الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1364

(2020/03)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

التطبيقات والخدمات الآمنة (2) – أمن إنترنت الأشياء (IoT)

متطلبات الأمن وإطار من أجل إنترنت الأشياء ضيقة النطاق

التوصية ITU-T X.1364

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.1–X.199
التوصيل البيني للأنظمة المفتوحة	X.200–X.299
التشغيل البيني للشبكات	X.300–X.399
أنظمة معالجة الرسائل	X.400–X.499
الدليل	X.500–X.599
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.600–X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.700–X.799
الأمن	X.800–X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.850–X.899
المعالجة الموزعة المفتوحة	X.900–X.999
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1000–X.1029
أمن الشبكة	X.1030–X.1049
إدارة الأمن	X.1050–X.1069
الخصائص البيومترية	X.1080–X.1099
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1100–X.1109
أمن الشبكة المحلية	X.1110–X.1119
أمن الخدمات المتنقلة	X.1120–X.1139
أمن الويب	X.1140–X.1149
بروتوكولات الأمن (1)	X.1150–X.1159
الأمن بين جهتين نظيرتين	X.1160–X.1169
أمن معرفات الهوية عبر الشبكات	X.1170–X.1179
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1180–X.1199
أمن الفضاء السيبراني	
الأمن السيبراني	X.1200–X.1229
مكافحة الرسائل الاقتحامية	X.1230–X.1249
إدارة الهوية	X.1250–X.1279
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1300–X.1309
أمن شبكات المحاسيس واسعة الانتشار	X.1310–X.1319
أمن شبكة الكهرباء الذكية	X.1330–X.1339
البريد المعتمد	X.1340–X.1349
أمن إنترنت الأشياء (IoT)	**X.1360–X.1369**
أمن أنظمة النقل الذكية (ITS)	X.1370–X.1389
أمن سجل الحسابات الموزع	X.1400–X.1429
أمن سجل الحسابات الموزع	X.1430–X.1449
البروتوكول الأمني (2)	X.1450–X.1459
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1500–X.1519
تبادل مواطن الضعف/الحالة	X.1520–X.1539
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540–X.1549
تبادل السياسات	X.1550–X.1559
طلب المعلومات الحدسية والمعلومات الأخرى	X.1560–X.1569
تعرف الهوية والاكتشاف	X.1570–X.1579
التبادل المضمون	X.1580–X.1589
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1600–X.1601
تصميم أمن الحوسبة السحابية	X.1602–X.1639
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1640–X.1659
تنفيذ أمن الحوسبة السحابية	X.1660–X.1679
أمن أشكال أخرى للحوسبة السحابية	X.1680–X.1699
الاتصالات الكمومية	X.1700–X.1729

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

التوصية ITU-T X.1364

متطلبات الأمن وإطار من أجل إنترنت الأشياء ضيقة النطاق

ملخص

تحلل التوصية ITU-T X.1364 مخططات مخطط النشر المحتمل وسيناريوهات التطبيق النمطية لإنترنت الأشياء ضيقة النطاق (NB-IoT). وهي تحدد التهديدات الأمنية ومتطلبات الأمن ذات الصلة الخاصة بعمليات نشر إنترنت الأشياء ضيقة النطاق تحديداً، وبالتالي تضع إطاراً أمنياً للمشغلين لحماية تطبيقات هذه التكنولوجيا الجديدة.

نتيجةً للتطورات الحالية في تكنولوجيا الاتصالات في مجال الاتصالات المتنقلة، تغير نمط الاتصالات من النمط "شخص إلى شخص" إلى النمط "شخص إلى شيء" والنمط "شيء إلى شيء"، بحيث أصبح تطوير إنترنت الأشياء من الأمور التي لا مناص منها.

ومقارنةً بتكنولوجيات الاتصالات قصيرة المسافة مثل Bluetooth وZigBee، من جملة تكنولوجيات أخرى، فإن الشبكات المتنقلة الخلوية التي تتسم بالتغطية الواسعة والتنقلية والتوصيلات الكثيفة والتي يمكن أن تحقق سيناريوهات تطبيق أكثر ثراء، يفترض أن تصبح التكنولوجيا الرئيسية للتوصيل البيني لإنترنت الأشياء.

وتقوم إنترنت الأشياء ضيقة النطاق (NB-IoT) على شبكة متنقلة خلوية تستخدم عرض نطاق لا يتجاوز 180 kHz تقريباً. ويمكن نشرها على شبكة تابعة للنظام العالمي للاتصالات المتنقلة (GSM) أو شبكة تابعة لنظام الاتصالات المتنقلة العالمية (UMTS) أو شبكة من شبكات التطور طويل الأجل (LTE) مباشرةً سعياً إلى خفض التكلفة مع القدرة على التحديث السلس.

ونتيجةً لاستهلاكها المنخفض للطاقة وتغطيتها الواسعة وتكلفتها المنخفضة وسعتها العالية، يتوقع اعتماد إنترنت الأشياء ضيقة النطاق بكثافة من جانب المشغلين مع استخدامها على نطاق واسع في العديد من الصناعات الرأسية.

وباعتبارها تكنولوجيا جديدة، تتسم إنترنت الأشياء ضيقة النطاق بخصائص خاصة بها قد تجلب مشكلات أمنية جديدة. ومن أجل ضمان الأمن في عمليات نشر وتطبيقات إنترنت الأشياء ضيقة النطاق، يجب تحليل التهديدات الأمنية ومتطلبات الأمن ذات الصلة الخاصة بإنترنت الأشياء ضيقة النطاق تحديداً مع وضع إطار أمني شامل من أجل إنترنت الأشياء ضيقة النطاق.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1364	2020-03-26	17	11.1002/1000/14088

مصطلحات أساسية

إطار، إنترنت الأشياء، ضيقة النطاق، متطلبات الأمن.

* للنفاذ إلى توصية، 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 متخصصة للأمم المتحدة 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/.

