الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1366

(2020/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

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

مخططات استيقان الرسالة المجمَّع في بيئة إنترنت الأشياء (IoT)

التوصية ITU-T X.1366

الاتحاد الدولي للاتصالات

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	
المصطلحات	X.1700–X.1701
مولِّد الأعداد العشوائية الكمومية	X.1702–X.1709
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1710–X.1711
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1712–X.1719
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1720–X.1729
أمن البيانات	
أمن البيانات الضخمة	X.1750–X.1759
أمن شبكات الجيل الخامس	X.1800–X.1819

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

مخططات استيقان الرسالة المجمَّع في بيئة إنترنت الأشياء (IoT)

ملخص

تتزايد أعداد أجهزة إنترنت الأشياء (IoT) وسيكون هناك في المستقبل القريب عدد ضخم من الأجهزة الموصولة بشبكة إنترنت الأشياء بما في ذلك تكنولوجيا الجيل الخامس. وتوصف التوصية ITU-T X.1366 مخططين لاستيقان الرسالة. أحدهما مخطط استيقان الرسالة المجمَّع (AMA) في إنترنت الأشياء كآلية أساسية. والآخر مخطط استيقان الرسالة المجمَّع التفاعلي (IAMA) ببروتوكول تفاعلي بصورة بسيطة ومأمونة. ومخططا استيقان الرسالة المجمَّع كلاهما يمكن تطبيقه من أجل ضمان "استيقان (هوية) الكيان" علاوةً على "استيقان الرسالة". وهذان المخططان قد يكونان غير قابلين للتطبيق في جميع حالات الاستعمال الخاصة باستخدام أجهزة إنترنت الأشياء، ولكنهما فعّالان ومناسبان تماماً لحالات الاستعمال في ظل الظروف التالية، عندما:

- يُتطلب استيقان الرسالة لأعداد من أجهزة إنترنت الأشياء تتراوح بين العشرات وعشرات الآلاف.
- يتم التعامل مع البيانات أو الرسالة من أجل عملية استيقان تحدث كثيراً وبصورة متقطعة.

فمثلاً، "تطبيقات المراقبة لاستعمال بيانات الصور" و"القياس عند بُعد" مثل عمليات مراقبة النباتات أو المصانع والمراقبة الصحية هي أمثلة نمطية مرشحة كحالات استعمال لهذين المخططين.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1366	2020-09-03	17	11.1002/1000/14262

مصطلحات أساسية

استيقان الرسالة المجمَّع (AMA)، إنترنت الأشياء (IoT).

* 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/.

جدول المحتويات

الصفحة

التوصية ITU-T X.1366

مخططات استيقان الرسالة المجمَّع في بيئة إنترنت الأشياء (IoT)

1 مجال التطبيق

توصف هذه التوصية مخططين لاستيقان الرسالة. أحدهما مخطط استيقان الرسالة المجمَّع (AMA) في إنترنت الأشياء كآلية أساسية. والآخر مخطط استيقان الرسالة المجمَّع التفاعلي (IAMA) مع بروتوكول تفاعلي بصورة بسيطة ومأمونة. ومخططا استيقان الرسالة المجمَّع كلاهما يمكن تطبيقه من أجل ضمان "استيقان (هوية) الكيان" علاوةً على "استيقان الرسالة".

أما كيفية تنفيذ هذين المخططين في بيئة محددة لإنترنت الأشياء، بالإضافة إلى تكنولوجيات التوقيع المجمَّع، فهي تقع خارج مجال تطبيق هذه التوصية.

2 المراجع

تضم توصيات قطاع تقييس الاتصالات المذكورة أدناه وغيرها من المراجع أحكاماً تؤلف، من خلال الإشارات الواردة إليها في هذا النص، أحكاماً لهذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع للمراجعة؛ 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. ولا تضفي الإشارة إلى وثيقة ما في هذه التوصية على تلك الوثيقة في حد ذاتها صفة التوصية.

لا توجد.

3 التعاريف

1.3 مصطلحات معرّفة في مكان آخر

تستخدم هذه التوصية التعريف التالي المعرّف في مصادر أخرى:

1.1.3 شفرة استيقان الرسالة (message authentication code) (MAC) [b-ITU-T X.813]: قيمة تحقق مجفّرة تستخدم لتوفير استيقان من منشأ البيانات وسلامتها.

2.3 مصطلحات معرّفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 استيقان رسالة (message authentication): خاصية تضمن عدم تعديل الرسالة أثناء الانتقال لضمان سلامة البيانات، وتتيح للطرف المستقبِل التحقق من مصدر الرسالة.

2.2.3 استيقان الرسالة المجمَّع (aggregate message authentication) (AMA): خاصية تسمح بتجميع شفرات متعددة لاستيقان رسالة، ينشئها مرسلون متعددون، في شفرة استيقان أقصر ويظل بإمكان المستقبِل الذي يمتلك مفاتيح المرسلين السرية أن يتحقق منها.

3.2.3 وسوم الاستيقان (authentication tags): قطعة من البيانات تُستخدم لاستيقان الرسالة.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات التالية:

AGT بروتوكول اختبار الزمرة التكيفي *(Adaptive Group Testing protocol)*

AMA استيقان الرسالة المجمَّع *(Aggregate Message Authentication)*

AMAC شفرة استيقان الرسالة المجمَّع *(Aggregate Message Authentication Code)*

IAMA استيقان الرسالة المجمع التفاعلي *(Interactive Aggregate Message Authentication)*

IoT إنترنت الأشياء *(Internet of Things)*

MAC شفرة استيقان الرسالة *(Message Authentication Code)*

XOR عملية التخيير الحصري *(Exclusive OR operation)*

5 الاصطلاحات

لا توجد.

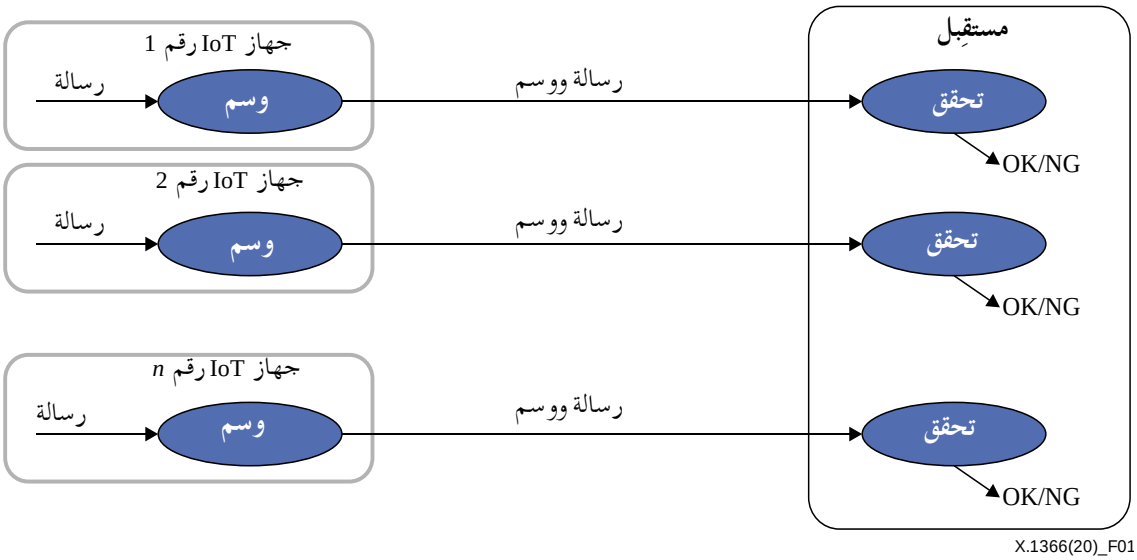
6 نظرة عامة والمفهوم الأساسي

1.6 نظرة عامة

تتزايد أعداد أجهزة إنترنت الأشياء (IoT) وسيكون هناك في المستقبل القريب عدد ضخم من الأجهزة الموصولة بشبكة إنترنت الأشياء بما في ذلك تكنولوجيا الجيل الخامس. وتقدم هذه التوصية نظام استيقان خفيفاً وآمناً يمكن تطبيقه في مثل هذه الحالة.

