الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1372

(2020/03)

السلسلة X: شبكات البيانات والاتصالات،
بين الأنظمة المفتوحة ومسائل الأمن

تطبيقات وخدمات آمنة (2) – أمن أنظمة النقل الذكية (ITS)

المبادئ التوجيهية للسلامة من أجل الاتصالات من مركبة إلى كل شيء (V2X)

التوصية ITU-T X.1372

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 على 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
المولد الكمومي للأعداد العشوائية	X.1702–X.1709
إطار أمن شبكات توزيع المفاتيح الكمومية (QKDN)	X.1710–X.1711
التصميم الأمني للشبكات QKDN	X.1712–X.1719
التقنيات الأمنية للشبكات QKDN	X.1720–X.1729
أمن البيانات	
أمن البيانات الضخمة	X.1750–X.1759
أمن الجيل الخامس	X.1800–X.1819

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

التوصية ITU-T X.1372

المبادئ التوجيهية للسلامة من أجل الاتصالات من مركبة إلى كل شيء (V2X)

ملخص

تقدم التوصية ITU-T X.1372 مبادئ توجيهية بشأن سلامة الاتصالات من مركبة إلى كل شيء (V2X). وهذا المختصر هو مصطلح عمومي لأنماط الاتصالات، التي يطلق عليها اسم الاتصالات من مركبة إلى مركبة (V2V) ومن مركبة إلى بنية تحتية (V2I) ومن مركبة إلى أجهزة جوالة (V2D) ومن مركبة إلى مشاة (V2P)، التي تُبحث في هذه التوصية.

لقد حدثت تطورات هامة طوال السنوات القليلة الماضية في مجال الاتصالات على متن المركبات في بيئة أنظمة النقل الذكية (ITS). ومن شأن الاتصالات من مركبة إلى كل شيء أن تعمل على تحسين السلامة على الطرق إلى حد كبير وأن تقلل من ازدحام حركة المرور وأن تعزز أسباب الراحة. ولكن من شأن هذه الاتصالات V2X أيضاً أن تعرّض الكيانات ذات الصلة في بيئة أنظمة النقل الذكية لمختلف أشكال الهجمات السيبرانية.

وتصدياً لمشكلة السلامة هذه، تتناول هذه التوصية التهديدات الكامنة في بيئات الاتصالات V2X وتحدد متطلبات السلامة لهذه الاتصالات بغية التخفيف من آثار هذه التهديدات. وتقدم هذه التوصية أيضاً وصفاً للتنفيذ المحتمل للاتصالات V2X الآمنة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1372	2020-03-26	17	11.1002/1000/14091

مصطلحات أساسية

سلامة أنظمة النقل الذكية، تحليل المخاطر، متطلبات السلامة، تحليل التهديدات، الاتصالات من مركبة إلى بنية تحتية، الاتصالات من مركبة إلى مركبة، الاتصالات من مركبة إلى أجهزة جوالة، الاتصالات من مركبة إلى مشاة، الاتصالات من مركبة إلى كل شيء.

* 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، كان 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

الصفحة

التوصية ITU-T X.1372

المبادئ التوجيهية للسلامة من أجل الاتصالات من مركبة إلى كل شيء (V2X)

1 مجال التطبيق

تقدم هذه التوصية مبادئ توجيهية بشأن سلامة الاتصالات من مركبة إلى كل شيء (V2X). وهذا المختصر، V2X، هو مصطلح عمومي لأنماط الاتصالات، التي يطلق عليها اسم الاتصالات من مركبة إلى مركبة (V2V) ومن مركبة إلى بنية تحتية (V2I) ومن مركبة إلى أجهزة جوالة (V2D) ومن مركبة إلى مشاة (V2P)، التي تُبحث في هذه التوصية. وتتناول هذه التوصية التهديدات الكامنة في بيئة الاتصالات V2X وتحدد متطلبات السلامة وتقدم وصفاً للتنفيذ المحتمل للاتصالات V2X الآمنة.

أما الضوابط الأمنية المحددة للاتصالات V2X فتقع خارج نطاق 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 التعاريف التالية المعرّفة في مكان آخر:

1.1.3 المساءلة (accountability) [b-ITU-T X.800]: خاصية تضمن أن أعمال كيان ما يمكن إسنادها إلى ذلك الكيان حصراً.

2.1.3 الاستيقانية (authenticity) [b-ITU-T X.641]: حماية من أجل الاستيقان المتبادل واستيقان أصل البيانات.

3.1.3 الاستيقان (authentication) [b-ITU-T X.1252]: عملية تستعمل لتحقيق قدر كاف من الثقة في الربط بين الكيان والهوية المقدمة.

ملاحظة – يؤخذ استعمال مصطلح استيقان في سياق إدارة الهوية (IdM) على أنه يعني استيقان كيان.

4.1.3 الترخيص (authorization) [b-ITU-T X.800]: منح الحقوق، الذي يتضمن إتاحة النفاذ استناداً إلى حقوق النفاذ.

5.1.3 التيسر (availability) [b-ITU-T X.800]: خاصية إمكانية النفاذ وإمكانية الاستعمال بناءً على طلب من كيان مرخص له.

6.1.3 سلطة الترخيص (certification authority (CA)) [b-ITU-T X.509]: جهة موثوق بها من جانب كيان أو أكثر لاستحداث شهادات المفاتيح العمومية والتوقيع رقمياً عليها. ويمكن، خيارياً، لسلطة الترخيص أن تستحدث المفاتيح المطلوبة.

7.1.3 الخصوصية (confidentiality) [b-ITU-T X.800]: خاصية عدم إتاحة المعلومات أو الكشف عنها لأشخاص غير مرخص لهم أو لكيانات أو عمليات غير مرخص لها.

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

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

10.1.3 جهاز جوال (nomadic device) (ND) [b-ITU-T F.749.1]: تشمل الأجهزة الجوالة جميع أنواع أجهزة المعلومات والاتصالات بالإضافة إلى أجهزة الترفيه التي يمكن للسائق و/أو الركاب نقلها إلى المركبة لاستخدامها أثناء القيادة. ومن الأمثلة على ذلك الهواتف المتنقلة والحواسيب والألواح المحمولة وأجهزة الملاحة المحمولة ومشغلات الوسائط المحمولة والهواتف الذكية متعددة الوظائف.

11.1.3 عدم التنصل بإثبات المصدر (non-repudiation with proof of origin) [b-ITU-T X.800]: يزوَّد متلقي البيانات بإثبات منشأ هذه البيانات. ويحمي ذلك من أي محاولة من جانب المرسل لأن ينكر زوراً إرسال البيانات أو محتوياتها.

12.1.3 استعارة الأسماء (pseudonym) [b-ITU-T X.1252]: معرّف هوية لا يُعرف إسناده إلى كيان، أو يُعرف على نطاق ضيق فقط في السياق الذي يُستعمل من أجله.

ملاحظة – يمكن استعمال الاسم المستعار لتفادي أو التقليل من المخاطر المتعلقة بالخصوصية المرتبطة باستعمال إسنادات معرف الهوية التي يمكن أن تكشف عن هوية الكيان.

13.1.3 شهادة مفتاح عمومي (public-key certificate) (PKC) [b-ITU-T X.509]: مفتاح عمومي لكيان ما، مصحوباً ببعض المعلومات الأخرى، يصبح غير قابل للتزوير بفضل التوقيع الرقمي مع المفتاح الخاص الصادر عن سلطة إصدار الشهادات.