© ITU 2020

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

جدول المحتويات

الصفحة

1 مجال التطبيق 1
2 المراجع 1
3 التعاريف 1
1.3 مصطلحات معرَّفة في وثائق أخرى 1
2.3 المصطلحات المعرفة في هذه التوصية 2
4 الاختصارات والأسماء المختصرة 3
5 الاصطلاحات 4
6 نظرة عامة لإنترنت الأشياء ضيقة النطاق 4
7 مخطط النشر وسيناريوهات التطبيق النمطية 5
1.7 مخطط النشر 5
2.7 التطبيقات النمطية 6
8 التهديدات التي تواجه إنترنت الأشياء ضيقة النطاق 7
1.8 خصائص إنترنت الأشياء ضيقة النطاق 7
2.8 طبقة إنترنت الأشياء ضيقة النطاق 8
9 متطلبات الأمن 9
1.9 متطلبات أمن الأجهزة المطرافية 9
2.9 متطلبات أمن الشبكات 10
3.9 متطلبات أمن التطبيقات 10
10 القدرات الأمنية لإنترنت الأشياء ضيقة النطاق 10
1.10 القدرات الأمنية للأجهزة المطرافية 10
2.10 القدرات الأمنية للشبكة 11
3.10 القدرات الأمنية للتطبيقات 11
4.10 العلاقة بين القدرات الأمنية ومتطلبات الأمن 11
بيبليوغرافيا 13

التوصية ITU-T X.1364

متطلبات الأمن وإطار من أجل إنترنت الأشياء ضيقة النطاق

1 مجال التطبيق

تحلل التوصية مخطط النشر المحتمل وسيناريوهات التطبيق النمطية لإنترنت الأشياء ضيقة النطاق (NB-IoT). وهي توصف التهديدات الأمنية ومتطلبات الأمن ذات الصلة الخاصة بعمليات نشر إنترنت الأشياء ضيقة النطاق تحديداً، وبالتالي تضع إطاراً أمنياً للمشغلين لحماية تطبيقات هذه التكنولوجيا الجديدة.

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.

[ETSI TS 123 401] ETSI TS 123 401 V15.8.0 (2019-10), *LTE; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (3GPP TS 23.401 version 15.8.0 Release 15)*.

[ETSI TS 123 501] ETSI TS 123 501 V15.6.0 (2019-10), *5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 15.6.0 Release 15)*.

3 التعاريف

1.3 مصطلحات معرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 استيقان (authentication) [b-ITU-T X.1141]: التحقّق من هوية المستعمل أو العملية أو الجهاز، غالباً كشرط أساسي للسماح بالنفاذ إلى الموارد في نظام المعلومات.

2.1.3 إمكانية (capability) [b-ITU-T X.1145]: قدرة يوفرها نظام أو معدة لتقديم خدمة.

3.1.3 إنترنت الأشياء الخلوية (cellular IoT) [ETSI TS 123 401]: شبكة خلوية تدعم أجهزة شبكة إنترنت الأشياء والتي تتسم بانخفاض التعقيد والصبيب. وتدعم إنترنت الأشياء الخلوية على السواء الحركة القائمة على بروتوكول الإنترنت وغير القائمة على بروتوكول الإنترنت.

4.1.3 سلامة البيانات (data integrity) [b-ITU-T X.800]: خاصية بقاء البيانات على حالتها دون أن يطرأ عليها تغيير أو تلف بطريقة غير مرخص بها.

5.1.3 التشفير (encryption) [b-ITU-T X.800]: التحويل المجفر للبيانات (انظر علم التجفير) لإنتاج نص مشفر.

ملاحظة – قد يكون التشفير غير قابل للعكس، وفي هذه الحالة لا يمكن إجراء عملية فك التشفير المقابلة.

6.1.3 كيان (entity) [b-ITU-T X.1252]: شيء له وجود قائم بذاته ومميز ويمكن تعريفه في سياق.

ملاحظة – يمكن أن يكون الكيان شخصاً طبيعياً أو حيواناً أو شخصاً اعتبارياً أو منظمة، أو شيئاً فاعلاً أو منفعلاً، أو تطبيقاً برمجياً، أو خدمة وما إلى ذلك، أو مجموعة مما تقدم. وفي سياق الاتصالات، تشمل أمثلة الكيانات نقاط نفاذ ومشتركين وعناصر شبكة وشبكات وتطبيقات برمجيات وخدمات وأجهزة وسطوح بينية، وما إلى ذلك.

7.1.3 الشبكة الأساسية المتطورة القائمة على الرزم (evolved packet core) [b-ITU-T Q.1743]: إطار لتطور أو انتقال نظام 3GPP إلى نظام يتسم بمعدل بيانات أعلى ومعدل كمون أقل بالاستخدام الأمثل للرزم يدعم عدة تكنولوجيات للنفاذ الراديوي (RAT).

8.1.3 نظام متطور قائم على الرزم (evolved packet system) [b-ITU-T Q.1743]: تطوير للجيل الثالث من النظام العالمي للاتصالات المتنقلة (3G UMTS) يتميز بنظام ذي معدل بيانات أعلى ومعدل كمون أقل بالاستخدام الأمثل للرزم يدعم عدة تكنولوجيات للنفاذ الراديوي. ويتألف النظام المتطور القائم على الرزم من شبكة أساسية متطورة قائمة على الرزم إلى جانب شبكة نفاذ راديوي متطورة (E-UTRA وE-UTRAN).

9.1.3 إدارة مفاتيح (key management) [b-ITU-T X.800]: توليد المفاتيح وتخزينها وتوزيعها وإلغاؤها وأرشفتها وتطبيقها طبقاً لسياسة الأمن.

10.1.3 إنترنت الأشياء ضيقة النطاق (narrowband-IoT) [ETSI TS 123 401]: تكنولوجيا للنفاذ الراديوي للمشروع 3GPP تشكل جزءاً من إنترنت الأشياء الخلوية. وهي تسمح بالنفاذ إلى خدمات الشبكة عبر شبكة نفاذ راديوي عالمي للأرض متطور (E-UTRAN) بعرض نطاق قناة لا يزيد عن 180 kHz (يقابل كتلة موارد مادية واحدة (PRB)). وما لم يذكر خلاف ذلك في أي فقرة، تعد إنترنت الأشياء ضيقة النطاق مجموعة فرعية من الشبكة E-UTRAN.

11.1.3 التهديد (threat) [b-ITU-T X.800]: خرق أمني محتمل.