وتعد شفرة استيقان الرسالة (MAC) أحد أكثر أسس التجفير أساسيةً، ويمكن استخدام شفرة MAC باعتبارها أساس تجفير خفيف لاستيقان الرسالة. ولكن على النحو الموضح في الشكل 1، في أنظمة إنترنت الأشياء الحالية، للرسالة المرسلة من أجهزة إنترنت الأشياء، تتولد وسوم الاستيقان (انظر الفقرة 3.2.3) بشكل فردي على جانب جهاز إنترنت الأشياء، ويُتحقق بشكل أساسي من كل رسالة تحتوي على وسم متولد بعملية التحقق على جانب المستقبِل. وتتمثل المشكلة الرئيسية المعروفة في سيناريو إنترنت الأشياء الحالي في أن عبء عمليات الاستيقان والتحقق الحالية يتزايد بما يتناسب مع الزيادة في عدد أجهزة إنترنت الأشياء.

وشفرة استيقان الرسالة المجمَّع (AMAC) هي تكنولوجيا قائمة تسمح بضغط العديد من وسوم شفرة استيقان الرسالة (MAC) على رسائل متعددة متولدة بواسطة أجهزة مختلفة في وسم كلي واحد دون الانتقاص من الأمن (انظر التذييل II). وتكمن ميزة شفرة AMAC في أن مقاس الوسم المجمَّع أصغر بكثير من إجمالي المقاسات المجمعة لوسوم شفرة MAC، ويستفاد بالتالي منها في تطبيقات في شبكات الاتصالات المتنقلة أو شبكات إنترنت الأشياء حيث يجري توصيل العديد من الأجهزة التي ترسل الرسائل. وعلى وجه التحديد، يمكن استخدام شفرة AMAC في التطبيقات لزيادة كفاءة الشبكات التي تستخدم شفرات MAC. ولكن لا يمكن لهذا الأسلوب تحديد الرسائل غير الصالحة من بين الرسائل المتعددة بمجرد اعتبار هذه الرسائل غير صالحة باستخدام وسم كلي في شفرة AMAC بشكل عام. وفي هذه التوصية، يوسَّع مخطط شفرة AMAC الحالي بحيث يسمح بضغط العديد من وسوم شفرة MAC مع إمكانية الكشف لتحديد الرسائل غير الصالحة.



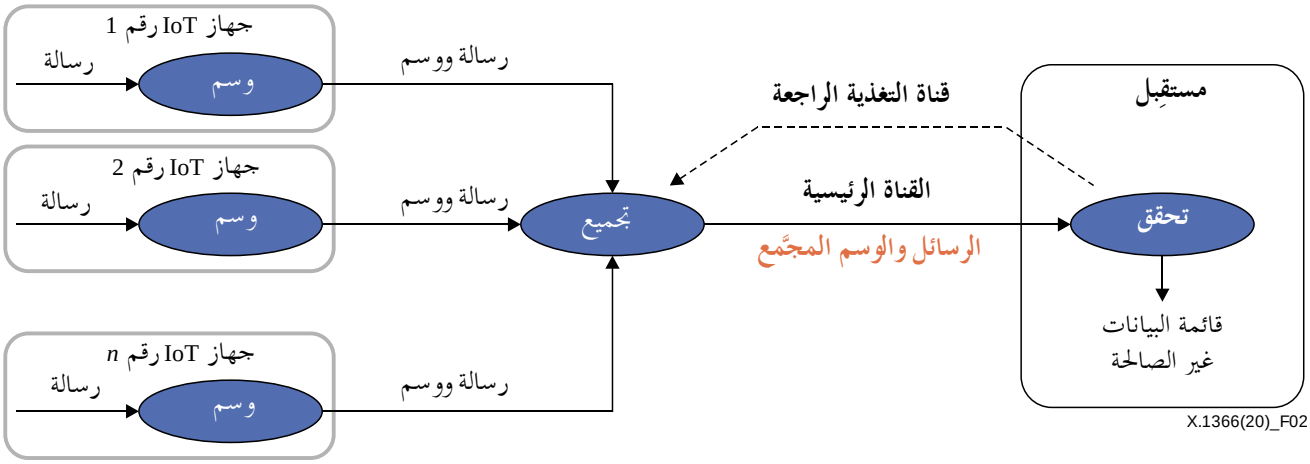
الشكل 1 – نظام الاستيقان الإفرادي (النظام التقليدي)

2.6 المفهوم الأساسي لنظام استيقان الرسالة المجمَّع

1.2.6 اعتبارات عامة

يبين الشكل 2 المخطط الأساسي لاستيقان الرسالة المجمَّع (AMA) المقترح في هذه التوصية. فتثبَّت عقدة التجميع في نظام شبكة إنترنت الأشياء لتجميع وسوم شفرة استيقان الرسالة (MAC)/وسوم الاستيقان دون تغيير أنساق المدخلات أو هياكل شفرات MAC الموجودة في الشبكة. وتضغط عقدة التجميع العديد من وسوم MAC المرفقة في رسائل متعددة متولد بواسطة أجهزة مختلفة في وسم مجمع واحد دون الانتقاص من الأمن، ويرسَل الوسم المجمع عبر قناة رئيسية إلى مستقبِل لإجراء عمليات التحقق للوسم. ويتحقق المستقبِل من صحة رسائل متعددة باستخدام الوسم المجمع ويمكنه تحديد الرسالة أو البيانات غير الصالحة من الوسم المجمع. وهذه التقنية فعّالة في تقليل حجم البيانات المرسلة عندما يكون مقاس الوسم المجمع أصغر بكثير من المقاس الإجمالي لوسوم MAC المتعددة.

وتصف هذه التوصية مخطط استيقان الرسالة المجمَّع (AMA) لإنترنت الأشياء كآلية أساسية ومخطط استيقان الرسالة المجمَّع التفاعلي (IAMA) لشرح كيفية تنفيذ عمليات التجميع والتحقق. ففي مخطط AMA، يكتفى باستخدام القناة الرئيسية من عقدة التجميع إلى المستقبِل لإرسال الوسم المجمَّع. وتوصَّف خوارزميات التجميع والتحقق من مخطط AMA في الفقرة 7. وفي مخطط استيقان الرسالة المجمَّع التفاعلي، تُستخدم أيضاً، بالإضافة إلى القناة الرئيسية، قناة تغذية راجعة وهي قناة استيقان ذات عرض نطاق منخفض من المستقبِل إلى عقدة التجميع. وبإرسال نتيجة تحقق من المستقبِل إلى عقدة التجميع عبر قناة التغذية الراجعة، يمكن لعقدة التجميع ضغط وسوم شفرة استيقان الرسالة (MAC) بفعالية أعلى من استيقان الرسالة المجمَّع في الفقرة 7. وينفَّذ بروتوكول تفاعلي بين عقدة التجميع والمستقبِل للتحقق ويرد توصيفه في الفقرة 8.



الشكل 2 – المفهوم الأساسي لنظام استيقان الرسالة المجمع

ملاحظة – في الحالات التي ترسل فيها أجهزة متعددة بيانات الخصوصيات باستخدام مخططات التجفير السابق لشفرة استيقان الرسالة (MAC)، يمكن تطبيق تقنية التجميع في هذه التوصية لضغط وسوم MAC متعددة.

وفي هذه التوصية، هناك أربع عمليات تُستخدم لأداء مخططي استيقان الرسالة المجمَّع (AMA) واستيقان الرسالة المجمَّع التفاعلي (IAMA) وهي: إنشاء المفاتيح والوسم والتجميع والتحقق كما يلي:

1) يأخذ إنشاء المفاتيح كمدخلات معلمة أمنية ومعرف (ID)، وينتج مفتاحاً سرياً للمعرف.

2) يأخذ الوسم رسالة ومعرفاً ومفتاحاً سرياً مطابقاً للمعرف كدخل، ويُخرج وسماً.

3) يأخذ التجميع عدة متراتبات من المعرفات والرسائل والوسوم من أجهزة متعددة كمدخلات، وينتج متراتبة من الوسوم المجمعة كمخرجات.

4) يأخذ التحقق جميع المفاتيح السرية، وأزواج متعددة من المعرفات والرسائل من أجهزة متعددة، ومتراتبة من الوسوم المجمعة كمدخلات. ويحدد الرسائل غير الصالحة، ويُخرج قائمة بمعرفات الأجهزة ذات الرسائل غير صالحة.