2.3 مصطلحات معرّفة في هذه التوصية

تعرّف هذه التوصية المصطلح التالي:

1.2.3 سوء السلوك (misbehaviour): السلوك الذي يجعل الأجهزة ترسل معلومات خاطئة قد تؤدي إلى قيام أجهزة أخرى باتخاذ إجراءات غير صحيحة، أو الذي يجعل الأجهزة تتخذ الإجراء الخاطئ على الرغم من تلقي المعلومات الصحيحة.

4 المختصرات

تستخدم هذه التوصية المختصرات التالية:

AES معيار تجفير متقدم *(Advanced Encryption Standard)*

AVN صوت وفيديو وملاحة *(Audio, Video, and Navigation)*

CA سلطة إصدار الشهادات *(Certification Authority)*

CAMP شراكة قياسات تجنب الاصطدام *(Crash Avoidance Metrics Partnership)*

CCM أسلوب معاكس مع شفرة استيقان من رسالة تسلسل كتل التجفير
(Counter mode with cipher block chaining message authentication code)

CCU وحدة الاتصالات المركزية *(Central Communication Unit)*

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

EEBL ضوء كابح إلكتروني في حالة الطوارئ *(Electronic Emergency Brake Light)*

ECDSA خوارزمية توقيع رقمي بمنحنى إهليلجي *(Elliptic Curve Digital Signature Algorithm)*

ECIES مخطط تجفير مدمج بمنحنى إهليلجي *(Elliptic Curve Integrated Encryption Scheme)*

ECU وحدة تحكم إلكتروني *(Electronic Control Unit)*

GPS النظام العالمي لتحديد الموقع *(Global Positioning System)*

HDMI واجهة متعددة الوسائط عالية الوضوح *(High-Definition Multimedia Interface)*

ID معرّف الهوية *(Identifier)*

ITS نظام النقل الذكي *(Intelligent Transportation System)*

IVN شبكة داخل المركبة *(In-Vehicle Network)*

KDF وظيفة اشتقاق المفاتيح *(Key Derivation Function)*

LDM خارطة دينامية محلية *(Local Dynamic Map)*

LOS خط البصر *(Line Of Sight)*

LTE التطور طويل الأجل *(Long Term Evolution)*

MAC شفرة استيقان الرسائل *(Message Authentication Code)*

MHL وصلة عالية الوضوح متنقلة *(Mobile High-definition Link)*

NFC اتصالات المجال القريب *(Near Field Communication)*

NGN شبكات الجيل التالي *(Next Generation Networks)*

NLOS خارج خط البصر *(Non-Line Of Sight)*

OBD نظام التشخيص على متن مركبة *(On Board Diagnostics)*

OBU وحدة على متن مركبة *(On-Board Unit)*

PII المعلومات المحدِّدة لهوية الشخص *(Personally Identifiable Information)*

PKI البنية التحتية للمفاتيح العمومية *(Public-Key Infrastructure)*

QoS جودة الخدمة *(Quality of Service)*

RSU وحدة بجانب الطريق *(Road-Side Unit)*

SCMS نظام إدارة بيانات اعتماد الأمن *(Security Credential Management System)*

SHA خوارزمية البعثرة الآمنة *(Secure Hash Algorithm)*

USB ناقل عمومي بالتسلسل *(Universal Serial Bus)*

V2I من المركبة إلى البنية التحتية *(Vehicle-to-Infrastructure)*

V2D من المركبة إلى جهاز جوال *(Vehicle-to-nomadic Device)*

V2P من المركبة إلى المشاة *(Vehicle-to-Pedestrian)*

V2V من مركبة إلى مركبة *(Vehicle-to-Vehicle)*

V2X من المركبة إلى كل شيء *(Vehicle-to-everything)*

VGP منصة بوابة المركبات *(Vehicle Gateway Platform)*

VRU مستعمل الطريق المستضعَف *(Vulnerable Road User)*

WAVE النفاذ اللاسلكي في بيئة المركبات *(Wireless Access in Vehicular Environments)*

WiFi الأمانة اللاسلكية *(Wireless Fidelity)*

5 الاصطلاحات

لا توجد.

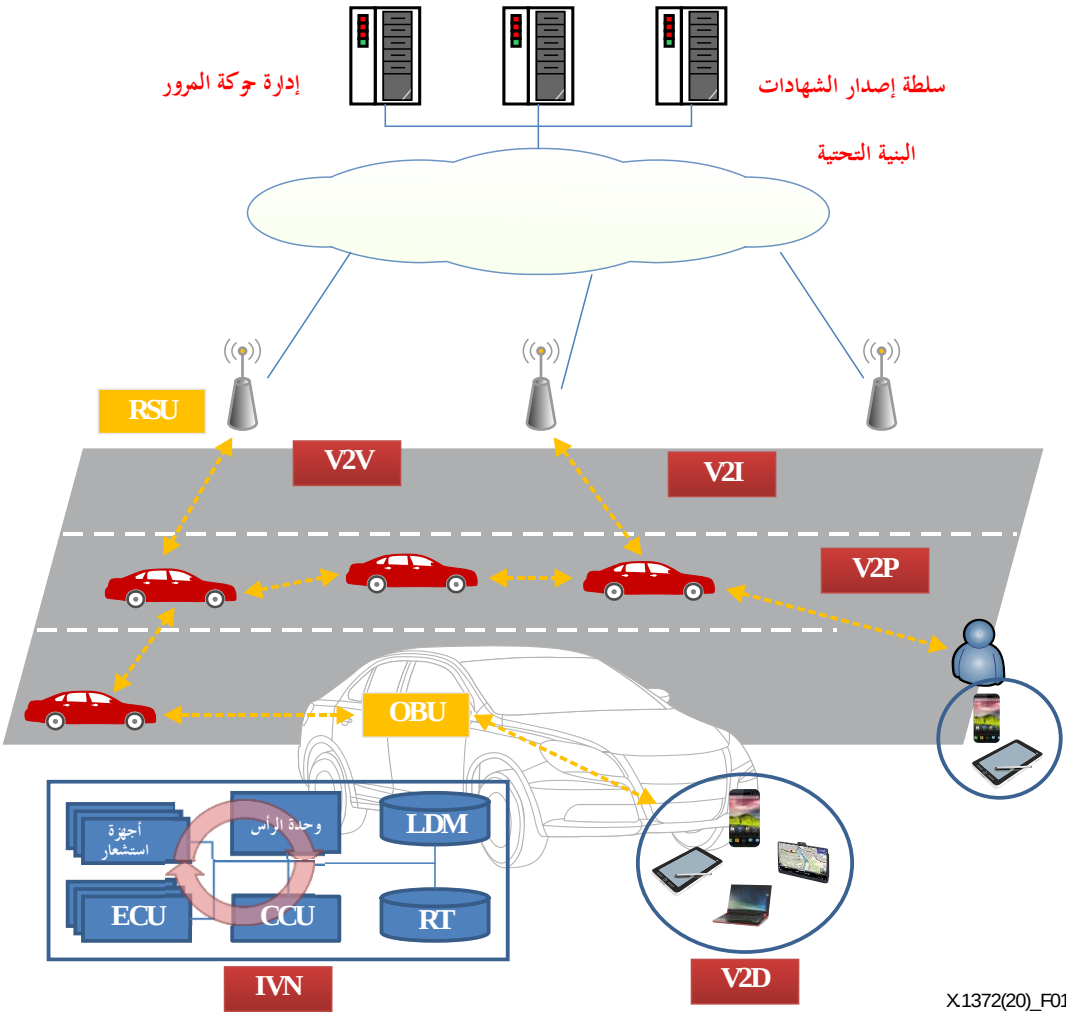
6 الاتصالات من مركبة إلى كل شيء

1.6 نظرة عامة

تتضمن أنظمة النقل الذكية (ITS) طائفة واسعة من تقنيات المعلومات والاتصالات تتوخى تحسين سلامة وكفاءة نظام النقل. وقد شهدت السنوات القليلة الماضية تطورات هامة في هذا الشأن، لاسيما فيما يتعلق بأنظمة الاتصالات بين المركبات.