2.3 المصطلحات المعرفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 عقدة بوابة خدمة إنترنت الأشياء الخلوية (CIoT serving gateway node) (C-SGN): عقدة بوابة خدمة إنترنت الأشياء الخلوية هي خيار تنفيذ شبكة أساسية متطورة قائمة على الرزم (EPC) ذات عقد مجمعة يقلل إلى أدنى حد من عدد الكيانات المادية بإسكان كيانات النظام المتطور القائم على الرزم (EPS) معاً في مسيرات مستويات التحكم والمستعملين (مثل كيان إدارة التنقلية (MME) وبوابة الخدمة (S-GW) وبوابة شبكة البيانات القائمة على الرزم (P-GW) والذي قد يكون خياراً منفصلاً في عمليات نشر إنترنت الأشياء الخلوية.

ملاحظة – تعود الوظائف المدرجة في هذا التعريف إلى المعيار [ETSI TS 123 401].

2.2.3 العقدة المتطورة B (evolved node B) (eNodeB): عقدة نفاذ لاسلكي تستضيف وظائف من أجل إجارة الموارد الراديوية وفك انضغاط بيانات الوصلة الصاعدة وتجفير تدفقات بيانات المستعملين وتسيير بيانات مستويات المستعملين وما إلى ذلك.

ملاحظة – تعود الوظائف المدرجة في هذا التعريف إلى المعيار [ETSI TS 123 401].

3.2.3 شبكة النفاذ الراديوي العالمي للأرض المتطور (E-UTRAN) (evolved universal terrestrial radio access network): شبكة نفاذ راديوية من بين وظائفها ضغط الرأسية وتشفير مستوى المستعمل واختيار كيان إدارة التنقلية وإنفاذ معدل مستوى الحمالة للوصلتين الصاعدة والهابطة والتحكم في دخول مستوى الحمالة والتحكم في الازدحام وما إلى ذلك.

ملاحظة – تعود الوظائف المدرجة في هذا التعريف إلى المعيار [ETSI TS 123 401].

4.2.3 مخدم المشترك المنزلي (home subscriber server) (HSS): أحد عناصر الشبكة الأساسية المتنقلة يقوم بوظائف تخزين معلومات الاشتراك الخاصة بالمستعمل وإدارتها.

ملاحظة – تعود الوظائف المدرجة في هذا التعريف إلى المعيار [ETSI TS 123 401].

5.2.3 كيان إدارة التنقلية (mobility management entity) (MME): أحد عناصر الشبكة الأساسية المتنقلة يقوم بوظائف إدارة قائمة مناطق التتبع وتقابل مواقع معدات المستعملين (UE) واختيار بوابة الخدمة (S-GW) وبوابة شبكة البيانات القائمة على الرزم (P-GW) واختيار التمرير والاستيقان والتحويل وإدارة الحمالة وما إلى ذلك.

ملاحظة – تعود الوظائف المدرجة في هذا التعريف إلى المعيار [ETSI TS 123 401].

6.2.3 بوابة شبكة البيانات القائمة على الرزم (packet data network gateway) (P-WG): عنصر من عناصر الشبكة الأساسية المتنقلة يقوم بوظائف ترشيح الرزم على أساس كل مستعمل وتوزيع عناوين بروتوكول الإنترنت (IP) لمعدات المستعملين (UE) ووسم رزم مستوى النقل وترسيم مستوى الخدمة وغيرها.

ملاحظة – تعود الوظائف المدرجة في هذا التعريف إلى المعيار [ETSI TS 123 401].

7.2.3 وظيفة عرض قدرات الخدمة (service capability exposure function) (SCEF): عنصر من عناصر الشبكة الأساسية المتنقلة يقوم بوظائف الاستيقان والتخويل واكتشاف قدرات الخدمة المعروضة وإدارة السياسات وتشكيل معلمات الشبكة وغيرها.

ملاحظة – تعود الوظائف المدرجة في هذا التعريف إلى المعيار [ETSI TS 123 401].

8.2.3 بوابة الخدمة (serving gateway) (S-WG): عنصر من عناصر الشبكة الأساسية المتنقلة يقوم بوظائف نقطة الارتكاز المحلية للتنقلية من جل التمرير بين العقد eNodeB وربط التنقلية من أجل التنقلية البينية للمشروع 3GPP وتسيير الرزم وإعادة التسيير ووسم رزم مستوى النقل والمحاسبة من أجل الترسيم بين المشغلين وما إلى ذلك.

ملاحظة – تعود الوظائف المدرجة في هذا التعريف إلى المعيار [ETSI TS 123 401].

4 الاختصارات والأسماء المختصرة

تستخدم هذه التوصية المختصرات التالية:

3G الجيل الثالث *(3rd Generation)*

3GPP مشروع شراكة الجيل الثالث *(3rd Generation Partnership Project)*

CDMA النفاذ المتعدد بتقسيم الشفرة *(Code Division Multiple Access)*

CIoT إنترنت الأشياء الخلوية *(Cellular Internet of Things)*

C-SGN عقدة بوابة خدمة إنترنت الأشياء الخلوية *(CIoT Serving Gateway Node)*

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

EPC شبكة أساسية متطورة قائمة على الرزم *(Evolved Packet Core)*

eNodeB العقدة المتطورة B *(Evolved Node B)*

EPS نظام متطور قائم على الرزم *(Evolved Packet System)*

E-UTRAN شبكة نفاذ راديوي عالمي للأرض متطور *(Evolved Universal Terrestrial Access Network)*

GSM النظام العالمي للاتصالات المتنقلة *(Global System for Mobile Communication)*

HSS مخدم المشترك المنزلي *(Home Subscriber Server)*

IMEI الهوية الدولية للمعدات المتنقلة *(International Mobile Equipment Identity)*

IP بروتوكول الإنترنت *(Internet Protocol)*

LTE التطور طويل الأجل *(Long Term Evolution)*

MME كيان إدارة التنقلية *(Mobility Management Entity)*

NB-IoT إنترنت الأشياء ضيقة النطاق *(Narrowband Internet of Things)*

P-GW بوابة شبكة البيانات القائمة على الرزم *(Packet Data Network Gateway)*

RAT تكنولوجيا للنفاذ الراديوي *(Radio Access Technology)*

SCEF وظيفة عرض قدرات الخدمة *(Service Capability Exposure Function)*

S-GW بوابة الخدمة *(Serving Gateway)*

SMS خدمة الرسائل القصيرة *(Short Message Service)*

SIM وحدة تحديد هوية المشترك *(Subscriber Identification Module)*

UE معدات المستعمل *(User Equipment)*

UMTS نظام الاتصالات المتنقلة العالمية *(Universal Mobile Telecommunications System)*

UTRA نفاذ راديوي عالمي للأرض *(Universal Terrestrial Radio Access)*

5 الاصطلاحات

لا توجد.