7 استيقان الرسالة المجمَّع

1.7 اعتبارات عامة

يقدم مخطط شفرة استيقان الرسالة المجمع (AMAC) المبين في هذه التوصية وظائف تجميع وسوم شفرة استيقان الرسالة (MAC) المتعددة في وسم أقصر، وتحديد الرسالة غير الصالحة منها. وتوضح هذه الفقرة كيفية إنشاء الخوارزميات الأربع: وتُنشأ المفاتيح والوسم والتجميع والتحقق لتوليد شفرة استيقان الرسالة المجمع.

2.7 الترميز المحدد

تُستعمل في هذه التوصية الرموز المحددة التالية:

n عدد الأجهزة

d عدد الرسائل غير الصالحة من الأجهزة

id معرف الجهاز. فتكون $ID = \{id_1, id_2, \ldots, id_n\}$ هي مجموعة جميع المعرّفات.

m رسالة

k_{id} مفتاح سري لمعرف الجهاز. وللتبسيط، يرمز k_i إلى المفتاح السري المقابل للمعرف id_i بدلاً من الرمز k_{id_i}

$F()$ دالة شفرة استيقان الرسالة (MAC) التي تأخذ مفتاحاً سرياً ورسالة كمدخلات وتُخرج وسم MAC.

$G = (g_{i,j})$ مصفوفة منفصلة بدرجة d ذات صفوف عددها u وأعمدة عددها n. وللمصفوفة G إدخالات بنسق {0,1}، وتُفهرس الأعمدة بالمعرفات، $id_1, id_2, \ldots, id_n$.. وتُعتبر مصفوفة G منفصلة بدرجة d، إن لم تحوِ المجاميع البولانية (Boolean) لأي أعمدة عددها d أي عمود آخر، حيث يحتوي $x = (x_1, x_2, \ldots, x_u)$ على $y = (y_1, y_2, \ldots, y_u)$ في حال $x_i \geq y_i$ لكل $1 \leq i \leq u$.

$I(G, i)$ مجموعة j $(1 \leq j \leq n)$ بحيث $g_{i,j} = 1$ لكل $i = 1,2, \ldots, u$.

$\oplus$ عملية التخيير الحصري (XOR) على مستوى البتات

$H()$ دالة الاختزال

3.7 توصيف الخوارزمية

لتغطية التطبيقات الأوسع، يقدَّم نوعان من شفرة استيقان الرسالة (MAC) المجمع مع خواص الكشف الوظيفية. أحدهما قائم على التخيير الحصري (XOR) (الفقرة 1.3.7) والآخر يعتمد على دالة الاختزال (الفقرة 2.3.7).

1.3.7 الإنشاء القائم على التخيير الحصري (XOR)

1.1.3.7 إنشاء المفاتيح

لكل معرف، تنشئ هذه العملية مفتاحاً عشوائياً يُشار إليه بالرمز k_{id}.

2.1.3.7 الوسم

يأخذ الوسم كمدخلات رسالة ومعرفاً ومفتاحاً سرياً تطابق المعرف، ويشار إليها بالرموز، id, m, k_{id}، على التوالي، ويُخرج الوسم t لشفرة استيقان الرسالة (MAC)، ويُحسب هذا الوسم بالدالة $F(k_{id}, m)$.

3.1.3.7 التجميع

يأخذ التجميع كمدخلات المعرفات والرسائل ووسوم شفرة استيقان الرسالة (MAC) الخاصة بها من أجهزة عددها n، ويشار إليها بالرموز $(id_1, m_1, t_1), \ldots, (id_n, m_n, t_n)$. ويأخذ لكل i $(1 \leq i \leq u)$، التخيير الحصري (XOR) على مستوى البتات لوسوم MAC التي تندرج معرفاتها المقابلة في مجموعة $I(G, i)$ وتعرَّف بالعملية T_i، أي $T_i = \oplus_{j \in I(G,i)} t_j$. ثم تُخرِج $(T_1, T_2, \ldots, T_u)$ كوسم مجمع.

4.1.3.7 التحقق

يأخذ التحقق كمدخلات جميع المفاتيح السرية التي يرمز لها بالرمز $(k_1, \ldots, k_n)$، وأزواج متعددة من المعرّفات والرسائل من أجهزة عددها n يشار إليها بالرمز $(id_1, m_1), \ldots, (id_n, m_n)$، ووسم مجمع يشار إليه بالرمز $(T_1, T_2, \ldots, T_u)$. ثم يُخرِج القائمة J بعد الإجراء التالي.

الخطوة 1: $J \leftarrow \{id_1, id_2, \ldots, id_n\}$

الخطوة 2: من أجل $i = 1,2, \ldots, u$ يجرى ما يلي:

في حال $T_i = \oplus_{j \in I(G,i)} t_j$، عندئذ $J \leftarrow J \setminus \{id_j\}$، لجميع $j \in I(G, i)$.

2.3.7 الإنشاء القائم على الاختزال

1.2.3.7 إنشاء المفاتيح

لكل معرف، تنشئ هذه العملية مفتاحاً عشوائياً يُشار إليه بالرمز k_{id}.

2.2.3.7 الوسم

يأخذ الوسم كمدخلات رسالة ومعرفاً ومفتاحاً سرياً تطابق المعرف، ويشار إليها بالرموز، id, m, k_{id}، على التوالي، ويُخرج الوسم t لشفرة استيقان الرسالة (MAC)، ويُحسب هذا الوسم بالدالة $F(k_{id}, m)$.

3.2.3.7 التجميع

يأخذ التجميع كمدخلات المعرفات والرسائل ووسوم شفرة استيقان الرسالة (MAC) الخاصة بها من أجهزة عددها n، ويشار إليها بالرموز $(id_1, m_1, t_1), \dots, (id_n, m_n, t_n)$. وتُحسب لكل i $(1 \le i \le u)$، قيمة اختزال وسوم شفرة استيقان الرسالة (MAC) التي تندرج معرفاتها المقابلة في مجموعة $I(G, i)$ وتعرَّف بالعملية T_i، أي $T_i = H(t_{j_1}, t_{j_2}, \dots)$ حيث $I(G, i) = \{j_1, j_2, \dots\}$ مع $1 \le j_1 < j_2 < \cdots$.

ثم تُخرِج $(T_1, T_2, \dots, T_u)$ كوسم مجمع.

4.2.3.7 التحقق

يأخذ التحقق كمدخلات جميع المفاتيح السرية التي يرمز لها بالرمز $(k_1, \dots, k_n)$، وأزواج متعددة من المعرّفات والرسائل من أجهزة عددها n يشار إليها بالرمز $(id_1, m_1), \dots, (id_n, m_n)$، ووسم مجمع يشار إليه بالرمز $(T_1, T_2, \dots, T_u)$. ثم يُخرِج القائمة J بعد الإجراء التالي.

الخطوة 1: $J \leftarrow \{id_1, id_2, \dots, id_n\}$

الخطوة 2: من أجل $i = 1,2, \dots, u$ يجرى ما يلي:

في حال $T_i = H(t_{j_1}, t_{j_2}, \dots)$، حيث $I(G, i) = \{j_1, j_2, \dots\}$ مع $1 \le j_1 < j_2 < \cdots$،

عندئذ $J \leftarrow J \setminus \{id_j\}$، لجميع $j \in I(G, i)$.

8 استيقان الرسالة المجمع التفاعلي (IAMA)

1.8 اعتبارات عامة

يقدم مخطط استيقان الرسالة المجمع التفاعلي (IAMA) المقترَح في هذه التوصية الخواص الوظيفية التي تمكِّن استيقان الرسالة المجمع التفاعلي من تحديد الرسائل غير الصالحة ذات مقاس الوسم الأصغر من مقاس وسم تلك الموجودة في مخطط استيقان الرسالة المجمع (AMA) في الفقرة 7. ويتكون مخطط IAMA من خوارزميتي إنشاء المفاتيح والوسم وبروتوكول تفاعلي بين التجميع والتحقق. وتشرح هذا الفقرة كيفية إنشاء هاتين الخوارزميتين والبروتوكول.

2.8 الترميز المحدد

تُستعمل في هذه التوصية الرموز المحددة التالية:

n عدد الأجهزة

d عدد الرسائل غير الصالحة من الأجهزة

id معرف الجهاز. فتكون $ID = \{id_1, id_2, \dots, id_n\}$ هي مجموعة جميع المعرّفات.

m رسالة

k_{id} مفتاح سري لمعرف الجهاز. وللتبسيط، يرمز k_i إلى المفتاح السري المقابل للمعرف id_i بدلاً من الرمز k_{id_i}.

