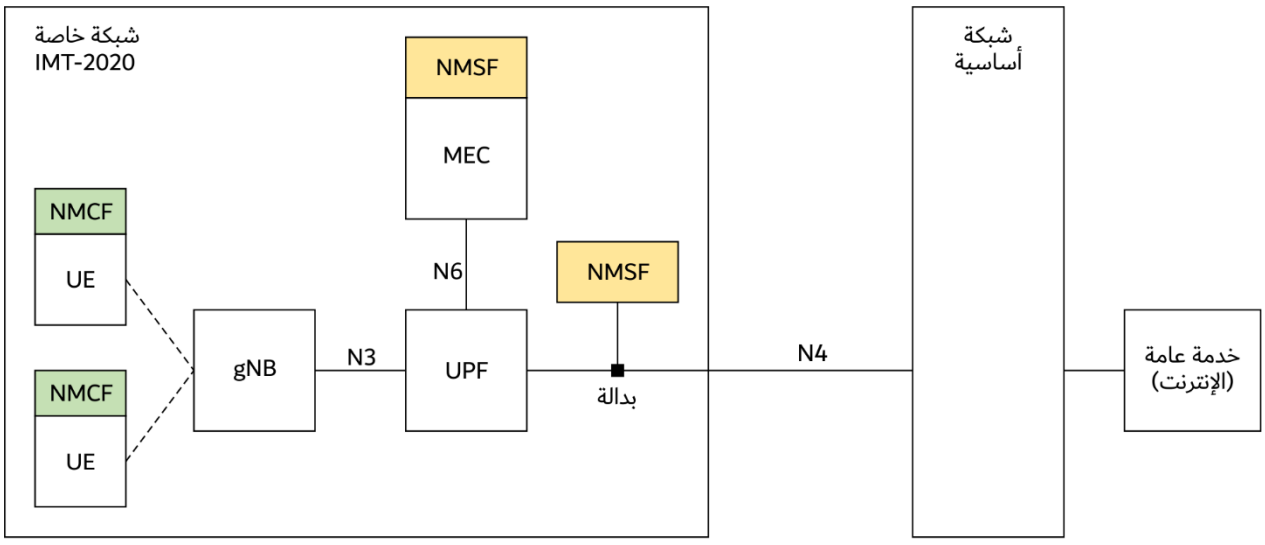
ويصف الشكل 4 سيناريو النشر B في معمارية أمنية لشبكة خاصة IMT-2020 حيث تُشكّل العديد من وظائف NMCF وNMSF.



الشكل 4 – سيناريو النشر B

بالإشارة إلى الشكل 4، تُنفذ الوظيفة NMSF كعقدة منفصلة خارج وظيفة مستوي المستعمل لمراقبة الرزم التي تولدها وظيفة مستوي المستعمل. ويمكن استخدام بدالة لاستنساخ الرزم من وظيفة مستوي المستعمل. وفي حال تخصيص عنوان IP للوظيفة NMSF، تتواصل الوظيفتان NMCF وNMSF مع بعضهما البعض عبر السطحين البينيين N3 وN4 لتبادل الإشارات الأمنية بينهما مثل نتيجة المراقبة المتولدة عند معدات المستعمل (عقدة العميل). وإذا كانت الشبكة الخاصة IMT-2020 تستخدم وظيفة تجفير من عقدة إلى عقدة مثل أمن بروتوكول الإنترنت (IPSec)، يمكن تشكيل وظائف NMSF عند نقطة تكون فيها الرزم التي أزيل تجفيرها خرجاً من العقدة.

ويصف الشكل 5 سيناريو النشر C في معمارية أمنية لشبكة خاصة IMT-2020 حيث تُشكّل العديد من وظائف مراقبة الشبكة (NMF).



الشكل 5 – سيناريو النشر C

وبالإشارة إلى الشكل 5، لا تُدمج الوظيفة NMSF في حوسبة الحافة متعددة النفاذ فحسب، بل تُنفّذ أيضاً كعقدة منفصلة خارج وظيفة مستوي المستعمل لمراقبة الرزم التي تولدها وظيفة مستوي المستعمل. وفي حال تخصيص عنوان IP للوظائف NMSF على التوالي، تتواصل الوظيفتان NMCF وNMSF مع بعضهما البعض عبر السطحين البينيين N3 وN4 لتبادل الإشارات الأمنية بينهما مثل نتيجة المراقبة المتولدة عند معدات المستعمل (عقدة العميل). وإذا كانت الشبكة الخاصة IMT-2020 تستخدم وظيفة تجفير من عقدة إلى عقدة مثل أمن بروتوكول الإنترنت (IPSec)، يمكن تشكيل وظائف NMSF عند نقطة تكون فيها الرزم التي أزيل تجفيرها خرجاً من العقدة.

والسيناريوهات الثلاثة المذكورة أعلاه لا يستبعد أي منها الآخر، ويعتمد أي أسلوب يتم استخدامه على التكلفة أو خصائص الشبكة، وغير ذلك. ويمكن أيضاً القيام بعمليات نشر مختلفة للوظيفتين NMCF وNMSF. فعلى سبيل المثال، يمكن دمج وظائف NMSF في أي من عقد الشبكة جنباً إلى جنب مع وظيفة مستوي المستعمل و/أو حوسبة الحافة متعددة النفاذ.

ولذلك، من منظور المعمارية الوظيفية للشبكة، يمكن إجراء مراقبة الأمن والأداء باستخدام وظيفة NMSF المثبتة على حوسبة الحافة متعددة النفاذ و/أو وظيفة مستوي المستعمل ووظيفة NMCF المثبتة على أجهزة إنترنت الأشياء وبروتوكول التشوير بين الوظيفتين NMCF وNMSF.

10 المتطلبات الأمنية والمراقبة من أجل تشغيل الخدمات الرأسية التي تدعم الاتصالات URLLC في الشبكات الخاصة IMT-2020

تحدد هذه الفقرة المتطلبات الأمنية والمراقبة من أجل تشغيل الخدمات الرأسية التي تدعم الاتصالات URLLC في شبكة خاصة IMT-2020. وتتطلب شبكة خاصة IMT-2020 مستوى أعلى من الأمن والأداء مقارنة بشبكات تقليدية بسبب الكميات الكبيرة من البيانات التي يتم تبادلها بين العديد من أجهزة العملاء/أجهزة الاستشعار والمخدمات المركزية التي تتحكم فيها. وبالإضافة إلى ذلك، يجب أيضاً متطلبات الاتصالات URLLC IMT-2020 في منطقة الحافة أيضاً وفقاً للتوصية [ITU-T Y.3102].