6 نظرة عامة لإنترنت الأشياء ضيقة النطاق

تؤدي التطورات الحالية في تكنولوجيا الاتصالات في مجال الاتصالات المتنقلة إلى تغييرات في أنماط الاتصالات من نمط الاتصالات من شخص إلى شخص إلى نمط الاتصالات من شخص إلى شيء ومن شيء إلى شيء مما يجعل التطور إلى إنترنت الأشياء (IoT) أمراً لا مناص منه.

ومقارنةً بتكنولوجيات الاتصالات قصيرة المسافة مثل Bluetooth وZigBee، وغيرها، فإن الشبكات المتنقلة الخلوية التي تتسم بالتغطية الواسعة والتنقلية والتوصيلات الكثيفة والتي تحقق سيناريوهات تطبيق أكثر ثراء، ستصبح التكنولوجيا الرئيسية للتوصيل البيني لإنترنت الأشياء.

وتقوم إنترنت الأشياء ضيقة النطاق (NB-IoT) على شبكة متنقلة خلوية تستخدم عرض نطاق لا يتجاوز 180 kHz تقريباً. ويمكن نشرها على شبكات تابعة للنظام العالمي للاتصالات المتنقلة (GSM) أو شبكة تابعة لنظام الاتصالات المتنقلة العالمية (UMTS) أو شبكات التطور طويل الأجل (LTE) مباشرةً سعياً إلى خفض التكاليف مع القدرة على التحديث السلس.

ومن بين الخصائص النمطية لإنترنت الأشياء ضيقة النطاق:

- استهلاك منخفض للطاقة: يمكن استخدام أجهزة إنترنت الأشياء ضيقة النطاق لمدد تتراوح بين 5 و10 سنوات؛
- تغطية واسعة: تتسم إنترنت الأشياء ضيقة النطاق، في نفس النطاق، بكسب يتراوح بين 15 و20 dB مقارنةً بالشبكة الحالية ومنطقة تغطية أكبر بنحو يصل إلى 100 ضعف؛
- سعة عالية: يمكن لقطاع واحد من إنترنت الأشياء ضيقة النطاق أن يدعم نحو 000 100 جهاز؛
- التكلفة المنخفضة: يبلغ سعر الجهاز الواحد من أجهزة إنترنت الأشياء ضيقة النطاق 5 دولارات أمريكية تقريباً.

وبناءً على استهلاكها المنخفض للطاقة وتغطيتها الواسعة وتكلفتها المنخفضة وسعتها العالية، يتوقع اعتماد إنترنت الأشياء ضيقة النطاق بكثافة من جانب المستعملين مع استخدامها على نطاق واسع في العديد من الصناعات الرأسية.

7 مخطط النشر وسيناريوهات التطبيق النمطية

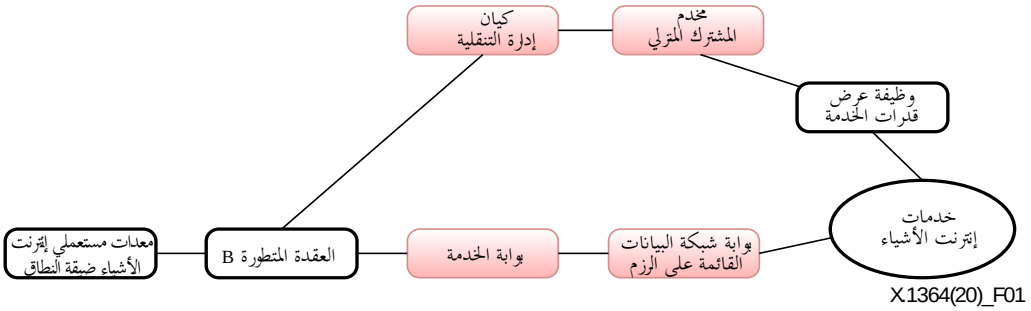
1.7 مخطط النشر

1.1.7 النشر باستخدام الشبكة الأساسية المتنقلة الحالية

في سيناريو النشر هذا، يقوم المشغلون بنشر إنترنت الأشياء ضيقة النطاق باستخدام الشبكات الأساسية المتنقلة 2/3/4G المنشورة حالياً.

وعناصر الشبكة الأساسية المتنقلة الحالية التي تشمل كيان إدارة التنقلية (MME) وبوابة الخدمة (S-GW) وبوابة شبكة البيانات القائمة على الرزم (P-GW)، يتعين استمثالها من أجل إنترنت الأشياء ضيقة النطاق لدعم الخصائص التالية [ETSI TS 123 401]:

- الاستهلاك فائق الانخفاض للطاقة في معدات المستعملين (UE)؛
- العدد الضخم من الأجهزة في كل خلية؛
- تكنولوجيات النفاذ الراديوي ذات الطيف ضيق النطاق (RAT)، مثل E-UTRA وUTRA وGSM وCDMA2000؛
- مستوى تغطية معزز.



ملاحظة – تظهر عناصر الشبكة الأساسية المتنقلة الحالية باللون الوردي.

الشكل 1 – النشر باستخدام الشبكة الأساسية الحالية للاتصالات المتنقلة

بالإضافة إلى عناصر الشبكة المستمثلة هذه، فيما يلي عناصر الشبكة الأخرى المبنية في الشكل 1 [ETSI TS 123 401]:

- العقدة المتطورة B (eNodeB): هذه عقدة النفاذ اللاسلكي التي تستضيف وظائف من أجل إدارة الموارد الراديوية وفك انضغاط بيانات الوصلة الصاعدة وتجفير تدفقات بيانات المستعملين وتسيير بيانات مستوى المستعمل وما إلى ذلك؛
- مخدم المشترك المنزلي (HSS): يخزن معلومات الاشتراك الخاص بالمستعمل مثل معلمات الاستيقان ومعلومات الموقع وما إلى ذلك؛
- وظيفة عرض قدرات الخدمة (SCEF): تعرض الخدمات وقدراتها بطريقة مؤمَنة والتي تقدم بواسطة السطوح البينية الشبكية 3GPP.