$F()$ دالة شفرة استيقان الرسالة (MAC) التي تأخذ مفتاحاً سرياً ورسالة كمدخلات وتُخرج وسم MAC.

AGT بروتوكول اختبار الزمرة التكيفي

$\oplus$ عملية التخيير الحصري (XOR) على مستوى البتات

$H()$ دالة الاختزال

3.8 توصيف البروتوكول التفاعلي

يمكن إنشاء استيقان الرسالة المجمع التفاعلي (IAMA) من دالة $F()$ وبروتوكول اختبار الزمرة التكيفي (AGT)، انظر التذييل III بشأن اختبار الزمرة التكيفي. وتُعرض هذه الإنشاءات هنا باستخدام نوعين من العمليات، عملية التخيير الحصري (XOR) أو دالة الاختزال على النحو الموضح في إنشاءات استيقان الرسالة المجمع (AMA).

1.3.8 الإنشاء القائم على التخيير الحصري (XOR)

1.1.3.8 إنشاء المفاتيح

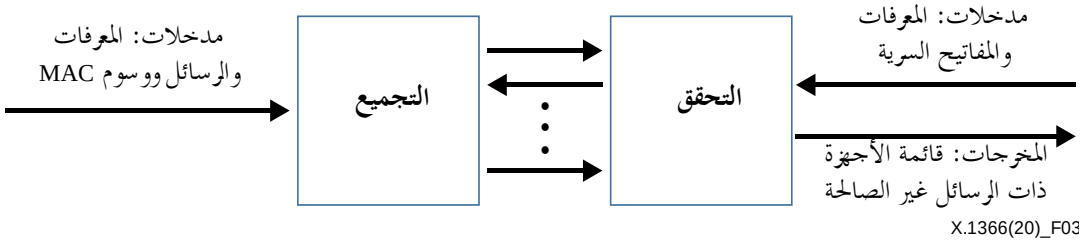
لكل معرف، تنشئ هذه العملية مفتاحاً عشوائياً يُشار إليه بالرمز k_{id}.

2.1.3.8 الوسم

يأخذ الوسم كمدخلات رسالة ومعرفاً ومفتاحاً سرياً تطابق المعرف، ويشار إليها بالرموز، id, m, k_{id}، على التوالي، ويُخرج الوسم t لشفرة استيقان الرسالة (MAC)، ويُحسب هذا الوسم بالدالة $F(k_{id}, m)$.

3.1.3.8 التجميع والتحقق

يُنشأ التجميع والتحقق استناداً إلى بروتوكول AGT على النحو الموضح في الشكل 3. ويأخذ التجميع كمدخلات المجموعة الكاملة من المعرفات $ID = \{id_1, id_2, \dots, id_n\}$، والرسائل ووسوم شفرة استيقان الرسالة (MAC) الخاصة بها من أجهزة عددها n، ويشار إليها بالرموز $(m_1, t_1), \dots, (m_n, t_n)$، حيث (m_i, t_i) $(1 \le i \le n)$ هو زوج وسوم رسالة يقابل id_i. ويأخذ التحقق كامل مجموعة المعرفات (ID) وجميع المفاتيح السرية k_i $(1 \le i \le n)$ التي تقابل id_i. فأولاً، يقوم التجميع باختيار مجموعة فرعية $S \subseteq ID$، ويقوم بإنشاء وسم مجمع، T_S، بضغط وسوم MAC في المجموعة الفرعية S: ويمكن إنشاء T_S بإجراء عملية XOR على وسوم MAC، $T_S = \oplus_{j \in S} t_j$. ثم يرسِل التجميع وسم T_S مع الرسائل $(m_1, \dots, m_n)$ إلى التحقق. وبعد ذلك، يضبط التحقق $J = ID$ ويتحقق من صلاحية وسم T_S باستخدام المفاتيح السرية للمجموعة الفرعية S: ويُعتبر وسم T_S صالحاً في حال $T_S = \oplus_{j \in S} t_j$، حيث $t_j = F(k_j, m_j)$؛ وإلا يُعتبر وسم T_S غير صالح. وإذا كان وسم T_S صالحاً، يُضبط $J \leftarrow J \setminus S$. ويرسل التحقق نتيجة تفحص وسم T_S (أي معلومات بتة واحدة) إلى التجميع. ثم، يقوم التجميع باختيار مجموعة فرعية أخرى $S' \subseteq ID$، ويقوم بإنشاء وسم مجمع، $T_{S'}$، بضغط وسوم MAC للمجموعة الفرعية S' ويرسل الوسم إلى التحقق. ويتحقق التحقق من صحة $T_{S'}$ باستخدام المفاتيح السرية للمجموعة الفرعية S'. وإذا كان وسم $T_{S'}$ صالحاً، يُضبط $J \leftarrow J \setminus S'$. ويرسل التحقق نتيجة تفحص وسم $T_{S'}$ إلى التجميع. وبعد تكرار الإجراءات المذكورة أعلاه بين التجميع والتحقق، ينتج عن التحقق أخيراً قائمة J التي تتكون من معرفات الأجهزة ذات الرسائل غير الصالحة.



الشكل 3 – بروتوكول تفاعلي بين التجميع والتحقق

2.3.8 الإنشاء القائم على الاختزال

1.2.3.8 إنشاء المفاتيح

لكل معرف، تنشئ هذه العملية مفتاحاً عشوائياً يُشار إليه بالرمز k_{id}.

2.2.3.8 الوسم

يأخذ الوسم كمدخلات رسالة ومعرفاً ومفتاحاً سرياً تطابق المعرف، ويشار إليها بالرموز، id, m, k_{id},، على التوالي، ويُخرج الوسم t لشفرة استيقان الرسالة (MAC)، ويُحسب هذا الوسم بالدالة $F(k_{id}, m)$.

3.2.3.8 التجميع والتحقق

يُنشأ التجميع والتحقق استناداً إلى بروتوكول AGT على النحو الموضح في الشكل 3. ويأخذ التجميع كمدخلات المجموعة الكاملة من المعرفات $ID = \{id_1, id_2, \dots, id_n\}$، والرسائل ووسوم شفرة استيقان الرسالة (MAC) الخاصة بها من أجهزة عددها n، ويشار إليها بالرموز $(m_1, t_1), \dots, (m_n, t_n)$، حيث (m_i, t_i) $(1 \le i \le n)$ هو زوج وسوم رسالة يقابل id_i. ويأخذ التحقق كامل مجموعة المعرفات (ID) وجميع المفاتيح السرية k_i $(1 \le I \le n)$ التي تقابل id_i. فأولاً، يقوم التجميع باختيار مجموعة فرعية $S \subseteq ID$، ويقوم بإنشاء وسم مجمع، T_S، بحساب قيمة الاختزال $T_S = H(t_{j_1}, t_{j_2}, \dots)$ حيث $S = \{id_{j_1}, id_{j_2}, \dots\}$ مع $1 \le j_1 < j_2 < \cdots$. ثم يرسِل التجميع وسم T_S مع الرسائل $(m_1, \dots, m_n)$ إلى التحقق. وبعد ذلك، يضبط التحقق $J = ID$ ويتحقق من صلاحية وسم T_S باستخدام المفاتيح السرية للمجموعة الفرعية S: ويُعتبر وسم T_S صالحاً في حال $T_S = H(t_{j_1}, t_{j_2}, \dots)$، حيث $t_j = F(k_j, m_j)$؛ وإلا يُعتبر وسم T_S غير صالح. وإذا كان وسم T_S صالحاً، يُضبط $J \leftarrow J \setminus S$. ويرسل التحقق نتيجة تفحص وسم T_S (أي معلومات بتة واحدة) إلى التجميع. ثم، يقوم التجميع باختيار مجموعة فرعية أخرى $S' \subseteq ID$، ويقوم بإنشاء وسم مجمع، T_S,، بضغط وسوم MAC للمجموعة الفرعية S' ويرسل الوسم إلى التحقق. ويتحقق التحقق من صحة T_S, باستخدام المفاتيح السرية للمجموعة الفرعية S'. وإذا كان وسم T_S, صالحاً، يُضبط $J \leftarrow J \setminus S'$. ويرسل التحقق نتيجة تفحص وسم T_S, إلى التجميع. وبعد تكرار الإجراءات المذكورة أعلاه بين التجميع والتحقق، ينتج عن التحقق أخيراً قائمة J التي تتكون من معرفات الأجهزة ذات الرسائل غير الصالحة.