فيما يتعلق بسيناريوهات نشر شبكة خاصة IMT-2020 باستخدام وظائف NMSF وNMCF، تشمل المتطلبات الأمنية والمراقبة للخدمات الرأسية التي تدعم الاتصالات URLLC ما يلي:

أ) يلزم رصد وكشف السلوك غير الطبيعي لمعدات المستعمل وشبكة خاصة IMT-2020 للتخفيف من المخاطر الأمنية.

ب) يلزم مراقبة أداء الخدمات الرأسية التي تدعم الاتصالات URLLC.

ج) يلزم تنبيه مدير الشبكة إلى السلوك غير الطبيعي لمعدات المستعمل والشبكات الخاصة IMT-2020 بحيث يمكن حل المشاكل واستعادة قدرات الاتصالات URLLC في الوقت المناسب.

ويوصى اختيارياً بتصور السلوك غير الطبيعي لمعدات المستعمل والشبكات الخاصة IMT-2020 بحيث يُعالج هذا السلوك على نحو أكثر فعالية. ويرد في الملحق C وصف لتصور نتائج الرصد.

1.10 أمن وظيفة مخدم مراقبة الشبكة (NMSF)

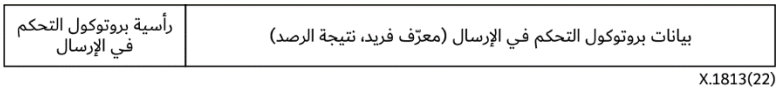
يشمل أمن وظيفة NMSF ما يلي:

أ) يشترط أن توفر الوظيفة NMSF على الأقل وظيفة استنساخ الرزم المرسلة والمستلمة بين عقدة العميل وعقدة المخدم، وبالتالي الحصول على رزمة مستنسخة واحدة على الأقل. وعقدة العميل هي معدات مستعمل أو جهاز إنترنت الأشياء. واستنساخ الرزم هو تقنية تتمثل في جمع وتحليل الرزم المتبادلة في عقدة محددة في الوقت الفعلي. ويمكن أن يكون للوظيفة NMSF وظيفة تبديل من أجل استنساخ الرزم.

ب) يشترط أن تحدد الوظيفة NMSF السلوك غير الطبيعي أو المشاكل الأمنية التي تهدد أمن وأداء شبكة خاصة IMT-2020 استناداً إلى المعلومات الواردة في الرزم المستنسخة.

ج) إذا خُصص عنوان IP لوظيفة NMSF، يجب أن تستلم الوظيفة NMSF من الوظيفة NMCF رزمة التحقق من الأمن باستخدام نسق رزمة بروتوكول التحكم في الإرسال (TCP) وأن تحسب مدة الذهاب والإياب (RTT) استناداً إلى رزمة التحقق من الأمن المستلَمة.

ويعرض الشكل 6 رزمة التحقق من الأمن باستخدام نسق رزمة بروتوكول التحكم في الإرسال (TCP).



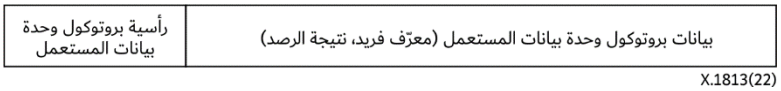
الشكل 6 – رزمة التحقق من الأمن باستخدام نسق رزمة بروتوكول التحكم في الإرسال

الجدول 1 – مجالات رزمة التحقق من الأمن

المجال	طول البايتة	الوصف
معرّف المستعمل (UID)	4	يشير هذا المجال إلى هوية مستعمل معدات المستعمل
الطول	2	يشير هذا المجال إلى طول البايتة لمجال نتيجة الرصد
نتيجة الرصد	متغيرة	يشير هذا المجال إلى المعلومات الحية، واستعمال وحدة المعالجة المركزية واستعمال ذاكرة معدات المستعمل

د) إذا لم يُخصص عنوان IP للوظيفة NMSF، فيجب أن تستنسخ هذه الوظيفة رزمة التحقق من الأمن باستخدام نسق رزمة بروتوكول وحدة بيانات المستعمل (UDP) المرسل من وظيفة NMCF إلى عقدة المخدم وأن تحسب مدة الذهاب والإياب (RTT) استناداً إلى رزمة التحقق من الأمن المستنسخة.

ويعرض الشكل 7 رزمة فحص الأمان التي تستخدم تنسيق رزمة بروتوكول وحدة بيانات المستعمل (UDP).



الشكل 7 – رزمة التحقق من الأمن باستخدام نسق رزمة بروتوكول وحدة بيانات المستعمل

الجدول 2 – مجالات رزمة التحقق من الأمن

المجال	طول البايتة	الوصف
معرّف المستعمل (UID)	4	يشير هذا المجال إلى هوية مستعمل معدات المستعمل
الطول	2	يشير هذا المجال إلى طول البايتة لمجال نتيجة الرصد
نتيجة الرصد	متغيرة	يشير هذا المجال إلى المعلومات الحية، واستعمال وحدة المعالجة المركزية واستعمال ذاكرة معدات المستعمل

هـ) يوصى بأن توفر وظيفة NMSF التنبيه إلى السلوك غير الطبيعي الذي يعيق متطلبات الاتصالات URLLC استناداً إلى حالة الأمن والأداء. وعند الكشف عن سلوك غير طبيعي يهدد الأمن والأداء، تنبه وظيفة NMSF المستعمل بحيث يتمكن من الاستجابة بشكل صحيح للسلوك غير الطبيعي. ثم ترسل وظيفة NMSF معلومات تنبيهية إلى وحدة تحكم أمنية تكلف وحدة التحكم الأمنية باتخاذ التدابير المناسبة للسلوك غير الطبيعي، أي إغلاق الشبكة. وتُرسل المعلومات التنبيهية عبر السطحين البينيين N3 وN4 اللذين يوفرهما بروتوكول التشوير 3GPP.