وتدعم أنظمة اتصالات المركبات تبادل البيانات بين المركبات وبين المركبة والبنية التحتية وبين المركبات والأجهزة الجوالة. وتشمل أنماط البيانات أشياء من قبيل الموقع الراهن وسرعة المركبة والتحذيرات المستمدة من أجهزة الاستشعار على متن المركبة. وبالإضافة إلى ذلك، يمكن للوحدات الموجودة على جانب الطريق (RSU) أن توفر وصلات اتصال بأنظمة مراقبة حركة المرور التي تجمع وتوزع التحذيرات بخصوص أحوال الخطر بين المركبات المجاورة. ولكن إذا لم تتوفر أسباب الحماية الأمنة فقد تشكل أنظمة النقل الذكية خطراً على سلامة حركة المرور، بل قد تشكل خطراً على حياة الإنسان. لذلك يجري تقصي جوانب الأمن في أنظمة النقل الذكية حرصاً على نجاح نشر هذه الأنظمة بطريقة آمنة.

الشكل 1 هو عبارة عن نظرة عامة على الاتصالات بين المركبات. ويمكن تصنيف اتصالات المركبات إلى اتصالات خارج المركبة واتصالات داخل المركبة. وتتضمن الشبكة الداخلية في مركبة ما، المعروفة باسم الشبكة داخل المركبة (IVN)، مكونات المركبة مثل أجهزة الاستشعار ووحدات التحكم الإلكتروني (ECU). ويمكن تصنيف الاتصالات خارج المركبة إلى اتصالات من مركبة إلى أخرى ومن مركبة إلى بنية تحتية ومن مركبة إلى جهاز جوال ومن مركبة إلى مشاة. والوحدات على متن المركبة (OBU) هي وحدات الاتصالات اللاسلكية المثبتة داخل المركبة، بينما تعرف الوحدات RSU بأنها وحدات النفاذ اللاسلكي الموجودة بجانب الطريق. وتتكون البنية التحتية من وحدات RSU والمرافق الخلفية، مثل إدارة حركة المرور وأنظمة المراقبة وسلطة إصدار الشهادات (CA). ويمكن توصيل وحدات RSU بالمرافق الخلفية عبر شبكات سلكية أو لاسلكية.



الشكل 1 – نظرة عامة للاتصالات بين المركبات

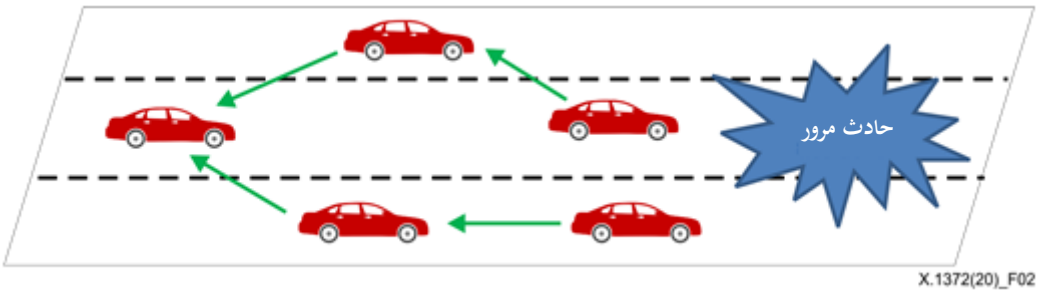
2.6 الاتصالات من مركبة إلى مركبة

الاتصالات من مركبة إلى مركبة (V2V) تتضمن الإرسال اللاسلكي للبيانات بين المركبات. والغرض من هذه الاتصالات V2V هو منع الحوادث بفضل تقاسم المعلومات وتبادلها بين المركبات. وتبعاً لكيفية تطبيق التكنولوجيا، قد تتلقى مركبة ما تحذيراً يبلغ عن احتمال وقوع حادث ما. عندئذ قد تتخذ المركبة إجراءات استباقية مثل عملية الكبح لتخفيف السرعة. والاتصالات بين فصائل المركبات في الشبكة V2V تجعل القيادة الجماعية ممكنة بتقاسم معلومات السرعة وأحوال الطريق. وبالإضافة إلى ذلك، يمكن استخدام المنارات الإلكترونية لتبادل المعلومات بين المركبات بغية تمكين القيادة السهلة والآمنة. وبفضل الاتصالات V2V، يمكن للمركبة جمع المعلومات عن أحوال البيئة المحيطة بما يشمل 360 درجة.

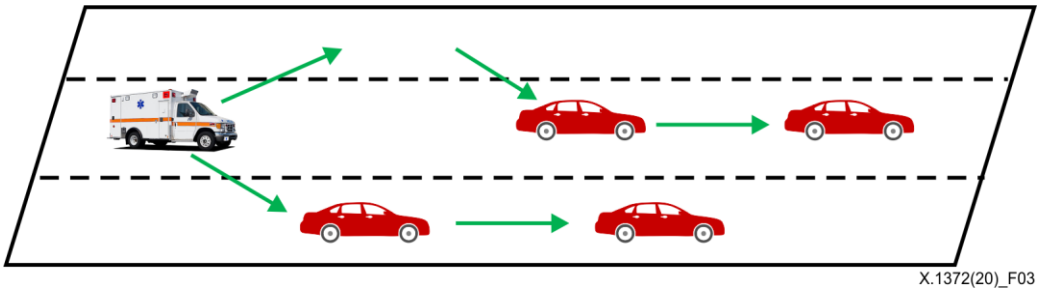
ويمكن تمييز سيناريوهات الاتصالات V2V التالية:

– انتشار التحذير V2V:

في سيناريو انتشار التحذير V2V، تنشر رسالة التحذير من مركبة إلى أخرى. مثال ذلك، إذا وقع حادث مرور، فينبغي إرسال تحذير نحو الخلف إلى جميع المركبات التي تقترب من مكان الحادث، لإعلامها بوجود الحادث نحو الأمام. ومن ناحية أخرى، إذا كانت هناك مركبة طوارئ، سيارة شرطة مثلاً، تقترب من الخلف، فينبغي إرسال رسالة تحذير إلى جميع المركبات القريبة والأمامية بما يضمن وصول مركبة الطوارئ بأمان على وجه السرعة. ويوضح الشكل 2 الحالة التي ينتشر فيها التحذير نحو الخلف بوقوع حادث في الأمام، ويوضح الشكل 3 الحالة التي تقترب فيها مركبة الطوارئ من الخلف وتنتشر رسالة الإنذار نحو الأمام.