الملحق A

الإرشادات والقيود

(يشكل هذا الملحق جزءاً أساسياً من هذه التوصية.)

1.A إرشادات بشأن استخدام استيقان الرسالة المجمَّع (AMA)

تناقش هذه التوصية إمكانية تطبيق دمج عقدة مجمعة في بروتوكولات شفرة استيقان الرسالة (MAC) القائمة دون تغيير أنساق المدخلات أو توصيلات الشبكة لشفرات MAC الأساسية. بالإضافة إلى ذلك، يعتبر التجميع إجراء بدون مفتاح، ولا يحتاج إلى صيانة أي مفتاح سري في عقدة التجميع. علاوةً على ذلك، لا ينفَّذ التجميع إلا بحساب عمليات XOR على مستوى البتات أو دوال الاختزال، وبالتالي فإن مخططي استيقان الرسالة المجمَّع (AMA) في هذه التوصية مناسبان للاستخدام من أجل الاستيقان بطريقة خفيفة.

في معالجة التجميع الموضحة في الفقرة 7، ينعين إنشاء منفصلة بدرجة d وتخزينها. وتُعرف عدة أساليب مثل تلك الموصوفة في المرجع [b-TM05] لتكوين مصفوفات منفصلة بدرجة d، ويمكن أيضاً استخدام شكل مضغوط من مصفوفة منفصلة بدرجة d على النحو الموضح في المرجع [b-MK19]. وتقترح هذه التوصية استخدام هذه التقنيات حتى في مخططي استيقان الرسالة المجمَّع (AMA). وفي مصفوفة منفصلة بدرجة d ذات صفوف عددها u وأعمدة عددها n، يكون مخطط AMA أكثر فعالية من الاستيقان التقليدي الإفرادي في حال $u < n$؛ وأكثر فعالية في حال $d \ll \sqrt{n}$.

ملاحظة – يرد هنا وصف مستويات الأمن لمخططات AMA (أو IAMA) المنشأة بدوال XOR أو الاختزال وفقاً للمخططات الموضحة في المرجعين [b-HS18] و[b-SS19]. وهناك ثلاثة أنواع من المفاهيم الأمنية هي، الحصانة ضد التزوير، واكتمال إمكانية التعرف وسلامة (أو تضعضع) إمكانية التعرف: وتضمن الحصانة ضد التزوير عدم تزييف أي رسالة؛ ويضمن اكتمال قابلية التعرف حكم المخطط على أي رسالة صالحة بأنها صالحة؛ وتضمن سلامة إمكانية التعرف حكم المخطط على أي رسالة غير صالحة بأنها غير صالحة؛ وفي حين أن مؤدى تضعضع سلامة إمكانية التعرف هو نفس مؤدى سلامة إمكانية التعرف إلا أنه يُفترض أن يمنع الخصم من الحصول على وسوم MAC صالحة وألا يفسد أي أجهزة قبل الهجوم. ويظل تضعضع السلامة مفيداً في التطبيقات، لأنه يغطي التلاعب بالرسالة.

ويرد وصف مستويات الأمن لمخططات AMA (أو IAMA) في هذه التوصية على النحو التالي. ويفي الإنشاء القائم على XOR بالحصانة ضد التزوير واكتمال إمكانية التعرف وسلامة –أو تضعضع– إمكانية التعرف إذا أوفت شفرة MAC الأساسية بالحصانة ضد التزوير. ويفي الإنشاء القائم على الاختزال بالحصانة ضد التزوير واكتمال إمكانية التعرف وسلامة إمكانية التعرف إذا أوفت شفرة MAC الأساسية بالحصانة ضد التزوير واعتُبرت دالة الاختزال دالة عشوائية.

2.A قيود استخدام استيقان الرسالة المجمَّع (AMA)

تفترض هذه التوصية أن عدد الرسائل غير الصالحة لا يتجاوز d في مخططي استيقان الرسالة المجمَّع (AMA)، وتُضبط هذه المعلمة كمعلمة نظام. هذا يعني أن هناك حاجة لتقدير العدد d مقدماً.

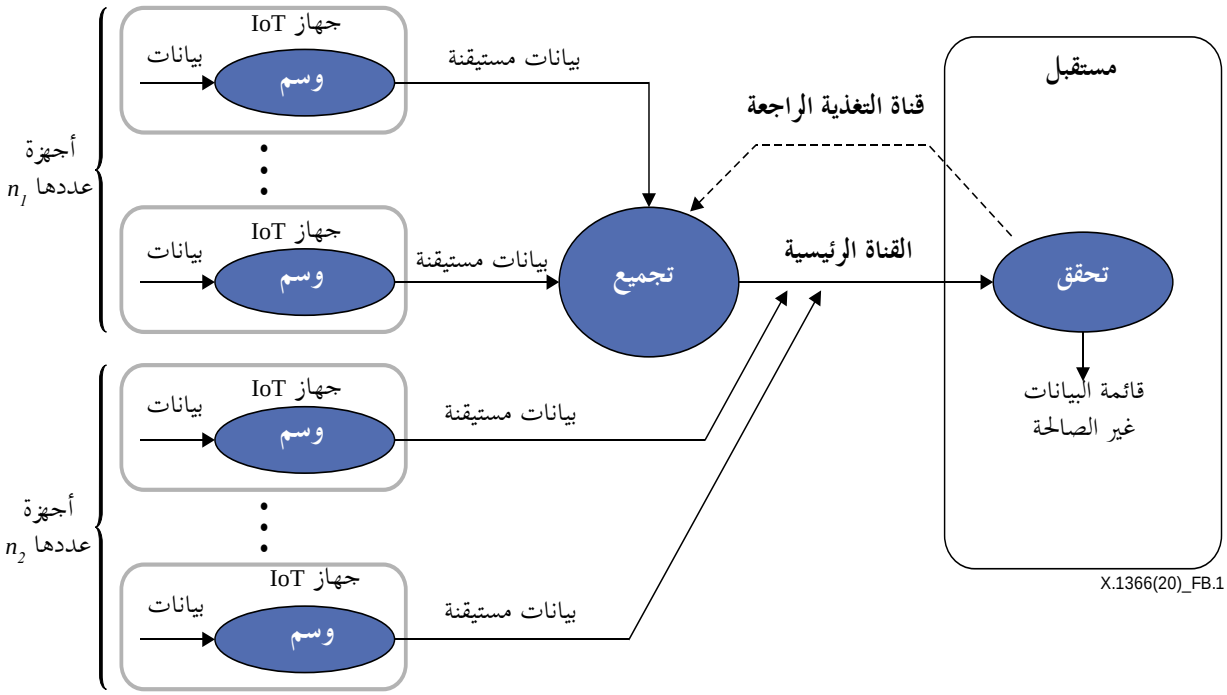
فماذا يحدث إذا تجاوز عدد الرسائل غير الصالحة القيمة d المفترضة؟ في هذه الحالة، ينتج عن التحقق أخيراً قائمة J التي تحتوي على معرفات أجهزة عددها أكثر من d؛ وتُدرَج معرفات الأجهزة التي أرسلت رسالة غير صالحة في القائمة J؛ ولكن، قد تُدرَج أيضاً بعض معرّفات الأجهزة التي لم ترسل رسالة غير صالحة في القائمة J. في هذه الحالة، يوصى بإعداد قيمة أكبر لمخطط AMA مرة أخرى.

الملحق B

الدمج مع بروتوكولات الاستيقان الإفرادية القائمة

(يشكل هذا الملحق جزءاً أساسياً من هذه التوصية.)

يمكن استخدام مخططات AMA (أو IAMA) في هذه التوصية بالاقتران مع الاستيقان التقليدي الإفرادي. ويُفهم الاستيقان التقليدي الإفرادي على أنه مخطط AMA تكون فيه مصفوفة الفصل الأساسية هي مصفوفة الهوية. وفي أجهزة عددها $n = n_1 + n_2$، إذا فُصل الاكتفاء بتجميع وسوم MAC عددها n_1 من بين وسوم MAC عددها n، يجرى ما يلي: يطبَّق مخطط AMA (أو IAMA) على الأجهزة التي يبلغ عددها n_1 ويطبَّق الاستيقان الإفرادي على الأجهزة الأخرى التي يبلغ عددها n_2 على النحو الموضح في الشكل 1.B.