يمكن تنفيذ الميزات التفصيلية للأداء/المراقبة الأمنية القائمة على الاستنساخ لوظيفة NMSF بواسطة الخوارزمية المعيارية الواردة في الملحق A.

2.10 أمن وظيفة عميل مراقبة الشبكة (NMCF)

يشمل أمن وظيفة NMCF ما يلي:

أ) يشترط أن تعمل وظيفة NMCF على موارد الحوسبة لعقد العميل الفردية أو أجهزة استشعار إنترنت الأشياء ويوصى باستخدام الحد الأدنى من الموارد بحيث تعمل الوظائف بطريقة مناسبة.

ب) يشترط أن تقوم وظيفة NMCF بجمع الرزم أو المعلومات الداخلية التي ترسلها أو تستقبلها عقد العميل عبر الشبكة

ج) يشترط أن تقوم وظيفة NMCF برصد وتحديد تهديد أمن الشبكة المرتبط بعقدة العميل بما في ذلك وظيفة NMCF نفسها استناداً إلى الرزم المجمعة أو المعلومات الداخلية. وإذا كانت القيمة المبينة بالمعلومات الداخلية تساوي أو تزيد عن عتبة، تقرر وظيفة NMCF أن هناك تهديداً لأمن الشبكة. وتتضمن أمثلة المعلومات الداخلية استعمال وحدة المعالجة المركزية لعقدة العميل واستعمال ذاكرة عقدة العميل وما إلى ذلك.

د) إذا خُصص عنوان IP لوظيفة NMSF، يتعين على وظيفة NMCF توليد رزمة التحقق من الأمن باستخدام نسق رزمة بروتوكول التحكم في الإرسال (TCP) بما في ذلك نتيجة الرصد المبينة في الشكل 6 وإرسال رزمة التحقق من الأمن إلى وظيفة NMSF.

هـ) إذا لم يُخصص عنوان IP لوظيفة NMSF، يتعين على وظيفة NMCF توليد رزمة التحقق من الأمن باستخدام نسق رزمة بروتوكول وحدة بيانات المستعمل (UDP) بما في ذلك نتيجة الرصد المبينة في الشكل 7 وإرسال رزمة التحقق من الأمن إلى عقدة العميل بحيث يمكن لوظيفة NMSF استنساخ رزمة التحقق من الأمن.

و) يوصى بعرض وظيفة NMCF لتنبيه بأي تشغيل غير عادي لمعدات المستعمل إلى مستعمل أجهزة إنترنت الأشياء.

في حالة وظيفة NMCF، من الأرجح جمع بيانات أكثر دقة، وقد تتوقف وظيفة NMCF أيضاً عن العمل عند حدوث مشكلة، حيث يتم مثلاً إيقاف قدرة التجهيزات في التشغيل العادي. ولذلك، فإن مراقبة الأداء والأمن بواسطة وظيفة NMCF أمر ضروري.

ومع ذلك، فإن مراقبة كل تدفق بيانات للعديد من معدات المستعمل الموصولة بالشبكة الخاصة IMT-2020 قد يشكل عبئاً كبيراً على وظيفة NMSF، وفي هذه الحالة، يلزم التعاون مع وظيفة NMCF لرصد التهديدات التي تتعرض لها الشبكة على نحو فعال.

ويمكن تنفيذ الميزات التفصيلية التي تنفذ متطلبات وظيفة NMSF بواسطة الخوارزمية المعيارية الواردة في الملحق B.

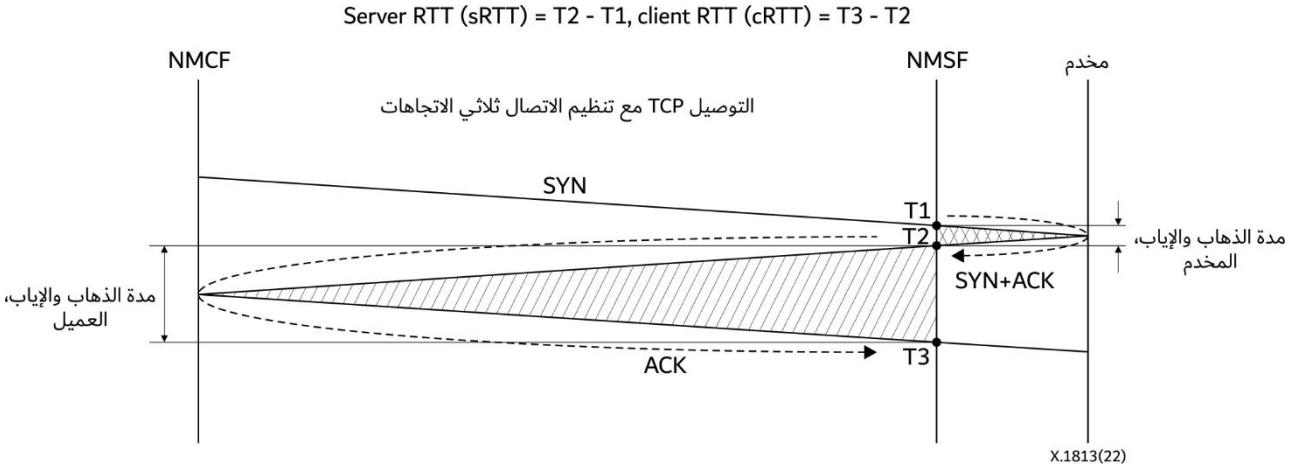
الملحق A

خصائص وظيفة مخدم مراقبة الشبكة (NMSF)

(يشكل هذا الملحق جزءاً أساسياً من هذه التوصية.)

وفقاً لهذه التوصية، تحدد وظيفة مخدم مراقبة الشبكة (NMSF) حدوث السلوك غير الطبيعي الذي يهدد الأمن والأداء استناداً إلى الرزم المستنسخة أو المعلومات المتعلقة بالرزم المستنسخة. وتحدد وظيفة NMSF السلوك غير الطبيعي من خلال حساب المؤشرات أو المعلمات ذات الصلة بأداء أو أمن الشبكة الخاصة IMT-2020 ومقارنة النتائج المحسوبة بالقيم المرجعية وفقاً لمتطلبات خدمة الاتصالات (IMT-2020 أو LTE). وبهذا الصدد، يمكن معرفة متطلبات خدمة الاتصالات من معلومات النفاذ لجهاز إنترنت الأشياء.