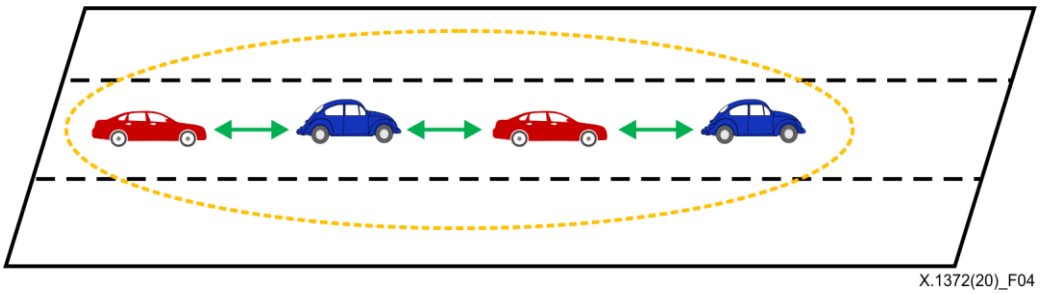
الشكل 2 – انتشار التحذير من مركبة إلى أخرى – انتشار نحو الخلف



الشكل 3 – انتشار التحذير من مركبة إلى أخرى – انتشار نحو الأمام

– الاتصالات V2V بين فصائل المركبات:

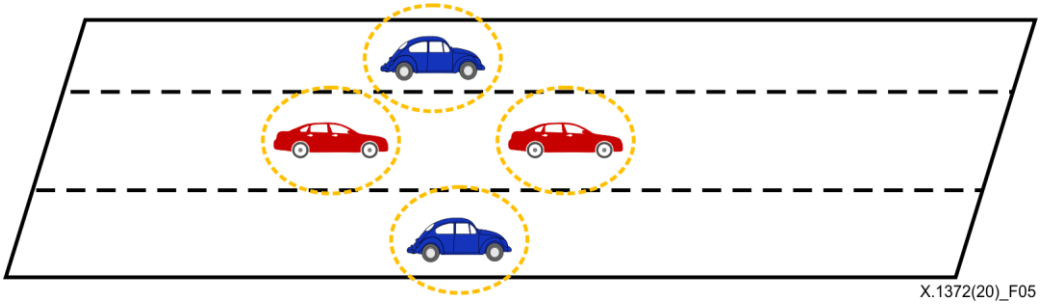
في سيناريو الاتصالات V2V بين فصائل المركبات، تقوم عدة مركبات بتشكيل فصيل ويمكنها التواصل فيما بينها ضمن هذا الفصيل. مثال ذلك، يمكن للمركبات التي تسلك نفس المسار، أو على الأقل نفس المسار لبعض الوقت، أن تشكل فصيلاً. ويمكن لهذا الفصيل تبادل المعلومات عن أحوال المركبات مما يساعد على القيادة الآمنة. ويبين الشكل 4 الاتصالات V2V ضمن فصيل ما.



الشكل 4 – التواصل V2V ضمن فصيل

– المنارات الإلكترونية V2V بين المركبات:

في سيناريو الاتصالات V2V بواسطة المنارات الإلكترونية، ترسل كل مركبة دورياً معلومات عن الأحوال الخاصة بها، من قبيل معدل السرعة الراهنة والاتجاه والموقع نسبة إلى المركبات القريبة. ويبين الشكل 5 الاتصالات V2V بواسطة المنارات الإلكترونية.



الشكل 5 – الاتصالات V2V بواسطة المنارات الإلكترونية

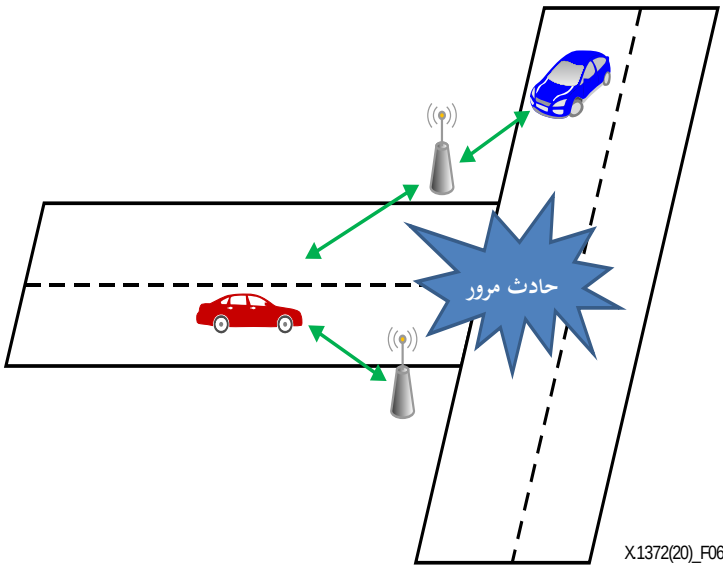
3.6 الاتصالات بين المركبة والبنية التحتية V2I

الاتصالات بين المركبة والبنية التحتية (V2I) هي عبارة عن الإرسال اللاسلكي للبيانات بين المركبة والبنية التحتية من قبيل الوحدات بجانب الطريق (RSU).

ويمكن تحديد سيناريوهات الاتصالات V2I التالية.

– التحذير بين المركبة والبنية التحتية

يسمح سيناريو التحذير V2I بالتواصل بين المركبة والبنية التحتية، من قبيل وحدات جانب الطريق. مثال ذلك، عندما يقع حادث مرور عند تقاطع ما، يمكن لوحدة جانب الطريق أن ترسل رسالة تحذير إلى المركبات المقتربة نحو ذلك التقاطع. وتعتبر إخطارات التحذير بقرب المركبة التي تحاول الانعطاف نحو اليمين أو اليسار ونقاط الالتقاء هي أيضاً حالات لاستخدام التحذير V2I. ويبين الشكل 6 مثالاً على سيناريو التحذير V2I.



الشكل 6 – اتصالات التحذير V2I بين المركبة والبنية التحتية

– تبادل المعلومات V2I بين المركبة والبنية التحتية (بما في ذلك V2V):

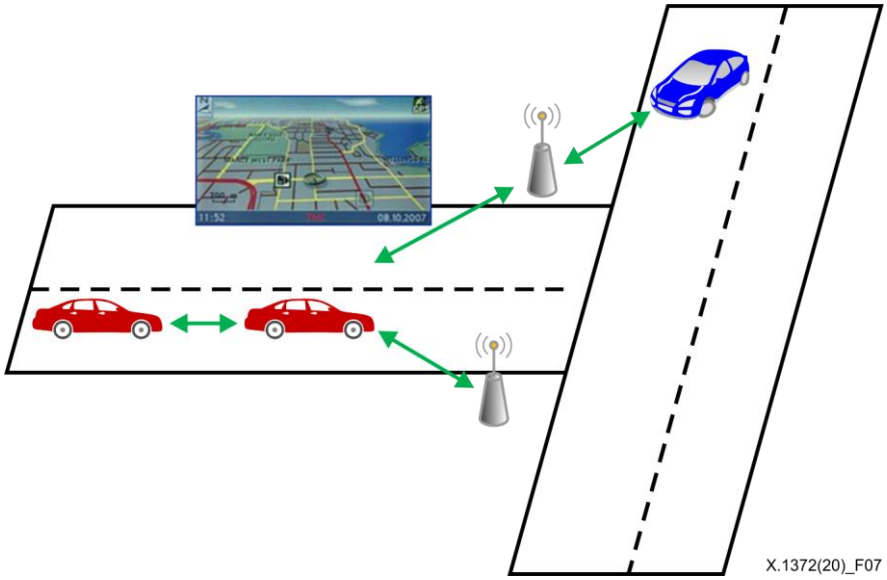
قد تتضمن الاتصالات V2I تبادل المعلومات واللافتات المعروضة داخل المركبة، ومعلومات طور وزمن إشارة المرور، وبيانات مسبار المركبة، ومعلومات المحاسبة (من قبيل تحصيل رسوم المرور)، وأحوال سطح الطريق/الطقس/مسافة الرؤية ومعلومات أشغال الطرق. وتشمل أمثلة حالات الاستخدام ما يلي:

- تنزيل بيانات النقل الأساسية:

في أنظمة النقل الذكية، قد يحتوي عدد من رسائل V2I على رسائل تحذير. وللتعامل مع هذه الرسائل، غالباً ما تتطلب المركبة خارطة للمكان الذي توجد فيه أو حيث تتحرك أو قد تحتاج إلى معلومات عن ظروف الوقت الحقيقي المحيطة بالمركبة. وغالباً ما يتم تنزيل هذه المعلومات من البنية التحتية، من قبيل وحدات جانب الطريق.

- بيانات دعم كفاءة النقل:

في أنظمة النقل الذكية، يمكن للمركبة التواصل مع البنية التحتية من حين لآخر للحصول على معلومات متعلقة بحركة المرور، من قبيل معلومات التحكم في حركة المرور المؤقتة وما إلى ذلك. ونتيجة لذلك، يمكن للمركبة معرفة الأماكن التي يحدث فيها ازدحام حركة المرور. ويمكنها عندئذٍ استمثال مسارها بمساعدة البنية التحتية، وذلك بتحديث مسارها مثلاً بالاستعانة بدليل الملاحة الموصول بشبكة للهاتف المتنقل. وهكذا يمكن تحسين كفاءة المركبات باستخدام الاتصالات V2I. وفي مثال آخر، يمكن للبنية التحتية أيضاً تحديث معلومات المرور استناداً إلى الرسالة التي ترسلها المركبة من خلال الاتصالات V2I. ويوضح الشكل 7 تبادل المعلومات عبر الاتصالات V2I.



الشكل 7 – تبادل المعلومات عبر الاتصالات V2I

4.6 الاتصالات بين المركبة والأجهزة الجوالة V2D

من الممكن، باستخدام تكنولوجيا الاتصالات بين المركبة والأجهزة الجوالة (V2D)، توصيل المركبة بالأجهزة الجوالة مثل الهواتف الذكية والحواسيب المحمولة وأنظمة الملاحة في المركبة، إما من خلال بنية تحتية مفتوحة مع واجهة موحدة نحو ناقلة شبكة منطقة التحكم (CAN) في المركبة أو عبر بوابة تتوسط الطلبات/الردود من الجهاز الجوال نحو النظام الذي يعمل على متن المركبة. ويمكن، باستخدام هاتف ذكي أو جهاز جوال، تمكين الوظائف عن بُعد لاستبانة معلومات حالة المركبة وإدارتها، من قبيل أماكن الصيانة. وعلاوةً على ذلك، من المتوقع مواصلة تطوير الخدمات المريحة.

فإذا أخذنا التخطيط لرحلة سفر مثلاً، حيث يختار السائق وجهة ما على جهاز جوال، ثم يمكن أن يخطط الجهاز الجوال المسار بتجميع عناصر مختلفة من المعلومات من مصادر مختلفة، مثل الجداول الزمنية للنقل العام (القطار أو المترو أو الحافلات، وغيرها) وكذلك معلومات حركة المرور في الوقت الفعلي. وتتبع المركبة المسار المخطط، وتحيد عنه في حالة حدوث تغييرات على المدى القصير في حركة المرور. ولا يتخذ الجهاز الجوال قرارات بشأن المناورات وينفذها فحسب بل يتفاعل أيضاً مع حالات حركة المرور المحلية، من قبيل تتبّع المركبات الأخرى، وتجنب العقبات وتغيير الممرات والتوقف عند إشارات المرور، وما إلى ذلك. ويمكن توصيل هذا الجهاز الجوال بالشبكات داخل المركبة. لذلك ربما يتمكن المهاجمون السيبرانيون من النفاذ إلى الأنظمة العاملة داخل المركبة.

وفي حالة تهديدات الأمان عبر Bluetooth، يمكن تنفيذ تعليمات شفرة خبيثة من خلال تطبيقات في الهواتف الذكية الموصولة بالمركبة. وتتعرض أنظمة الصوت والفيديو والملاحة (AVN) داخل المركبة لهجمات البرمجيات الثابتة عبر مواقع تخزين الوسائط المتعددة ويمكن أن تتعرض بسهولة للتسلل عبر النظام العالمي لتحديد الموقع (GPS) أو قنوات الراديو الساتلية. وينبغي السيطرة على الهجمات عبر الأجهزة الجوالة لدرء المخاطر التي تتهدد سلامة المركبات.

وفيما يلي مناقشات بشأن نوعين مختلفين من الاتصالات V2D:

- الاتصالات V2D عبر الروابط غير المباشرة:

يمكن للمركبات والأجهزة الجوالة التواصل عبر روابط غير مباشرة. ويعني التواصل عبر الروابط غير المباشرة وجود معدات تابعة لأطراف ثالثة مثل نقاط النفاذ وأجهزة التوجيه لتقدم الاتصالات بين العقد الطرفية. وتَستخدم الهواتف الخلوية والهواتف الذكية تقنية النطاق العريض اللاسلكي المتنقل من قبيل التطور طويل الأجل (LTE) وشبكات الأمانة اللاسلكية (Wi-Fi) وغير ذلك. ويتزايد استخدام شبكات Wi-Fi في الهواتف الذكية من أجل التواصل مع المركبات. وتقنيات 5G هي أيضاً قناة اتصال رئيسية لهذه الروابط غير المباشرة.

- الاتصالات V2D عبر الروابط المباشرة:

يمكن للمركبات والأجهزة الجوالة التواصل عبر روابط مباشرة دون أي تدخل فيما بينها أو عبر تقنيات الاتصالات اللاسلكية مثل Bluetooth وZigBee واتصالات المجال القريب (NFC).