وعناصر الشبكة هذه إلى جانب وظائفها تدعم خدمات إنترنت الأشياء ضيقة النطاق عبر شبكة الاتصالات المتنقلة.

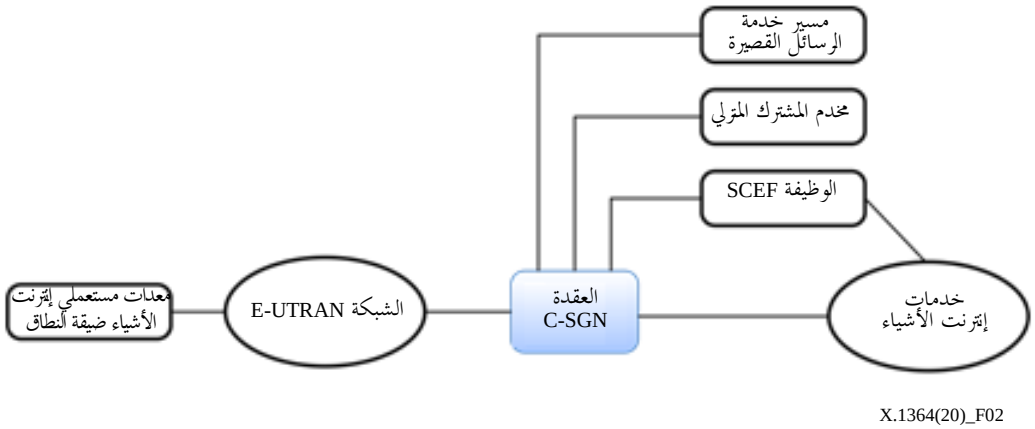
2.1.7 النشر باستخدام شبكة أساسية متنقلة مخصصة منشأة حديثاً

في سيناريو النشر هذا، ينشئ المشغلون شبكة أساسية متنقلة مخصصة تبنى بشكل جديد من أجل خدمات إنترنت الأشياء ضيقة النطاق.

وتعرف عقدة بوابة خدمة إنترنت الأشياء الخلوية (C-SGN) بالمعيار [ETSI TS 123 401].

وتدعم أي عقدة C-SGN مجموعة فرعية من الوظائف والوظائف اللازمة لعناصر الشبكة الأساسية للنظام الحالي المتطور القائم على الرزم (EPC). وهي عقدة مجمعة لشبكات أساسية متطورة قائمة على الرزم. وهي تطبق خيار العدد الأدنى من الكيانات المادية للنظام المتطور القائم على الرزم؛ وهي تضع في نفس المكان وظائف كيانات النظام EPS في مسيرات كل من مستوى التحكم ومستوى المستعمل. وتجمع العقدة C-SGN وظائف الكيان MME والبوابات P-GW وS-GW من أجل توفير حل إنترنت الاشياء

الخلوية المستمثل إلى حد كبير. ويدعم تنفيذ العقدة C-SGN خيارات سطوحها البينية الخارجة. وتقابل هذه السطوح البينية السطوح البينية للكيانات EPC المقابلة مثل MME وS-GW وP-GW.



ملاحظة – تظهر عناصر الشبكة المنشأة حديثاً باللون الأزرق.

الشكل 2 – النشر باستخدام شبكة أساسية متنقلة مخصصة منشأة حديثاً

وإلى جانب عناصر الشبكة المنشأة حديثاً، فيما يلي عناصر الشبكة الأخرى المبنية في الشكل 2 [ETSI TS 123 401]:

- الشبكة E-UTRAN: تستضيف وظائف مثل ضغط الرأسية وتشفير مستوى المستعمل واختيار الكيان MME وإنفاذ معدل مستوى الحمالة والتحكم في الازدحام ووسم رزم مستوى النقل في الوصلة الصاعدة وما إلى ذلك؛
- المخدم HSS: يخزن ويدير معلومات اشتراك المستعمل مثل معلمات الاستيقان ومعلومات الموقع؛
- الوظيفة SCEF: توفر عرضاً مؤمناً للخدمات والقدرات المقدمة عبر السطوح البينية الشبكية 3GPP؛
- مسير خدمة الرسائل القصيرة (SMS): يدعم طلبات إرفاق النقل بدون إرفاق النظام EPS المجمع (طلبات من أجل خدمات للنظام EPS وخدمات لغير النظام EPS) ولا تتاح هذه الخاصية إلا لمعدات المستعملين التي تدعم إنترنت الأشياء ضيقة النطاق فقط.

وعناصر الشبكة هذه إلى جانب وظائفها تدعم خدمات إنترنت الأشياء ضيقة النطاق عبر شبكة الاتصالات المتنقلة.

2.7 التطبيقات النمطية

1.2.7 قراءة العدادات عن بُعد

في سيناريو التطبيق هذا، تستخدم أجهزة إنترنت الأشياء ضيقة النطاق لاستقبال قراءة عداد استهلاك الأسرة للمرافق مثل المياه والغاز ولإرسال نتائج القراءة عبر شبكة لاسلكية إلى موردي خدمات المرافق.

ويسهل استخدام تكنولوجيا إنترنت الأشياء ضيقة النطاق كثيراً من قراءة العدادات ويجعلها أكثر دقة وأكثر كفاءة مقارنةً بالتقنيات التقليدية اليدوية للقراءة.

2.2.7 المرآب الذكي

في سيناريو التطبيق هذا، تنشر أماكن وقوف السيارات أجهزة إنترنت الأشياء ضيقة النطاق كأجهزة استشعار لبيان ما إذا كان في المرآب أمكنة متاحة لوقوف السيارات أم لا. ويتيح ذلك لقائدي السيارات أيضاً من مستخدمي تطبيق المرآب الذكي الحصول على اختيارات أماكن الوقوف الموصى بها واستعمال السداد الإلكتروني لرسوم صف السيارات أيضاً.

ويمكن لاستخدام تكنولوجيا إنترنت الأشياء ضيقة النطاق المساعدة في تذليل صعوبات العثور على مرائب وأماكن مفتوحة لوقوف السيارة فضلاً عما يرتبط بذلك من مسائل خاصة بالسداد.