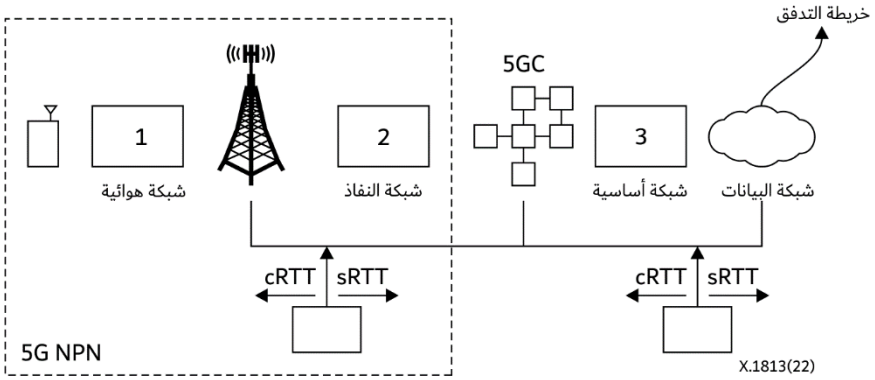
ويبين الشكل 1.A طريقة لقياس مدة الذهاب والإياب (RTT) باستخدام رزمة مستنسخة كمؤشر يتعلق بأداء أو أمن الشبكة الخاصة IMT-2020 وتحديد السلوك غير الطبيعي الذي يهدد أداء أو أمن الشبكة الخاصة IMT-2020 استناداً إلى مدة الذهاب والإياب.



الشكل 1.A – قياس مدة الذهاب والإياب

وبالإشارة إلى الشكل 1.A، في سيناريو الاتصال ثلاثي الاتجاهات (3-way handshake) فيما يتعلق بإرسال واستقبال إشارة المزامنة (SYN)، تقوم الوظيفة NMSF بحساب مدة الذهاب والإياب للشبكة باستخدام الرزم المستنسخة بين مستعمل ومخدم عبر الشبكة. فعلى سبيل المثال، بعد استخراج وتخزين النقاط الزمنية لإرسال واستقبال ثلاث رزم (SYN وSYN + ACK وACK) يتم تبادلها بين NMCF (أي عميل) ومخدم NMSF (أو حوسبة الحافة متعددة النفاذ)، تؤمن وظيفة NMSF معلومة زمنية واحدة على الأقل بين T1 وT2 وT3. وتحسب وظيفة NMSF مدة الذهاب والإياب (sRTT) الناجمة عن مخدم NMCF بطرح القيمة T1 من T2 (T2 – T1)، وتحسب مدة الذهاب والإياب (cRTT) الناجمة عن العميل من خلال T3 – T2، وتحسب مجموع مدة الذهاب والإياب للشبكة من خلال sRTT + cRTT أو T3 – T1. وتحسب وظيفة NMSF مدة الذهاب والإياب للشبكة بأكملها من خلال إجراء حساب لكل معاملة.

تحلل وظيفة NMSF وجود تهديدات لأداء أو أمن الشبكة الخاصة IMT-2020 بتحديد ما إذا كانت sRTT وcRTT ومدة الذهاب والإياب للشبكة تفي بمتطلبات الشبكة الخاصة IMT-2020. ويبين الشكل 2.A كيفية تحديد مناطق تدهور الأداء باستخدام sRTT وcRTT في الشبكة الخاصة IMT-2020.



الشكل 2.A – تحديد مناطق تدهور الأداء في شبكة خاصة IMT-2020

بالإضافة إلى مدة الذهاب والإياب، يمكن استخدام مؤشرات أخرى مختلفة كمؤشر لتحديد الأداء أو التهديد الأمني. وتشمل الأمثلة النموذجية للمؤشر معلومات وقت انتظار الاستجابة التي تمثل وقت الانتظار حتى تلقي مخدم NMSF (أو MEC) للبيانات الأولى المرتبطة بالمحتوى من عنوان URL المرتبط بطلب العميل للمحتوى؛ ومعلومات رقم دورة الانتظار التي تمثل عدد الدورات في حالة لا تتلقى استجابة لطلب مرسل من العميل؛ وBPS أو CPS أو TPS أو HTTP 40x أو 50x؛ ومعلومات بشأن إرسال واستقبال البيانات يتم الحصول عليها من رزمة مستنسخة؛ ومعلومات إحصائية يتم الحصول عليها من تعدد الرزم المستنسخة؛ ومعلومات حية تمثل إمكانية التوصيل بجهاز إنترنت الأشياء أو بمخدم NMCF.

باستخدام هذه المؤشرات، يمكن تنفيذ خوارزمية لتحديد الأداء والتهديدات الأمنية بأساليب مختلفة. فعلى سبيل المثال، تحدد الوظيفة NMSF وجود تهديد لأمن الشبكة استناداً إلى معلومات الحركة (طبقة OSI 3 أو OSI 4) بما في ذلك المعلومات المتعلقة بتدفق الرزمة ومعلومات البروتوكول (طبقة OSI 7).

وبالإضافة إلى ما سبق، يمكن اعتماد تقنيات متنوعة، منها كشف التهديدات الأمنية استناداً إلى معلومات الرزم اللازمة لكشف تهديد أمن الشبكة (على سبيل المثال، عندما يتجاوز عدد التوصيلات عبر قسم من عنوان IP لمصدر محدد مسبقاً إلى مقصد IP أو مخدّم BPS أو طلب الحصول على عنوان URL، قيمة عتبة محددة مسبقاً، يُحدد على أنه تهديد أمني)، وكشف التهديدات الأمنية استناداً إلى معلومات الحركة (على سبيل المثال، استخدام تقنية تجميعية تستند إلى رسم بياني لتوزيع الحركة من أجل تحديد أن الحركة التي تتجاوز قيمة عتبة محددة مسبقاً قد حدثت، ثم يتم تحديد حدوث مشكلة أمنية في شبكة خاصة IMT-2020)، والكشف القائم على معلومات البروتوكول، والكشف القائم على الشذوذ أو الكشف القائم على التوقيع أو على سوء الاستعمال، وكشف تحليل البروتوكول الذي يحافظ على الحالة، والكشف القائم على المواصفات. ويمكن أيضاً تضمين محتوى الاتصالات بين مخدّمي NMCF وNMCF في محتوى تحليل الوظيفة NMSF.