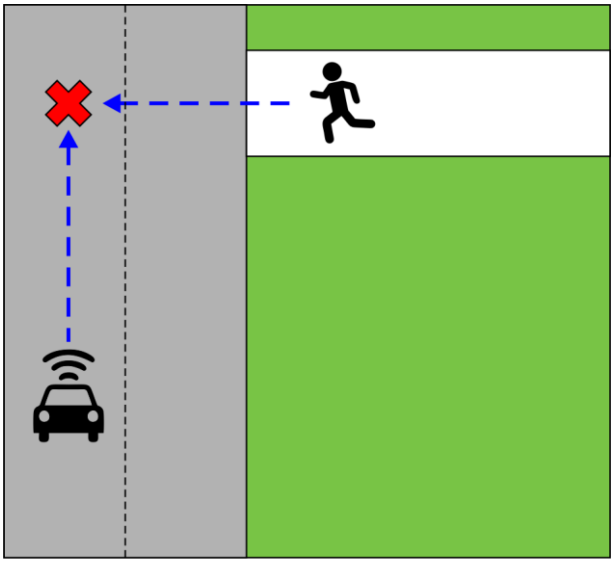
ويمكن للمركبات والأجهزة الجوالة أيضاً التواصل عبر الروابط السلكية. مثال ذلك، يمكن للجهاز الجوال الاتصال بمركبة من خلال نفاذ مادي من قبيل الناقل العمومي بالتسلسل (USB)، ورابط متنقل عالي الوضوح (MHL) وواجهة وسائط متعددة عالية الوضوح (HDMI). وتحدد معايير التشخيص II على متن المركبة (OBD-II) واجهات التشخيص وتوفر أيضاً قائمة مرشحة لمعلمات المركبة والإجراءات من أجل نقل البيانات.

وعلى وجه الخصوص، يمكن اعتبار الاتصال من المركبة إلى المشاة (V2P) كحالة محددة للاتصالات من مركبة إلى جهاز جوال (V2D) عندما تتواصل المركبة مع جهاز جوال يرتبط بأحد المشاة.

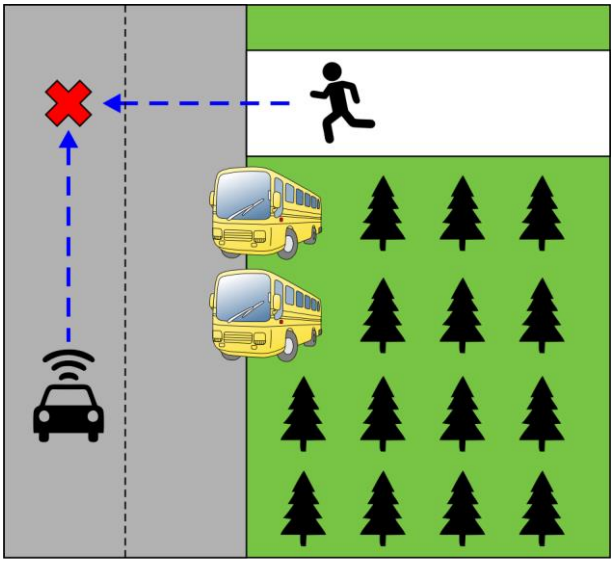
ويحتوي نهج الاتصالات V2P على تطبيقات لطائفة واسعة من مستخدمي الطرق المستضعَفين (VRU)، بما في ذلك مستخدمي الطرق دون محركات، من قبيل المشاة وراكبي الدراجات بالإضافة إلى راكبي الدراجات النارية وذوي الإعاقة أو القدرة المحدودة على الحركة.

ونظراً لارتفاع مستوى حوادث المرور التي تنطوي على مستخدمي الطرق المستضعَفين، تقترح أنظمة النقل الذكية حلولاً لتعزيز السلامة على الطرق من خلال جمع بيانات أجهزة الاستشعار، ومفاهيم مثل التصور الإدراكي وتمكين تبادل المعلومات بين المركبات والمشاة. والأهم من ذلك هو أن الاتصالات V2P لن تحذر سائق مركبة ما من اقتراب أحد المشاة لكي يعمد إلى إيقاف المركبة فحسب ولكنها ستنبه أيضاً هاتف الشخص الماشي المتنقل لإشعاره باقتراب المركبة.

ويمكن لأنظمة النقل الذكية أن تتحرى مستخدمي الطرق المستضعَفين وأن تساعد على منع التصادم المحتمل بين المركبات ومستخدمي الطرق المستضعَفين. ويوضح الشكل 8 أحد المشاة في سيناريو خط البصر (LOS) بالنسبة للسائق ويوضح الشكل 9 أحد المشاة في سيناريو خارج خط البصر (NLOS) بالنسبة للسائق كيف يمكن لأنظمة النقل الذكية تحسين السلامة على الطرق لمستخدمي الطرق المستضعَفين.



الشكل 8 – خط البصر



الشكل 9 – خارج خط البصر

- المشاة في خط البصر بالنسبة للسائق (LOS):

كما هو مبين في الشكل 8، تعتمد أجهزة الاستشعار النشطة، مثل الرادارات وأجهزة الاستشعار بالموجات فوق الصوتية وأجهزة قياس المسافة بالليزر وكاميرات الفيديو، طرائق قائمة على رؤية الحاسوب تنطبق على تحري وجود المشاة حيث يمكن رؤية هؤلاء المشاة من المركبة. وعندما يقترب أحد المشاة، تتحرى المركبة المتحركة اقترابه وتتخذ من ثم القرار الحاسم. وفي الوقت نفسه، يمكن للمركبة أن ترسل تحذيراً عبر الهاتف الخلوي لدى الشخص الماشي لتنبيهه إلى الخطر المحتمل.

- وجود المشاة خارج خط البصر بالنسبة للسائق (NLOS):

القدرة على تحري وجود المشاة محدودة بحكم مجال رؤية أجهزة الاستشعار. وفي الشكل 9، يُحتجب الشخص الماشي من مجال الرؤية بسبب العوائق، من قبيل الأشجار والحافلات الواقفة. ولكن اتصالات المركبات قادرة على إعلان المعلومات ونشرها بما يتجاوز مجال رؤية أجهزة الاستشعار. وحالما تتلقى المركبة إشعار التحذير، تقوم بتحديث الخارطة الدينامية المحلية (LDM) الخاصة بها وتقييم مدى خطورة الموقف لاتخاذ قرار. وفي الوقت نفسه، يتلقى الهاتف الخلوي لدى الشخص الماشي إشعاراً تحذيرياً.

7 التهديدات المحددة

1.7 تهديدات للكتمان

يوضح الشكل 10 التهديدات للكتمان الموصوفة في هذه الفقرة.

– التنصت:

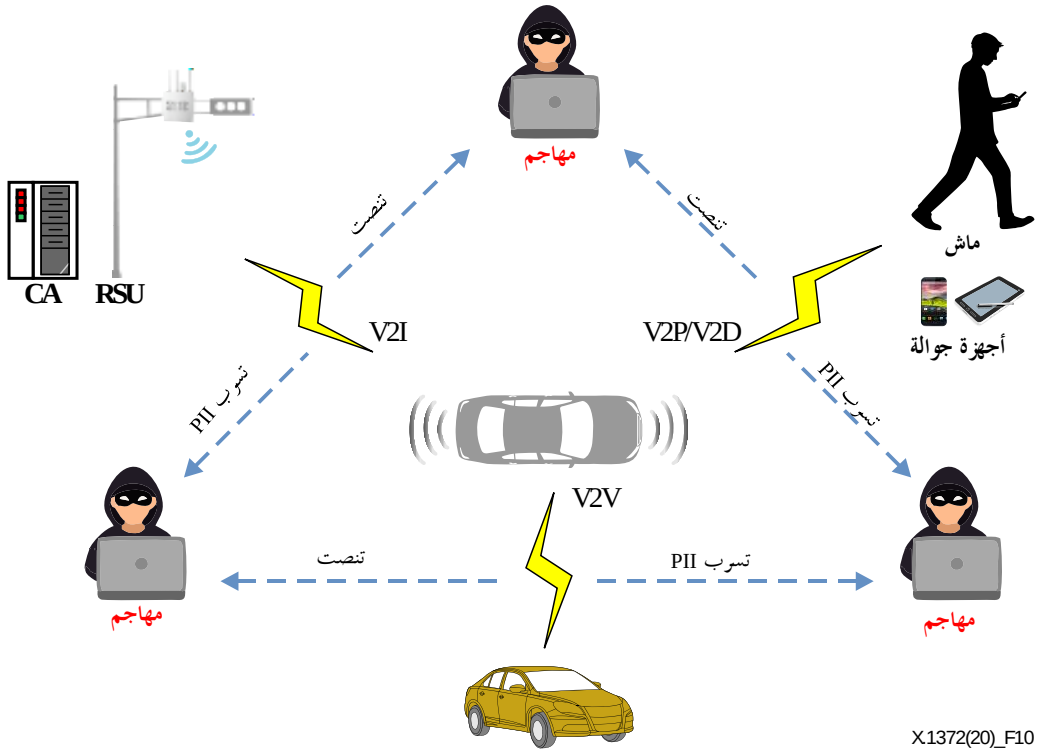
يمكن للمهاجم التقاط (أي قراءة و/أو تسجيل) رسائل الاتصالات V2V الخاصة بالمركبات القريبة ورسائل V2I الخاصة بوحدات جانب الطريق، ثم يقوم هذا المهاجم بتحليل معلومات حركة المرور عن طريق معالجة الرسائل الملتقَطة.