الشكل 1.B – الدمج مع بروتوكولات الاستيقان الإفرادية

التذييل I

حالات استخدام استيقان الرسالة المجمَّع (AMA)

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

1.I مقدمة

مخططا استيقان الرسالة المجمَّع كلاهما يمكن تطبيقه من أجل ضمان "استيقان (هوية) الكيان" علاوةً على "استيقان الرسالة". وهذان المخططان قد يكونان غير قابلين للتطبيق في جميع حالات الاستعمال الخاصة باستخدام أجهزة إنترنت الأشياء (IoT)، ولكنهما فعّالان ومناسبان تماماً لحالات الاستعمال في ظل الظروف التالية، عندما:

- يُتطلب استيقان الرسالة لأعداد من أجهزة إنترنت الأشياء تتراوح بين العشرات وعشرات الآلاف.
- يتم التعامل مع البيانات/الرسالة من أجل عملية استيقان تحدث كثيراً وبصورة متقطعة.

وفيما يلي أمثلة على التطبيقات التي يمكن افتراض أنها على وجه التحديد ستستخدم تكنولوجيا الاستيقان المجمَّع:

أ) تطبيقات لإرسال البيانات/الرسائل بشكل موجز ومتكرر مثل بيانات شبه الأفلام (صور ثابتة)

- تطبيقات المراقبة باستخدام بيانات الصورة

ب) تطبيقات القياس عن بُعد:

- تطبيقات مراقبة عمليات المصنع
- تطبيقات استطلاع حراك الجمهور
- تطبيقات مراقبة الصحة كماراثون المواطنين على سبيل المثال
- تطبيقات إدارة المرافق مثل أضواء الشوارع المثبتة في المناطق الحضرية
- تطبيقات مراقبة حركة المرور
- تطبيقات مراقبة مستوى مياه النهر

وبتطبيق تكنولوجيا الاستيقان المجمَّع هذه في تطبيقات إنترنت الأشياء المذكورة أعلاه، يمكن تحسين كفاءة إرسال الرسالة ومعالجة الاستيقان في كامل نظام إنترنت الأشياء تحسيناً كبيراً.

وفي حالات الاستخدام التالية أمثلة لاستخدام مخطط الاستيقان المجمع الموصَّف في هذه التوصية.

2.I حالة الاستخدام 1: مدن الملاهي ومراكز الترفيه

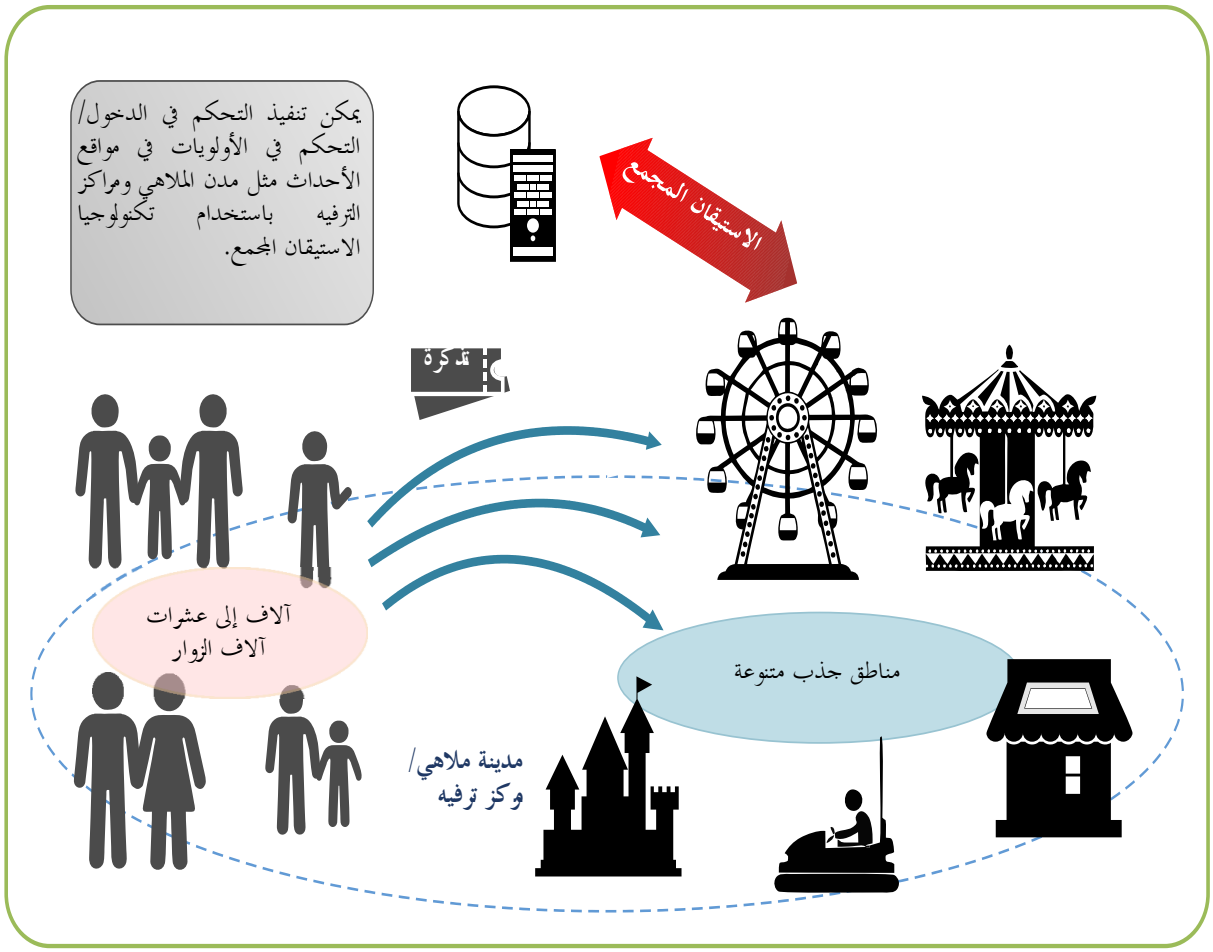
في حالة المتنزهات ومراكز الترفيه وما إلى ذلك، يمكن افتراض وجود ما بين 000 1 إلى 000 10 زائر في نفس الوقت. وهذا يعني أن الحاجة قد تدعو إلى التحقق في نفس الوقت من آلاف الزوار ممن لديهم امتيازات مناسبة لاستخدام مناطق الجذب في المنتزه/المركز. وفي هذه الحالة، يمكن أن يكون نظام الاستيقان المجمع مناسباً تماماً للقيام بإدارة التخويل بكفاءة. وعلى النحو الموضح في الشكل 1.I، يمكن أن تكون المخدِّمات المجمعة في كل منشأة جذب لجمع وتجميع وسوم الاستيقان من أجل طلب التحقق من مخدِّم الاستيقان الخلفي.

وبعبارة أدق، يشتري الزائرون مسبقاً تذكرة دخول تضمَّن فيها دمجاً في رقائق سيليكونية معلومات عن إمكانية النفاذ إلى أحداث، ومعالم سياحية، وخدمات الإنترنت التي ستقدَّم. وتُستخدم هذه التكنولوجيا على نطاق واسع في سباقات الماراثون. ويمكن أيضاً اعتبار أساور المعصم ذات الرقائق المدمجة بديلاً من تذاكر الدخول.

وفي بوابة موقع الحدث الرئيسية أو عند فرادي بوابات كل معلم سياحي، تُقرأ محتويات تذكرة الدخول وتجمَّع باستخدام تكنولوجيا الاستيقان المجمع وترسَل إلى مخدِّم الاستيقان المجمع.

ويقوم مركز مخدِّم الاستيقان المجمع بتحليل محتويات ومتطلبات الخدمة المقدمة للزوار، وبإبلاغ أماكن الجذب المختلفة ومقدمي خدمات الإنترنت، وباستخدامها لتحليل الازدحام والتنبؤ به.

وبعد التحقق، يمكن للزوار الاستفادة من مختلف خدمات الإنترنت المسجلة باستخدام هواتفهم الذكية أو الأجهزة القابلة للارتداء من نوع النظارات على سبيل المثال.



X.1366(20)_FI.