الملحق B

خصائص وظيفة عميل مراقبة الشبكة (NMCF)

(يشكل هذا الملحق جزءاً أساسياً من هذه التوصية.)

لتكامل مخدم NMCF وNMSF لا بد من بروتوكول لتبادل المعلومات المتعلقة بالأمن بين NMCF (أو مخدم NMCF) وNMSF.

أولاً، يحدد NMCF ما إذا كان هناك تهديد لأمن الشبكة باستخدام حالات أجهزة إنترنت الأشياء اللازمة لخدمته الخاصة أو معلومات السجل ومدة الذهاب والإياب. وتتضمن حالة جهاز إنترنت الأشياء اللازمة للخدمة حمولة وحدة المعالجة المركزية، واستخدام الذاكرة، واستخدام التخزين، والمعلومات الحية. فعلى سبيل المثال، عندما يكون استخدام الذاكرة مساوياً لقيمة عتبة مسبقة التشكيل أو أكبر منها أو عندما تكون مدة الإياب والذهاب أكبر من قيمة عتبة مسبقة التشكيل، يحدد NMCF حدوث سلوك غير طبيعي يهدد الأمن والأداء. ومن الأمثلة الأخرى على ذلك، الحالة التي تشير فيها معلومات السجل إلى أن كياناً له عنوان IP محظور قد حاول تسجيل الدخول إلى عقدة عميل، أو أن عملية غير معروفة قد حدثت، عندئذ، يحدد NMCF أن سلوكاً غير طبيعي يهدد الأمن والأداء قد حدث.

ثم يقوم NMCF بإرسال قيمة نتيجة المراقبة المحددة بشأن ما إذا كان هناك تهديد أمني أم لا إلى مخدّم NMCF أو NMSF. وبمعنى آخر، يتلقى NMSF قيمة مراقبة بشأن تهديد أمن الشبكة كما تدركه نقطة طرفية في الوقت الفعلي. وفي هذا الوقت، ينبغي تحديد جهاز إنترنت الأشياء باستعمال المعلومات التي يجمعها المخدم NMCF بخصوص NMCF ومحتوى تحليل NMSF بحيث يمكن تمييز المحتوى المتولد من نفس جهاز إنترنت الأشياء عن المحتويات الأخرى.

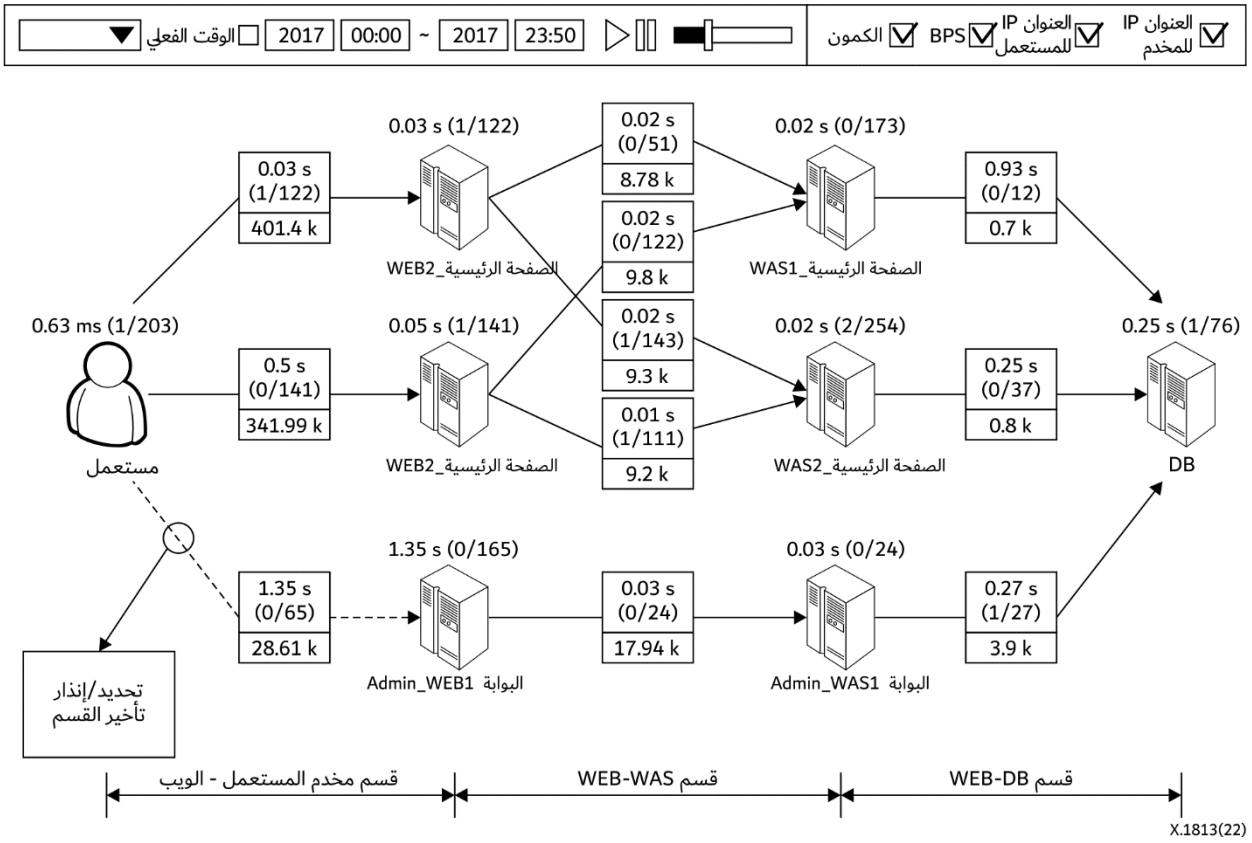
ويمكن للطريقة الموصوفة أعلاه أن تقلل من العبء على المخدم NMSF المركزي من خلال إجراء مراقبة التهديدات في النقاط الطرفية مثل NMCF ونتيجةً لذلك، يمكن أن تحسّن أداء المراقبة مقابل أداء الشبكة والتهديدات الأمنية.