3.2.7 الزراعة الذكية

في سيناريو التطبيق هذا، تستخدم أجهزة إنترنت الأشياء ضيقة النطاق كأجهزة استشعار لتسجيل المعلمات الزراعية مثل الملوحة والرطوبة ودرجة الحرارة وغيرها. وبناءً على هذه السجلات، يمكن لمزارع الحصول على توصيات بشأن الحلول المتعلقة بالري أو التسميد.

وباستخدام تكنولوجيا إنترنت الأشياء ضيقة النطاق تتيسر الزراعة الأكثر ذكاءً بالاستفادة من تحليل المعلومات في الوقت الفعلي بدلاً من تجارب المزارعين في الممارسات الزراعية التقليدية.

8 التهديدات التي تواجه إنترنت الأشياء ضيقة النطاق

لتحليل التهديدات الأمنية التي تواجه إنترنت الأشياء ضيقة النطاق منظوران: خصائص إنترنت الأشياء ضيقة النطاق ومنظور الإطار الوظيفي لإنترنت الأشياء ضيقة النطاق، كما هو موضح في الفقرتين 1.8 و2.8.

1.8 خصائص إنترنت الأشياء ضيقة النطاق

الخصائص النمطية لإنترنت الأشياء ضيقة النطاق هي الاستهلاك المنخفض للطاقة والتغطية الواسعة والسعة العالية والتكلفة المنخفضة.

1.1.8 تقليل استهلاك الطاقة

1) وصف الخاصية

من بين سمات أجهزة إنترنت الأشياء ضيقة النطاق، الاستهلاك المنخفض للطاقة والقدرة على التحمل وبالتالي تنخفض وتيرة الحاجة إلى إعادة الشحن وانخفاض قدرة الحساب وما إلى ذلك. والأنظمة المدمجة هي الأخرى خفيفة الوزن وأكثر بساطة.

وبوجه عام، تتسم الأنظمة التي تعمل على معدات مطرافية لإنترنت الأشياء التقليدية بخواص مثل قدرة حساب قوية فهي تستخدم بروتوكولات إرسال شبكية معقدة وحلول صارمة للتعزيز الأمني. ونتيجةً لارتفاع استهلاك الطاقة، تحتاج إلى إعادة الشحن من حين لآخر.

2) التهديدات الواقعة على إنترنت الأشياء ضيقة النطاق

يمكن تنفيذ تهديدات الحرمان من الخدمة ببساطة من خلال استهلاك موارد جهاز إنترنت الأشياء ضيقة النطاق. وتكاليف هذه الهجمات مقابل البرمجيات والعتاد منخفضة نسبياً.

وبالنظر إلى خواص جهاز إنترنت الأشياء ضيقة النطاق المتمثلة في خفة الوزن وانخفاض استهلاك الطاقة وقدرة الحساب المنخفضة، فإن تجفير البيانات أثناء الإرسال لأغراض أمنية يتعذر ضمانه. ويمكن إرسال البيانات في بعض الأوقات في نص غير مشفر. وبالتالي قد تكون هناك تهديدات أمنية مرتفعة في الاستيقان والتحقق من البيانات. فعلى سبيل المثال، قد يستخدم المهاجمون أجهزة غير مرخصة للاتصال بالمحطة القاعدة لإرسال بيانات مزيفة.

2.1.8 السعة العالية

1) وصف الخاصية

سعة إنترنت الأشياء ضيقة النطاق أكبر بكثير من إنترنت الأشياء التقليدية، فمثلاً يمكن لقطاع واحد من إنترنت الأشياء ضيقة النطاق دعم نحو 100 000 جهاز.

2) التهديدات الواقعة على إنترنت الأشياء ضيقة النطاق

مع هذه الأعداد الهائلة من الأجهزة، يمكن لموطن ضعف طفيف أن يتسبب في تأثيرات حاسمة على أمن الشبكة. فمثلاً، يمكن لفيروس حصان طروادة أن يصيب معدات مطرافية أخرى ويتسبب في عدم تيسر الشبكة.

وبالنظر إلى سيناريو نشر يتسنى فيه لأجهزة إنترنت الأشياء ضيقة النطاق أن تستعمل الشبكة الأساسية المتنقلة القائمة، وقد يكون للمعدات المطرافية القدرة على إصابة عناصر الشبكة الأساسية المتنقلة مثل: كيان إدارة التنقلية، ومخدم المشترك المنزلي، وغيرها من

الأجهزة للتأثير على مستعملي الاتصالات المتنقلة. وفي هذه الحالة، قد يرفض نفاذ المستعمل إلى الشبكة أو قد تعدل معلومات المشتركين لتجنب دفع رسوم النداءات الهاتفية أو الرسائل القصيرة أو حركة البيانات على سبيل المثال.

3.1.8 انخفاض التكلفة

1) وصف الخاصية

تكلفة أجهزة إنترنت الأشياء ضيقة النطاق منخفضة جداً عادةً.

2) التهديدات الواقعة على إنترنت الأشياء ضيقة النطاق

تتحقق التكاليف المنخفضة للأجهزة من خلال استعمال بروتوكولات مبسطة، من جملة أشياء أخرى، وبالتالي، يمكن لمهاجمين استغلال مواطن الضعف الخاصة بالبروتوكولات المبسطة وتنفيذ هجمات على الأجهزة وعلى الشبكة.

4.1.8 التغطية الواسعة

1) وصف الخواص

تحقق إنترنت الأشياء ضيقة النطاق تغطية أوسع بكثير من إنترنت الأشياء التقليدية، فمثلاً في نفس النطاق، يكون لإنترنت الأشياء ضيقة النطاق كسب تبلغ قيمته 15-20 dB مقارنةً بالشبكة الحالية وتقدم منطقة تغطية واسعة تصل إلى 100 ضعف.

2) التهديدات الواقعة على إنترنت الأشياء ضيقة النطاق

يمكن للمهاجمين الاستحواذ على الأجهزة المنشورة في مواقع نائية بسهولة واستخدامها.

2.8 طبقة إنترنت الأشياء ضيقة النطاق

1.2.8 طبقة الأجهزة

يمكن للمهاجمين تنفيذ الهجمات باستنساخ البطاقات SIM لأغراض غير قانونية مثل النفاذ المجاني إلى الشبكة.

وقد توجد مواطن الضعف الأمنية في كدسات البروتوكولات والخاصة بالوحدات المطرافية خفيفة الوزن المطورة حديثاً.