ويمكن للمهاجم التقاط رسائل V2D بين وحدة الاتصالات المركزية والجهاز الجوال. ويمكنه بعد ذلك تحليل المعلومات الدينامية عن المركبة، مثل الموقع الراهن ومعدل السرعة.

ويمكن للمهاجم التقاط رسائل V2P وتضليل المشاة وإيقاعهم في وضع خطير على الطريق.

– تسرب المعلومات المحدِّدة لهوية الشخص (PII):

يمكن للمهاجم تحليل المعلومات لاكتشاف هوية صاحب مركبة ما من خلال جمع رسائل V2X الخاصة به وتتبّع موقع المركبة على مسار القيادة لشخص معين.



الشكل 10 – تهديدات للكتمان

2.7 تهديدات للسلامة

يوضح الشكل 11 التهديدات للسلامة الموصوفة في هذه الفقرة.

– التلاعب في رسالة التوجيه:

من شأن استحداث عقدة وسيطة خبيثة أن تعدل رسالة التوجيه، وعندئذ تتلقى المركبات معلومات خاطئة.

– التلاعب بمعلومات الاعتماد:

يعني التلاعب بمعلومات الاعتماد تعديل المفتاح أو المعرّف الخاص بالمركبة، بحيث يمكن للمهاجم استخدام معلومات اعتماد مركبة أخرى دون ترخيص.

– التلاعب بمعلومات جهاز الاستشعار:

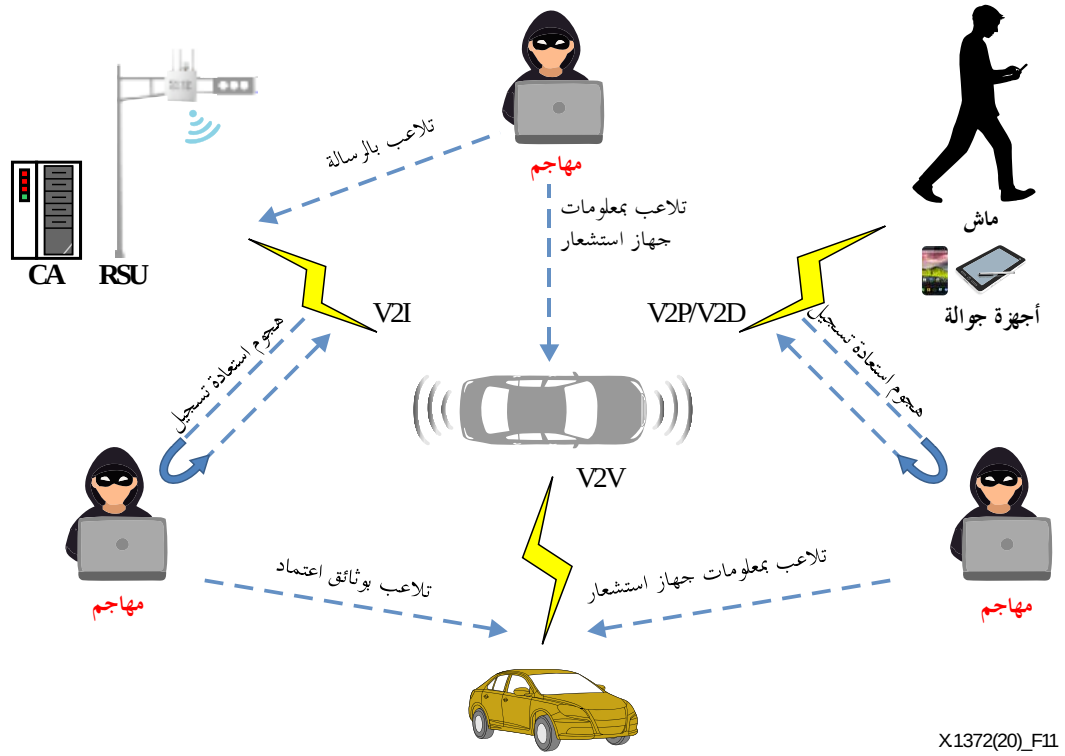
يمكن للمهاجم تعديل العنوان الفعلي لوحدة الاتصالات أو يمكنه التلاعب بمعلومات وحدة التحكم الإلكتروني، من جهاز استشعار معدل السرعة مثلاً. وعلاوةً على ذلك، هناك العديد من أجهزة الاستشعار الأخرى على متن المركبة، مثل الرادار والكاميرا، وهي تعمل بمثابة تجهيزات لمساعدة السائق. ومن الممكن توجيه بيانات جهاز الاستشعار الخاطئة، فيما يتعلق بخطوط الطول والعرض والارتفاع والسرعة والاتجاه وزاوية عجلة القيادة والتسارع، إلى الوحدات على متن المركبة أو الوحدات بجانب الطريق الأخرى. ومن شأن بيانات جهاز الاستشعار المغلوطة هذه أن تؤدي إلى اضطراب حركة المرور. مثال ذلك، قد تؤدي قيمة التسارع الخاطئة إلى تشغيل مصابيح كوابح الطوارئ الإلكترونية (EEBL) في السيارات المجاورة لتقليل فرصة حدوث تصادمات متعددة للمركبات، حتى لو كانت حالة المرور الواقعية حسنة.

- التلاعب في تطبيقات جهاز جوال:

يؤدي التلاعب في التطبيقات إلى أثر ضار على المركبة من خلال واجهة اتصالات V2D. مثال ذلك، يمكن أن يؤدي التلاعب في التطبيق إلى إجبار الجهاز الجوال على إرسال عدد كبير من الرسائل الحميدة إلى المركبة، وتعرف هذه الممارسة باسم الإغراق. وعلاوةً على ذلك، يمكن أن يفضي التلاعب بالتطبيق إلى دس شفرة خبيثة في الوحدة على متن المركبة وإرسال رسالة تتطلب الكثير من موارد الحوسبة. ويمكن لهذا التطبيق أيضاً أن يرسل عدداً أكبر من الرسائل ذات حجم أكبر بكثير من سعة التخزين المتوفرة في الوحدة OBU.