الملحق C

عرض نتائج المراقبة

(يشكل هذا الملحق جزءاً أساسياً من هذه التوصية.)

يوضح الشكل 1.C مثالاً على عرض أداء الشبكة/النظام ومراقبة الأمن باستخدام NMSF.



الشكل 1.C – مثال على عرض أداء الشبكة/النظام ومراقبة الأمن

إشارة إلى الشكل 1.C، تُعرض النتائج المحللة استناداً إلى مؤشرات الأداء أو مؤشرات الأمن في الوقت الفعلي ثم تقدم إلى المستعملين كإنذار. ويستطيع مديرو الشبكات التعامل مع التهديدات على الفور باستخدام هذه النتائج. أي أن النتائج المحللة تُفسر من حيث الأداء والمنظور الأمني. وبمجرد اكتشاف السلوك غير الطبيعي تنتقل علامة التحذير إلى مديري الشبكة.

ومن المرغوب فيه أن يعبّر العرض بشكل بديهي وواضح عن الروابط بين الكيانات في الشبكة. ويُنفذ العرض بحيث يولّد NMSF مؤشراً يتعلق بالأداء والأمن ككائن، وينفذ الكائن المولَّد في حيز مرئي، ويضع خريطة تدفق تمثل تدفق الحركة في الشبكة. ولهذا الغرض، يجب الحصول على الكائنات عن طريق إنشاء مؤشرات تتعلق بالأداء/الأمن بالاشتراك مع كيان أول، وتوليد مؤشرات تتعلق بالأداء/الأمن بالاشتراك مع كيان ثان، وتوليد مؤشرات تتعلق بالأداء/الأمن بالاقتران مع وصلة تربط بين الكيان الأول والكيان الثاني.

لتحسين الوضوح، يُمثَّل خط بين الكيان الأول والكيان الثاني على خريطة التدفق استناداً إلى تجسيد المؤشرات المتعلقة بالأداء/الأمن المرتبطة بالوصلات. ويمكن إضافة عناصر اللون للتمييز. وبعبارة أخرى، يمكن عرض تصور واحد على الأقل ضمن الألوان والأشكال والسُّمك بشكل مميز وفقاً لمؤشرات الأداء/الأمن المرتبطة بالوصلات.

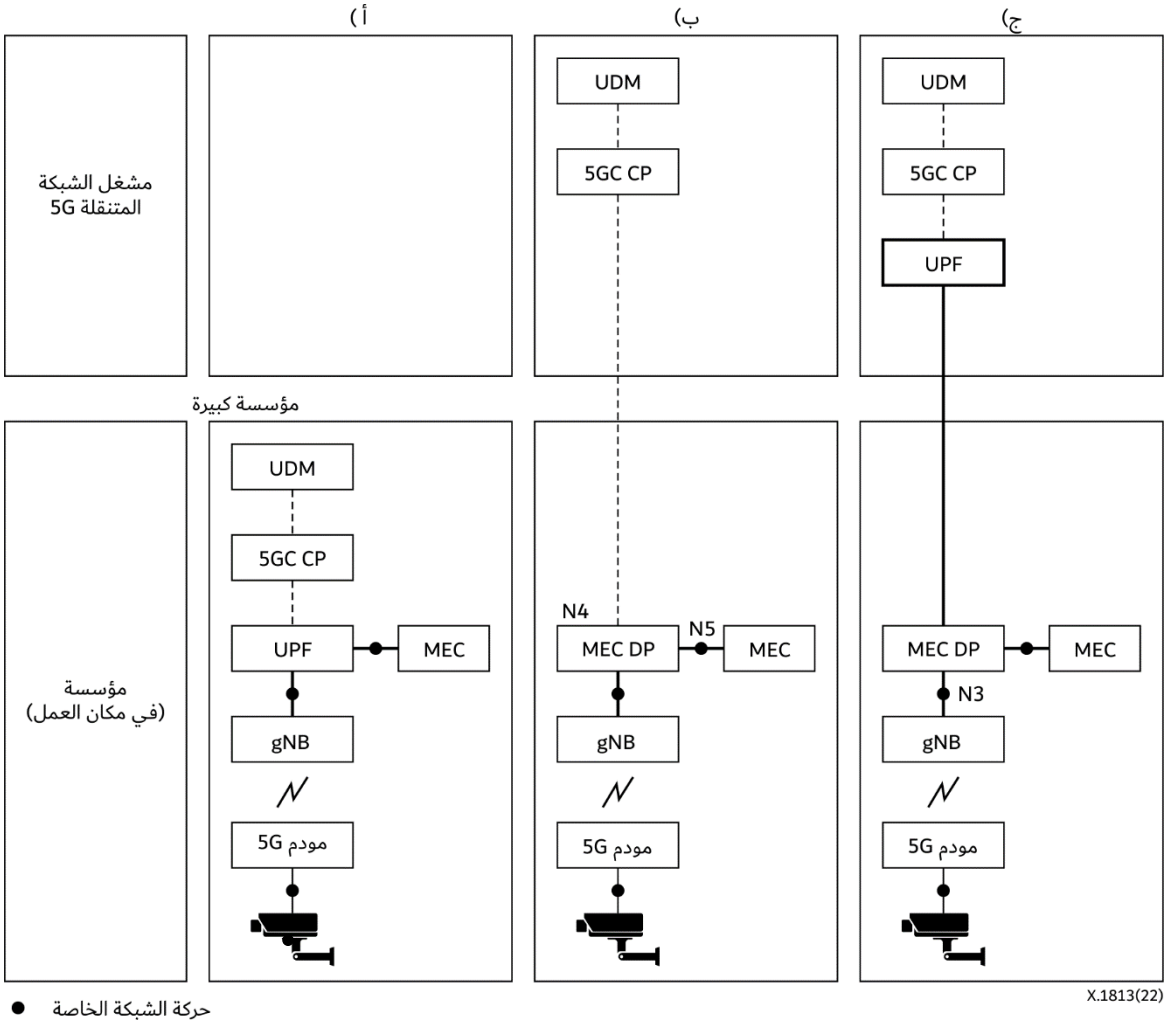
ومن خلال استخدام وظيفة العرض هذه، يمكن تحقيق الرؤية والوضوح في جميع أقسام الخدمة. ولا يقتصر الأمر على تحسين الوقاية من مشاكل خدمة الشبكة من خلال إدارتها، بل يمنح الشبكة القدرة على التعامل بسهولة مع التهديدات في بنية تحتية واسعة لإنترنت الأشياء مثل المصانع الذكية والمدن الذكية.