وقد يستخدم مصنعو المعدات المطرافية لإنترنت الأشياء الحالية العتاد الذي يدعم البروتوكولات Wi-Fi وBluetooth وZigBee وغيرها عند نشر معدات جديدة تدعم إنترنت الأشياء ضيقة النطاق. ونظراً إلى أنهم قد يضيفون ببساطة دعم إنترنت الأشياء ضيقة النطاق لهذه المعَدة، من الممكن ظهور مواطن ضعف وتهديدات أمنية خلال مراحل التطوير. ومن مجالات الأمثلة على ذلك، قد لا تتحقق الحماية لمنافذ إزالة الأعطال على النحو الأمثل، قد تستخدم خوارزميات تجفير ضعيفة وقد يحدث تعثر في تطبيق تحديثات العتاد والافتقار إلى التحقق من السلامة في الوقت المناسب عند الحاجة.

2.2.8 طبقة الشبكة

يمكن لأدوات اختطاف اتصالات بيانات الشبكة أن تراقب الدورات بين المعدات المطرافية والمحطات القاعدة للاستحواذ على رزم البيانات المتبادلة بين هذه المكونات. وبناءً على ذلك، يتم اختطاف الاتصالات وينتج عن ذلك تمكين المهاجمين من تحليل مواطن الضعف الأمنية عبر البيانات المستخلصة من رسائل الاتصالات المختطفة.

ومع وجود هذه الأعداد الهائلة من الأجهزة وتقاسم شبكة الاتصالات المتنقلة مع مشتركي الاتصالات المتنقلة، يمكن لأجهزة إنترنت الأشياء ضيقة النطاق المتلاعّب بها أن تفضي إلى عاصفة من عواصف التشوير.

وقد تكون هناك مخاطر لكشف البيانات نتيجةً لتعدد عمليات جمع البيانات من جانب خدمات إنترنت الأشياء ضيقة النطاق وتنقل على الشبكة وتعالج من قبل العديد من عناصر الشبكة.

ويمكن لتشوير الشبكة الأساسية لإنترنت الأشياء ضيقة النطاق أن يتعرض للتزييف أو الغش أو هجمات إعادة التشغيل نتيجةً لعدم وجود آلية استيقان ضمن عناصر الشبكة.

ويمكن لهجمات متعددة عبر الإنترنت إلحاق الضرر بالسطح البيني بين الشبكة الأساسية المتنقلة والإنترنت، ففي النظام 5G مثلاً، يُعرف السطح البيني بين الشبكة الأساسية المتنقلة والإنترنت باسم السطح البيني N6 [ETSI TS 123 501]، ويوصل هذا السطح البيني N6 وظيفة مستوى المستعمل والإنترنت.

3.2.8 طبقة التطبيق

تعد إنترنت الأشياء ضيقة النطاق مناسبة لسيناريوهات الأعمال ذات الأعمال السكونية وقليلة الحساسية للكمون وذات الحركات غير المستمرة وإرسال البيانات في الوقت الفعلي.

قد يحدث إغفال أو إنذار كاذب في أعمال الإبلاغ الأتوماتي عن الأحداث غير الاعتيادية (مثل كاشف إنذار الدخان) وأعمال الإبلاغ الدورية (مثل نظام مراقبة الوضع البيئي). فمثلاً، إذا استحوذ مهاجم على قراءة عداد كهربائي ذكي لأحد المستعملين، يمكن تعديل الأرقام أو تزييفها وبالتالي المساس بالفوائد العائدة على المستعمل.

وفوق ذلك، يمكن أيضاً للإرشادات الخبيثة أن تشكل خطراً على أعمال توجيه الإرشادات عن بُعد (مثل معدات المنازل الذكية التي يمكن تشغيلها وإبطالها من جانب المستعملين عن بُعد).

وتدمج أعمال إنترنت الأشياء ضيقة النطاق بعمق مع صناعات مختلفة، ولذا، فهي عرضة لمواطن ضعف مثل تلك المتأصلة في القواعد المنطقية للأعمال المعقدة وبروتوكولات التطبيق المتعددة.

وقد يساء إلى خدمات إنترنت الأشياء ضيقة النطاق من خلال فصل بطاقة الضبط، مثلاً، من خلال إدراج بطاقة إنترنت الأشياء ضيقة النطاق لمشترك في جهاز آخر خلاف جهاز إنترنت الأشياء ضيقة النطاق، أو عند إرسال رسالة تطفلية قصيرة بهذه البطاقة.

9 متطلبات الأمن

1.9 متطلبات أمن الأجهزة المطرافية

1.1.9 الأمن المادي

يوفر الجهاز المطرفي لإنترنت الأشياء ضيقة النطاق الحماية المادية للسطوح البينية والشرائح وهو ما يضمن تعذر نفاذ أي مهاجم إلى البيانات حتى وإن استحوذ على العتاد.

ولسطوح بينية مختلفة، يدعم الجهاز المطرافي لإنترنت الأشياء ضيقة النطاق وظيفتي الاستيقان والتخويل.

2.1.9 أمن عمليات التحديث

يحتاج نظام جهاز إنترنت الأشياء ضيقة النطاق وبرمجياته وعتاده إلى القدرة على التحديث لضمان أمن النظام والتطبيق.

ويتعين حماية سرية ملفات التحديث وسلامتها لتفادي التلاعب.

3.1.9 حماية الخصوصية

يتعين وجود آليات مرنة لحماية الخصوصية في الجهاز المطرافي لإنترنت الأشياء ضيقة النطاق لدعم حماية الخصوصية استناداً إلى متطلبات خدمة إنترنت الأشياء ضيقة النطاق.

2.9 متطلبات أمن الشبكات

1.2.9 الاستيقان

يلزم الاستيقان للتحقق من هويات كيانات إنترنت الأشياء ضيقة النطاق التي تستعمل خدمة إنترنت الأشياء ضيقة النطاق. ويضمن الاستيقان صحة الهويات التي تدعيها الكيانات ويقدم الضمان بأن الكيانات لا تحاول انتحال صفة كيانات مخوَّلة.

والاستيقان الخفيف هو المطلوب مراعاةً لخصائص إنترنت الأشياء ضيقة النطاق.

2.2.9 منع هجمات الحرمان من الخدمة الموزع

هذا الأمر مطلوب من أجل النشر المسبق لآليات الأمن اللازمة لمنع هجمات الحرمان من الخدمة الموزع (DDoS) والتعامل معها في الوقت المناسب.