الشكل 1.I – مخطط الاستيقان المجمَّع في مدن الملاهي ومراكز الترفيه

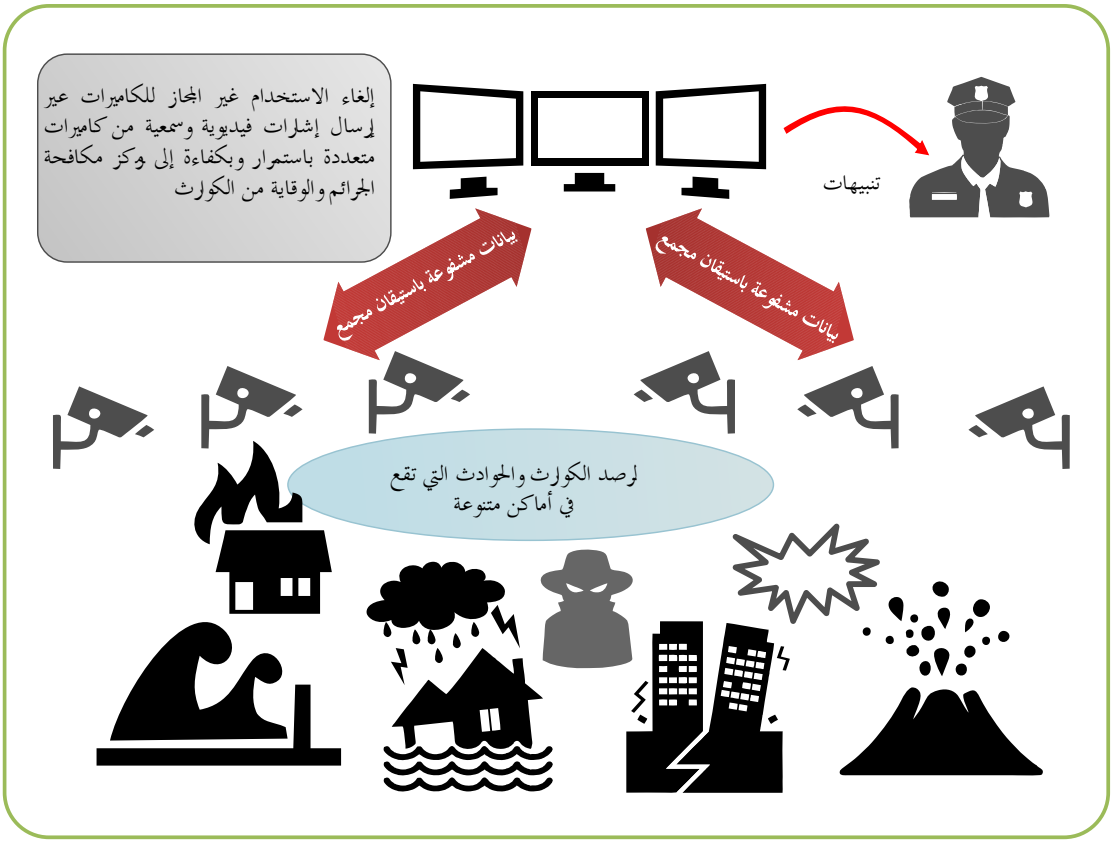
3.I حالة الاستخدام 2: أجهزة استشعار الرقابة

1.3.I اعتبارات عامة

يمكن أن تكون مراقبة الأنشطة باستخدام أجهزة استشعار الرقابة مثل الكاميرات في أجهزة إنترنت الأشياء حالة استخدام لمخططات الاستيقان المجمع التي تقدمها هذه التوصية، من أجل التنبه والتدخل في مرحلة مبكرة من الكوارث الطبيعية والحوادث/الأحداث. وفي هذه الحالة، ترسَل صور شبه فيديوية أو صور ثابتة تُلتقط بواسطة عدد من كاميرات الرقابة إلى مركز مراقبة في الوقت الفعلي تقريباً (أو بشكل دوري) ولكن من المهم ضمان موثوقية وسلامة البيانات التي ترسَل.

ولكن عندما يرتفع عدد أجهزة استشعار الرقابة كثيراً، تنعدم كفاءة التحقق من شفرة الاستيقان في بيانات الصورة من كل كاميرا بالتحقق من شفرة الاستيقان لكل كاميرا – واحدةً تلو الأخرى. وفي مثل هذه البيئة، تظهر فعالية مخطط الاستيقان المجمع. ويمكن تجميع شفرات الاستيقان مع البيانات في المخدِّمات المجمعة قبل إرسالها إلى مركز الرقابة، كي يتمكن نظام إنترنت الأشياء كله من

تقديم استيقان واتصالات بكفاءة. ويعتمد عدد مخدِّمات التجميع على عدد أجهزة استشعار الرقابة. ويوضح الشكل 2.I أجهزة استشعار الرقابة في مخطط الاستيقان المجمَّع.



X.1366(20)_FI.2

الشكل 2.I – أجهزة استشعار الرقابة في مخطط الاستيقان المجمَّع

2.3.I حالات الاستخدام المحددة

1) مراقبة البيئات المعيشية مثل المجتمعات المحلية والسكنية

تجمَّع معلومات بيئة المعيشة من أجهزة استشعار متنوعة مثل كاميرات الرقابة المرفقة بمباني الكتل السكنية، والمجتمعات الذكية، والمنازل الخاصة، وما إلى ذلك عند بوابة (مركز إنترنت الأشياء) وترسَل إلى مخدِّم مركزي باستخدام تكنولوجيا الاستيقان المجمَّع.

وسيقوم المركز بتحليل المعلومات الواردة، وباستخدامها للمساعدة في مراقبة البيئة المعيشية، والتنبؤ بالاختلالات والأعطال، والاستجابة الفورية، ومنع وقوع الجريمة والكوارث.

وبعبارة أدق، فإن البيانات التي تُلتقط في مختلف أجهزة الاستشعار البيئية وأجهزة استشعار الأجهزة المنزلية وكاميرات الرقابة وأجهزة استشعار حالة فتح/غلق الباب/النافذة وأجهزة استشعار حالة تشغيل البنية التحتية للغاز/الماء/الكهرباء وأجهزة استشعار مراقبة المصعد وما إلى ذلك، ترسَل إلى مراكز خارجية. وتُعتبر مخططات الاستيقان المجمَّع التي تستخدم استيقان المطراف واستيقان البيانات مخططات فعالة كوسيلة للاستيقان من أجل جمع كميات متنوعة وكبيرة من البيانات وإرسال البيانات بكفاءة.

2) صيانة ومراقبة البنية التحتية الاجتماعية والاستجابة للكوارث

يجري إدخال صيانة وإدارة البنية التحتية الاجتماعية مثل الجسور والأنفاق والطرق التي تستخدم إنترنت الأشياء في مجالات مختلفة، ويُتوقع على نطاق واسع أن تؤدي خدمات إنترنت الأشياء دوراً بالغ الأهمية في تحقيق مجتمع سالم وآمن في المستقبل القريب. فعلى سبيل المثال، تُلتقط، في حالات الجسور المتقادمة والطرق المرتفعة، بيانات ذات صلة بأمور مثل الإجهادات والاهتزازات والإزاحة والميل وما إلى ذلك، ومعلومات فيديوية مفصَّلة بواسطة أجهزة استشعار مختلفة. ويصبح حجم البيانات التي ينبغي إرسالها إلى المركز كبيراً للغاية.

وفي الوقت الحالي، أثبت أسلوب الاستيقان المجمع فعاليته الكبيرة كأحد التدابير المستخدمة لتحسين كفاءة استخدام دائرة الإنترنت اللاسلكية وتجنب الازدحام. وبالإضافة إلى صيانة هذه البنى التحتية الاجتماعية وإدارتها، يمكن أيضاً تطبيق أسلوب الاستيقان المجمَّع على بوابة نظام إنترنت الأشياء لاستخدام الأنظمة من أجل المراقبة المستمرة لمستويات المياه وتغيرات التدفق في الأنهار والبحيرات في البيئات الزراعية.

3) أنظمة الوقاية من الكوارث باستخدام كاميرات الرقابة

تركَّب كاميرات الرقابة وتشغَّل لأغراض مختلفة بما في ذلك منع الجريمة والوقاية من الكوارث في أماكن مختلفة في جميع أنحاء العالم. وبوجه عام، تقتضي الضرورة، في شبكة تتعامل مع معلومات الصورة والصوت، أن ترسَل كمية كبيرة من البيانات باستمرار إلى الجانب المركزي، وتُتوخى الفعالية في تطبيق تقنية الاستيقان المجمَّع من أجل الإرسال الكفء. أي يمكن تحسين كفاءة الاتصالات بين جهاز إنترنت الأشياء وبوابة إنترنت الأشياء وبين بوابة إنترنت الأشياء والمركز بتطبيق أسلوب الاستيقان المجمَّع.