التذييل I

حالات استعمال شبكة خاصة IMT-2020 في الخدمات الرأسية

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

تستند هذه التوصية إلى ثلاثة أنواع من معمارية الشبكة الخاصة IMT-2020 على النحو المبين في الشكل 1.I.



الشكل 1.I – ثلاثة أنواع من نشر شبكة خاصة IMT-2020

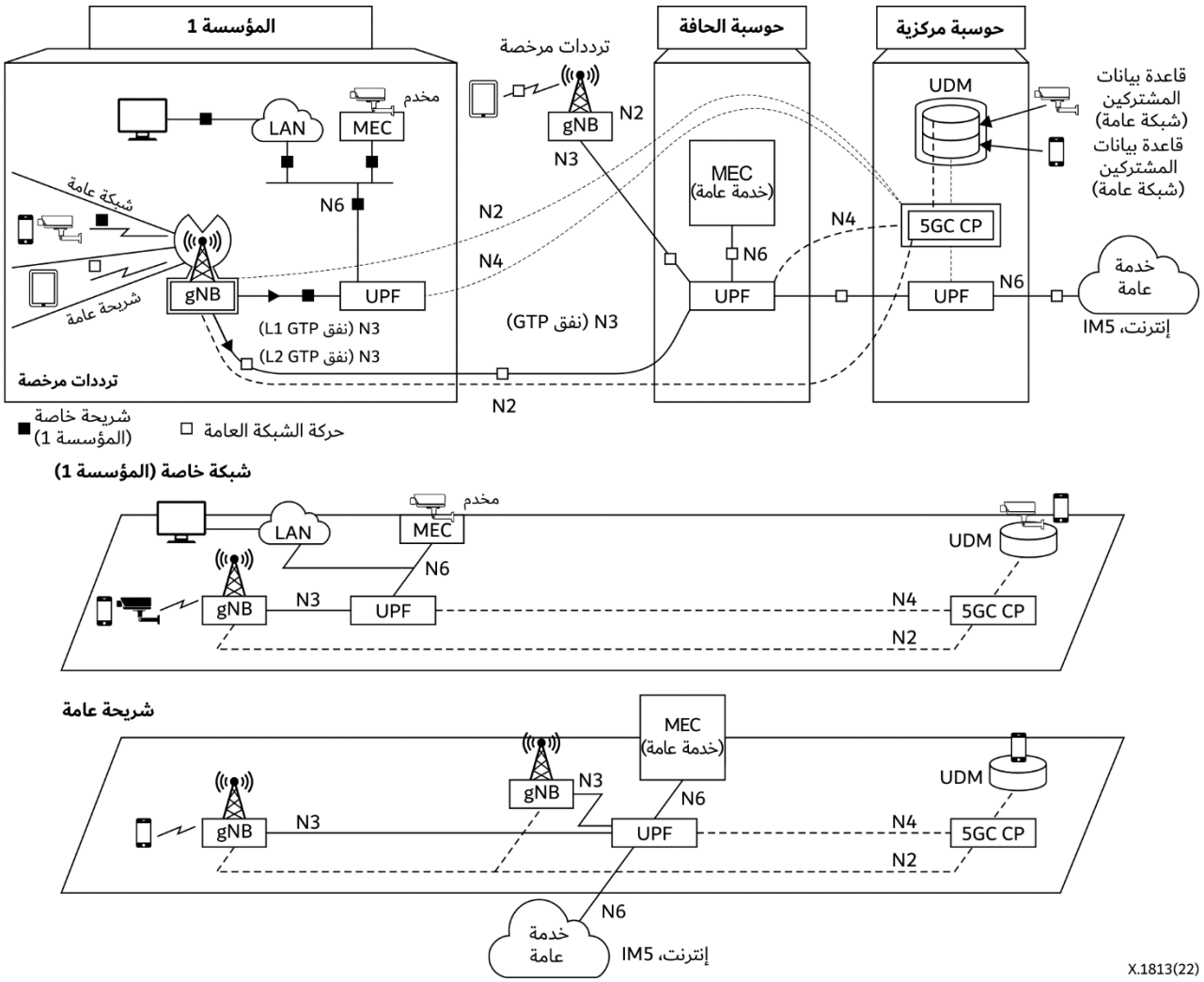
وفقاً للمعيار [b-Harrison]، يمكن نشر الشبكات الخاصة IMT-2020 كشبكات معزولة تماماً (أ) أو شبكات مستقلة أو يمكن نشرها كشريحة PLMN بالاقتران مع شبكة عامة (ب أو ج) كما هو مبين في الشكل 1.I.

فيما يخص (أ) تكون الشبكة الخاصة منفصلة مادياً عن الشبكة العامة، مما يوفر الأمن الكامل للبيانات. ونظراً إلى أن تأخر الشبكة بين الجهاز ومخدم التطبيق يقع في حدود بضع أجزاء من الألف من الثانية (ms)، يمكن تنفيذ خدمات التطبيقات URLLC.