3.2.9 أمن كيانات الشبكة

يلزم وجود كيانات الشبكة الأساسية لإنترنت الأشياء ضيقة النطاق لدعم قدرات الأمن لمقاومة هجمات التزوير والتلاعب وإعادة التشغيل.

3.9 متطلبات أمن التطبيقات

1.3.9 مراقبة الامتثال لاستعمال/تشغيل الخدمة

تلزم مراقبة الامتثال لاستعمال/تشغيل الخدمة لمراقبة القيم القصوى وإجمالي عدد التدفقات ولاكتشاف الحالات غير الاعتيادية لاستعمال/تشغيل الخدمة طبقاً لمتطلبات خدمات إنترنت الأشياء ضيقة النطاق.

2.3.9 منع إساءة استعمال الخدمة

يلزم منع إساءة استعمال الخدمة من خلال فصل بطاقة الاتصالات عن طريق مراقبة خصائص تغير الهوية الدولية للمعدات المتنقلة.

3.3.9 تحديد تحليل واستيعاب قدرات التهديدات الأمنية

يلزم تحديد تحليل واستيعاب قدرات التهديدات الأمنية بناءً على تحليل البيانات الضخمة لسلوك الجهاز المطرافي لإنترنت الأشياء ضيقة النطاق.

10 القدرات الأمنية لإنترنت الأشياء ضيقة النطاق

1.10 القدرات الأمنية للأجهزة المطرافية

ينبغي للجهاز المطرافي لإنترنت الأشياء ضيقة النطاق أن يتضمن القدرات الأمنية التالية:

- SC_terminal device 1: قدرة إدارة المفاتيح؛
- SC_terminal device 2: قدرة التفاوض بشأن خوارزمية التجفير؛
- SC_terminal device 3: قدرة تجفير البيانات؛
- SC_terminal device 4: قدرة سلامة البيانات؛
- SC_terminal device 5: قدرة التحديث الآمن بما في ذلك للنظام والبرمجيات والعتاد وما إلى ذلك؛
- SC_terminal device 6: قدرة تنفيذ بروتوكولات آمنة استناداً إلى التجفير الخفيف.

2.10 القدرات الأمنية للشبكة

ينبغي لشبكة إنترنت الأشياء ضيقة النطاق أن تتضمن القدرات الأمنية التالية للشبكة:

- SC_network 1: قدرة إدارة المفاتيح؛
- SC_network 2: قدرة التفاوض بشأن خوارزمية التجفير؛
- SC_network 3: قدرة تجفير البيانات؛
- SC_network 4: قدرة سلامة البيانات؛
- SC_network 5: قدرة التحكم في النفاذ للتأكد من أنه لا يسمح للنفاذ إلى عناصر شبكة إنترنت الأشياء ضيقة النطاق والمعلومات المخزنة وتدفقات المعلومات والخدمات والتطبيقات إلا للكيانات المخوَّلة؛
- SC_network 6: قدرة الكشف عن التلاعب و/أو منعه؛
- SC_network 7: قدرة ضد هجمات رفض الخدمة الموزع؛
- SC_network 8: قدرة لإجراء تشكيلات آمنة؛
- SC_network 9: قدرة لاكتشاف فصل بطاقة الاتصالات.

3.10 القدرات الأمنية للتطبيقات

ينبغي للتطبيقات أن تتضمن ما يلي من القدرات الأمنية:

- SC_applications 1: قدرة للحماية ضد الإصابة بالبرمجيات الخبيثة عبر استخدام برمجية حماية من البرمجيات الخبيثة؛
- SC_applications 2: قدرة لمراقبة الامتثال لاستعمال/تشغيل الخدمة عبر المؤشرات الرئيسية للشبكة (مثل القيمة القصوى وإجمالي عدد التدفقات)؛
- SC_applications 3: قدرة بشأن أمن مستوى التطبيق لمنع التهديدات الأمنية استناداً إلى تحليل البيانات الضخمة لسلوك الجهاز المطرافي لإنترنت الأشياء ضيقة النطاق.

4.10 العلاقة بين القدرات الأمنية ومتطلبات الأمن

تستعمل القدرات الأمنية الواردة والموصوفة في الفقرة 10 لاستيفاء بعض متطلبات الأمن الموصفة في الفقرة 9. ويعرض في الجدول 1 التقابل بين القدرات الأمنية ومتطلبات الأمن.

وفي الجدول 1، يشير الرمز "√" في كل خلية إلى متطلب الأمن المتعلق بقدرة أمنية معينة. وبشكل أدق، ينبغي لمتطلب الأمن المؤشر عليه بالرمز "√" أن يُدعم من خلال تنفيذ القدرة المؤشر عليها.

الجدول 1 – توضيح العلاقة بين متطلبات الأمن والقدرات الأمنية

المتطلبات / القدرات	الأمن المادي	أمن عمليات التحديث	حماية الخصوصية	الاستيقان	منع هجمات رفض الخدمة الموزع	مراقبة الامتثال لاستعمال/ تشغيل الخدمة	منع إساءة استعمال الخدمة	تحديد وتحليل واستيعاب التهديدات الأمنية
SC_terminal device 1	√			√				
SC_terminal device 2	√							
SC_terminal device 3			√					
SC_terminal device 4		√						
SC_terminal device 5	√	√						
SC_terminal device 6			√	√				
SC_network 1				√				
SC_network 2		√	√					
SC_network 3		√	√					
SC_network 4		√						
SC_network 5			√	√				
SC_network 6						√		
SC_network 7					√			
SC_network 8		√						
SC_network 9							√	
SC_applications 1		√						
SC_applications 2					√	√	√	
SC_applications 3			√					√

بيبليوغرافيا

[b-ITU-T Q.1743] Recommendation ITU-T Q.1743 (2016), *IMT-Advanced references to Release 11 of LTE-Advanced evolved packet core network*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for open systems interconnection for CCITT applications*.

[b-ITU-T X.1141] Recommendation ITU-T X.1141 (2006), *Security Assertion Markup Language (SAML 2.0)*.

[b-ITU-T X.1145] Recommendation ITU-T X.1145 (2017), *Security framework and requirements for open capabilities of telecommunication services*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

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، 2020