4) مراقبة الأعمال اللوجيستية وتحسين كفاءة أنظمة النقل

تُستخدم أنظمة إنترنت الأشياء في أنظمة الأعمال اللوجستية والنقل بشكل متزايد لتحسين الكفاءة والخواص الوظيفية العالية لمصالح الأعمال. فعلى سبيل المثال، يُستخدم الحل الذي يدير بدقة معلومات حالة السلع والحزم من مرحلة الشحن حتى مرحلة التسليم استخداماً عملياً في مختلف المجالات. وفي مثل هذا النظام، يمكن تحقيق إدارة لوجستية أكثر استقراراً وكفاءة من خلال تطبيق تكنولوجيا الاستيقان المجمَّع على النظام الذي يرسل معلومات أجهزة الاستشعار المختلفة عن جميع الحزم إلى المركز. ويمكن أيضاً تصور تقديم بوابة إنترنت الأشياء لمركبات مثل السيارات المجهزة بعدد هائل من أجهزة الاستشعار وتطبيق تكنولوجيا الاستيقان المجمَّع في بوابة المركبة لأنظمة النقل.

التذييل II

الأنشطة ذات الصلة بمخططي استيقان الرسالة المجمَّع (AMA)

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

اقترح كاتز وليندل لأول مرة في المرجع [b-KL08] مخطط AMA يختلف عن المخطط الموضح في الفقرة 7، وهو يسمح بتجميع العديد من وسوم MAC لرسائل متعددة في وسم أقصر. وعلى وجه التحديد، قام كاتز وليندل في المرجع [b-KL08] بإضفاء الطابع الرسمي على نموذج وأمن AMA، وقدما إنشاء AMA البسيط باتباع عملية XOR على مستوى البتات لجميع وسوم MAC. ويمكن التحقق من صحة رسائل متعددة بوسم واحد أقصر فقط، ولكن يستحيل عموماً تحديد الرسالة غير الصالحة في مخطط AMA الخاص بهما بمجرد اعتبار رسائل متعددة غير صالحة بالنسبة على الوسم الواحد. ويحقق مخططا AMA في هذه التوصية الخواص الوظيفية لتجميع عدة وسوم MAC في وسم أقصر وكذلك تحديد الرسائل غير الصالحة منها. وتستند شفرة AMA الواردة في الفقرة 7 من هذه التوصية إلى المرجع [b-HS18]، بينما يستند بروتوكول الاستيقان التفاعلي لاستخدام استيقان الرسالة المجمَّع (AMA) الوارد في الفقرة 8 إلى المرجع [b-SS19].

التذييل III

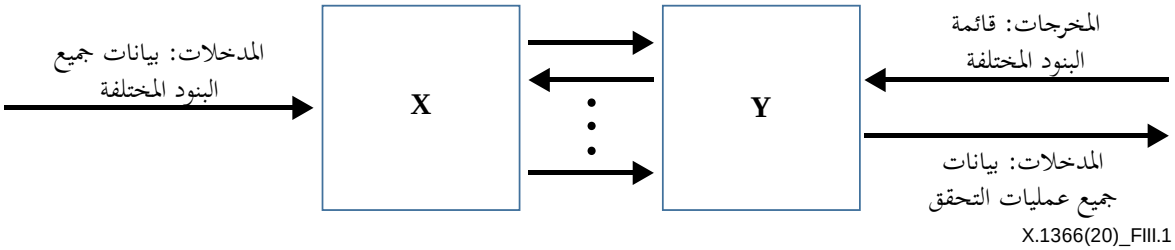
بروتوكول اختبار الزمرة التكيفي

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

إن بروتوكول اختبار الزمرة التكيفي، كما ورد بحثه في المرجع [b-DH00]، هو أسلوب لتحديد بنود خاصة تسمى البنود المختلة بين عدد كبير من البنود الكاملة باستخدام عدد صغير من الاختبارات بدلاً من إجراء اختبار فردي لكل بند.

وفي المثال التالي لبروتوكول الاختبار الزمرة الموضح في الشكل 1.III، يُفترض أن هناك بنوداً مختلة d عددها الإجمالي n.

وفي اختبار الزمرة التكيفي، يمكن إجراء الاختبارات عدة مرات بحيث يمكن اختيار مجموعة فرعية من البنود المراد اختبارها بعد ملاحظة نتائج الاختبار السابق. واختبار الزمرة التنافسي هو اختبار زمرة تكيفي لا يحتاج إلى معرفة عدد البنود المختلة d مسبقاً.



الشكل 1.III – بروتوكول اختبار الزمرة التكيفي

ومن الناحية الرسمية، يعد اختبار الزمرة التكيفي بروتوكولاً تفاعلياً بين X وY على النحو الموضح في الشكل 1.III.

ويأخذ X المجموعة الكاملة من المعرفات $ID = \{id_1, id_2, \ldots, id_n\}$ وجميع بيانات البنود $(1 \le i \le n)$ التي تقابل id_i. ويأخذ Y المجموعة الكاملة من المعرفات (ID) وجميع بيانات التحقق ans_i $(1 \le i \le n)$ التي تقابل id_i. فأولاً، يختار X مجموعة فرعية $S \subseteq ID$، وينشئ الاختبار test_S بضغط بيانات البنود S، ويرسل test_S إلى Y. ثم يقوم Y بضبط $J = ID$ ويتحقق من صحة الاختبار test_S باستخدام بيانات التحقق من المجموعة الفرعية S. فإذا كان الاختبار test_S صالحاً، يُضبط $J \leftarrow J \setminus S$. ويرسل Y نتيجة الاختبار test_S (أي معلومات بتة واحدة) إلى X. ثم يختار X مجموعة فرعية أخرى من المعرّفات، ويكرر الإجراءات بين X وY. وبعد تكرار الإجراءات المذكورة أعلاه بين X وY، يُخرج Y أخيراً القائمة J التي تتكون من معرفات البنود المختلة.

فعلى سبيل المثال، تتضمن بروتوكولات اختبار الزمرة التكيفي البحث الاثنيني، وخوارزمية التمشيط والغربلة (rake-and-winnow) [b-EGH07]، وخوارزمية Li متعددة المراحل [b-Li62]، وخوارزمية الحفر الموضحة في الفقرة 6.4 من المرجع [b-DH00].

بيبليوغرافيا

[b-ITU-T X.813] Recommendation ITU-T X.813 (1996), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*.

[b-DH00] D. Z. Du and F. K. Hwang, *Combinatorial Group Testing and Its Applications*, Series on Applied Mathematics, vol. 12, 2nd edn. World Scientific, Singapore, 2000.

[b-EGH07] D. Eppstein, M. T. Goodrich, and D. S. Hirschberg, *Improved Combinatorial Group Testing Algorithms for Real-world Problem Sizes*, SIAM J. Comput. 36(5), pp. 1360-1375, 2007.

[b-HS18] S. Hirose and J. Shikata, *Non-adaptive Group-Testing Aggregate MAC Schemes*, The 14th International Conference on Information Security Practice and Experience (ISPEC 2018), LNCS 11125, pp. 357-372, Springer, 2018.

[b-KL08] J. Katz and A.Y. Lindell, *Aggregate message authentication codes*, CT-RSA 2008, LNCS 4964, pp. 155-169. Springer, 2008.

[b-Li62] C. H. Li, *A Sequential Method for Screening Experimental Variables*, J. Am. Stat. Assoc. 57 (298), pp. 455-477, 1962.

[b-MK19] K. Minematsu and N. Kamiya, *Symmetric-key Corruption Detection: When XOR-MACs meet combinatorial group testing*, ESORICS 2019, Part I, LNCS 11735, pp. 595-615, Springer, 2019.

[b-MOV96] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, October 1996, Fifth Printing (August 2001).

[b-SS19] S. Sato and J. Shikata, *Interactive Aggregate Message Authentication Scheme with Detecting Functionality*, The 33rd International Conference on Advanced Information Networking and Applications (AINA-2019), pp. 1316-1328, Springer, 2019.

[b-TM05] N. Thierry-Mieg, *A New Pooling Strategy for High-throughput Screening: the Shifted Transversal Design, BMC Bioinformatics*, vol. 7, no. 28, 2005.

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، 2021