وفيما يخص (ب) يتم نشر gNB وUPF وMIC داخل المؤسسة. وفي هذه المعمارية، يجري تقاسم الشبكة RAN ومستوي التحكم بين الشبكات الخاصة والعامة، ويمكن تعزيز الأمن وتقليل التأخير

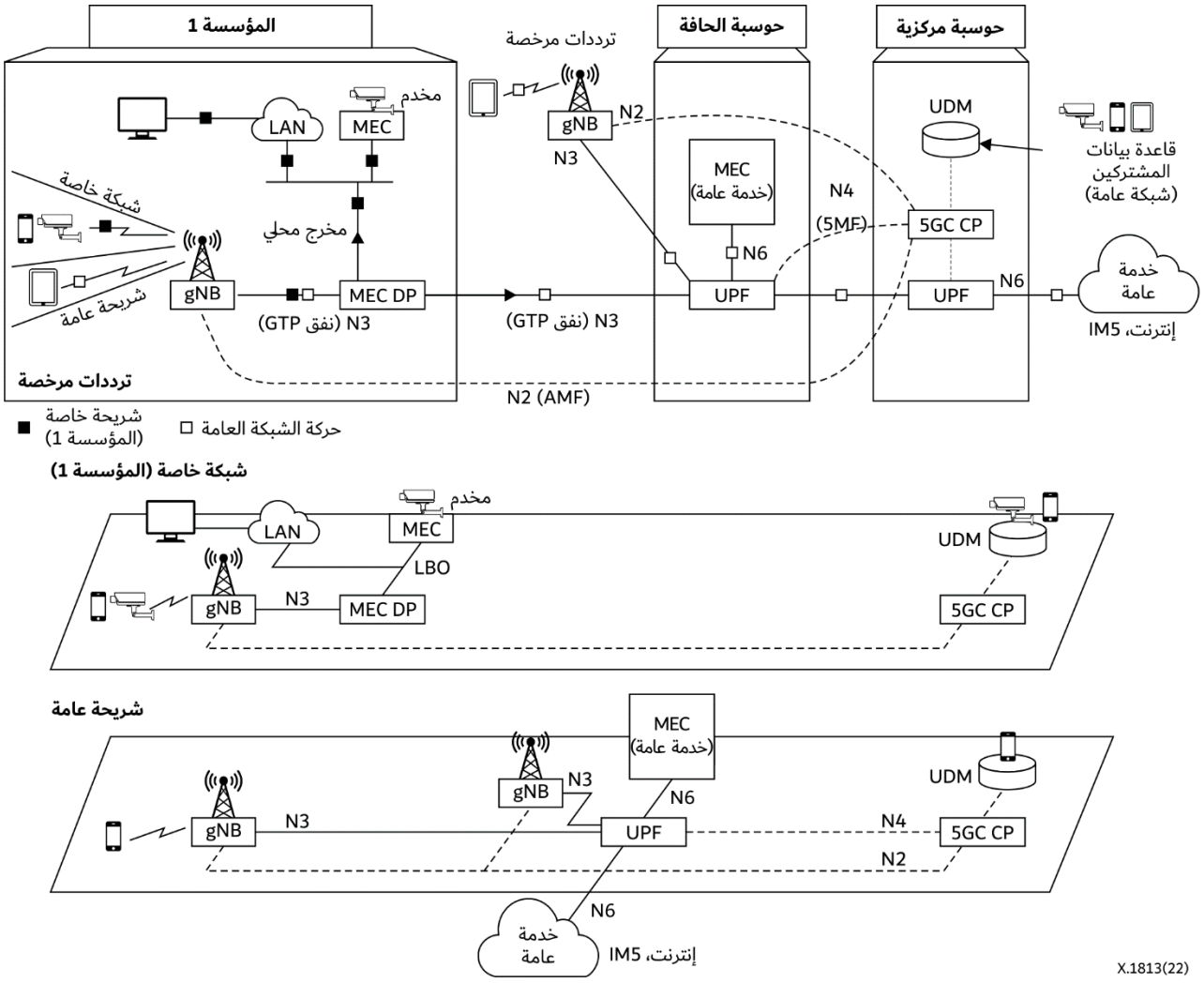
أما فيما يخص (ج) يتم نشر العقدة gNB ومستوي البيانات MEC (DP) وMEC داخل المؤسسة، وتوضع وظيفة مستوي المشغل في سحابة حافة مشغل الاتصالات المتنقلة البعيد عن الأجهزة. وينظر مستوي البيانات MEC DP في عناوين IP للمقصد للرزم التي تنتمي إلى جميع أنفاق بروتوكول إنشاء أنفاق الخدمة GPRS (GTP) القادمة من العقدة gNB (GTP decap) ويوجه رزمة IP الخاصة بالمستعمل إلى الشبكة الخاصة الداخلية إذا كانت حركة محلية. وفي هذه المعمارية، يمكن تعزيز الأمن وتقليل التأخير.

ووفقاً للمرجع [b-Harrison]، يمكن وصف نوع النشر (ب) في الشكل 1.I على النحو المبين في الشكل 2.I من العرض الرأسي باستخدام تقسيم الشبكة. ويوضح الشكل 2.I معمارية وظيفية مفصلة لنوع النشر (ب) الوارد في الشكل 1.I، تتقاسمها شبكة خاصة IMT-2020 وشبكة عامة.



الشكل 2.I – معمارية وظيفية مفصلة لنوع النشر (ب) الوارد في الشكل 1.I

وفقاً للمرجع [b-Harrison]، يمكن وصف نوع النشر (ج) في الشكل 1.I على النحو المبين في الشكل 3.I من العرض الرأسي باستخدام تقسيم الشبكة. ويوضح الشكل 3.I معمارية وظيفية مفصلة لنوع النشر (ج) الوارد في الشكل 1.I، تتقاسمها شبكة خاصة IMT-2020 وشبكة عامة.



الشكل I.3 – معمارية وظيفية مفصلة لنوع النشر (ج) الوارد في الشكل I.1

جميع المعماريات الوظيفية للشبكة الخاصة IMT-2020 المذكورة أعلاه ينشرها مشغلو الشبكات لتعزيز أمن الاتصالات URLLC وتحسين أدائها. والحفاظ على أداء وأمن شبكة خاصة IMT-2020 هو أحد أهم العوامل بالنسبة للخدمات الرأسية التي تدعم الاتصالات URLLC. وتسمى إحدى المنهجيات المرشحة تفحص الرزم المتعمق (DPI) الموصوف أيضاً في [b-ITU-T Y.2774] و[b-ITU-T Y.2775]. غير أن مجال تطبيق هاتين التوصيتين يقتصر فقط على الشبكات المتنقلة العامة وبالتالي لا يمكن تطبيقه على الشبكات الخاصة IMT-2020، وبصورة أكثر تحديداً، على الخدمات الرأسية الداعمة للاتصالات URLLC.

بيبليوغرافيا

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2022