- الهجوم باستعادة التسجيل:

يمكن للمهاجم اعتراض رسائل الاتصالات V2V من المركبات القريبة ورسائل V2I الخاصة بالوحدات على جانب الطريق. ويمكن لهذا المهاجم، في وقت لاحق، استعادة تسجيل تلك الرسائل أو المعلومات لأغراض خبيثة.



الشكل 11 – تهديدات للسلامة

3.7 تهديدات للتيسر

يوضح الشكل 12 التهديدات للتيسر الموصوفة في هذه الفقرة.

- الهجوم بالتشويش ورفض الخدمة الموزع (DDoS) على قناة اتصالات V2X:

يمكن للمهاجم إرسال العديد من الرسائل عديمة الفائدة؛ وتُعرف هذه التقنية باسم الإغراق. ويمكن تصنيف إعادة توجيه رسالة محددة فقط بواسطة عقدة توجيه في فئة هذا النوع من الهجوم.

- هجوم رفض الخدمة الموزع على الوحدة على متن المركبة:

يمكن للمهاجم دس الشفرات الخبيثة في الوحدة على متن المركبة وإرسال رسائل تتطلب موارد حوسبية كبيرة. ويمكن لهذا المهاجم أيضاً إرسال العديد من الرسائل التي يكون حجمها، تراكمياً، أكبر من سعة التخزين في الوحدة OBU. وعلى وجه الخصوص، تعتبر التحديثات المتكررة للبرمجية دون ترخيص مثالاً على هجوم شديد من هذا النوع.

- هجوم التوقيت:

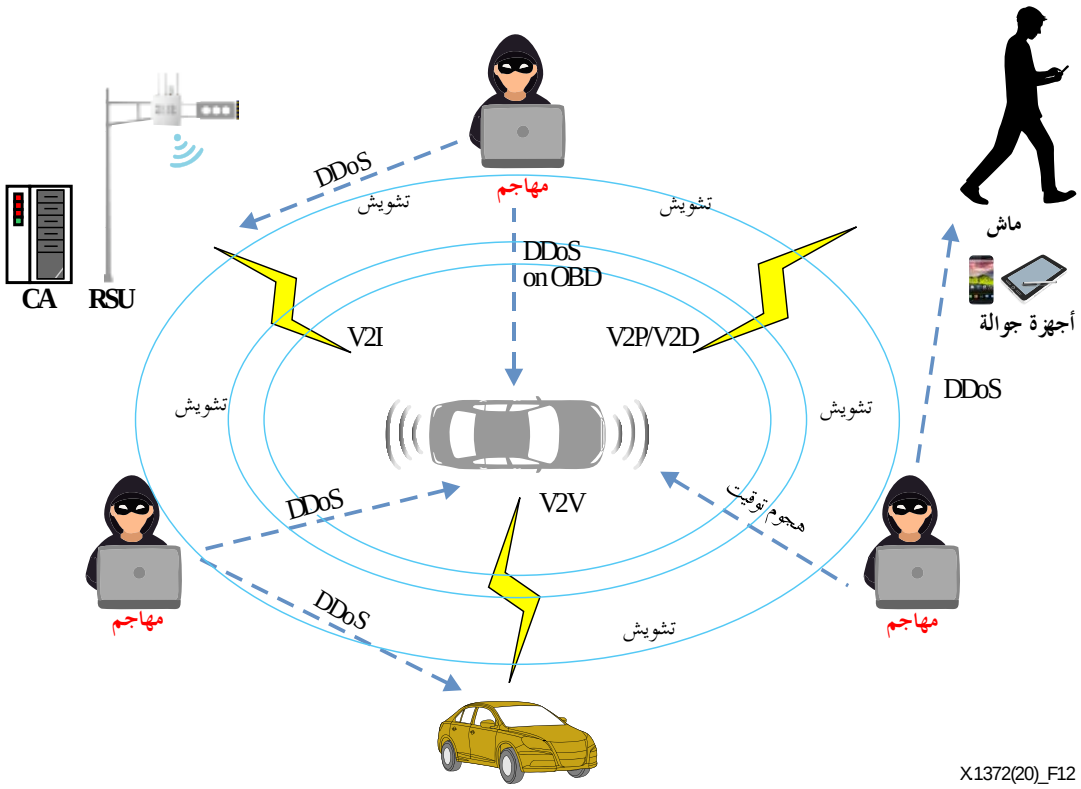
هجوم التوقيت، على سبيل المثال، هو تأخير تسليم رسالة سلامة إلى المركبات الأخرى. وبذلك قد يمنع خدمات الاتصالات من المركبة إلى كل شيء المناسبة، من قبيل بث رسائل التحذير.

- التسلل في أجهزة الاستشعار:

قد تتعرض أجهزة الاستشعار للهجوم وتتسبب في حدوث أخطاء بتقديم قيم خبيثة. وهناك عموماً نوعان من الأخطاء يمكن أن تحدث في جهاز الاستشعار: خطأ عابر وخطأ دائم. وقد يحدث الخطأ العابر أثناء التشغيل العادي للنظام ويختفي بسرعة. وفي الواقع، يبدي معظم أجهزة الاستشعار نموذج خطأ عابراً يحدد مقدار الوقت الذي تقدم فيه قياسات خاطئة. مثال ذلك، ليس من غير المألوف أن يفقد نظام GPS الاتصال بالسواتل مؤقتاً (أو أن يستقبل إشارات ضوضاء)، لا سيما في المدن ذات المباني الشاهقة. وكذلك قد يعجز جهاز استشعار يرسل البيانات باستخدام شبكة مثقلة بالاتصالات (تستخدم مثلاً بروتوكول التحكم في النقل/بروتوكول الإنترنت TCP/IP مع إعادة الإرسال) عن تقديم قياساته في الوقت المحدد، ومن ثم توفير معلومات خاطئة عند وصول الرسائل. ولكن نظراً لقصر المدة الزمنية، ينبغي ألا تشكل الأخطاء العابرة تهديداً لأمن النظام.

وعلى النقيض من ذلك، فإن الأعطال الدائمة هي عيوب في أجهزة الاستشعار تستمر لفترة أطول من الزمن وقد تؤثر جدياً على تشغيل النظام. فقد يعاني جهاز الاستشعار مثلاً من أضرار مادية تفضي إلى تحيز دائم في قياساته. وفي هذا السيناريو، وما لم يكن بالإمكان تصحيح الخطأ في البرمجية، فمن الأفضل للنظام الاستغناء عن جهاز الاستشعار هذا كلياً.

وتبعاً للهدف الذي يتوخاه المهاجم، قد تظهر الهجمات على قياسات جهاز الاستشعار في شكل أخطاء عابرة أو دائمة. ولكل من الفئتين مزايا وعيوب بالنسبة للمهاجم. إذ من شأن جعل جهاز الاستشعار يتصرف كما لو كان خللاً مؤقتاً أن يحول دون اكتشاف المهاجم ولكنه يحد أيضاً من قدراته، في حين قد يكون الهجوم المطول الذي يشبه الخطأ الدائم أشد وطأة ولكن يمكن اكتشافه بسرعة.



الشكل 12 – تهديدات للتيسر

4.7 تهديدات لعدم الرفض

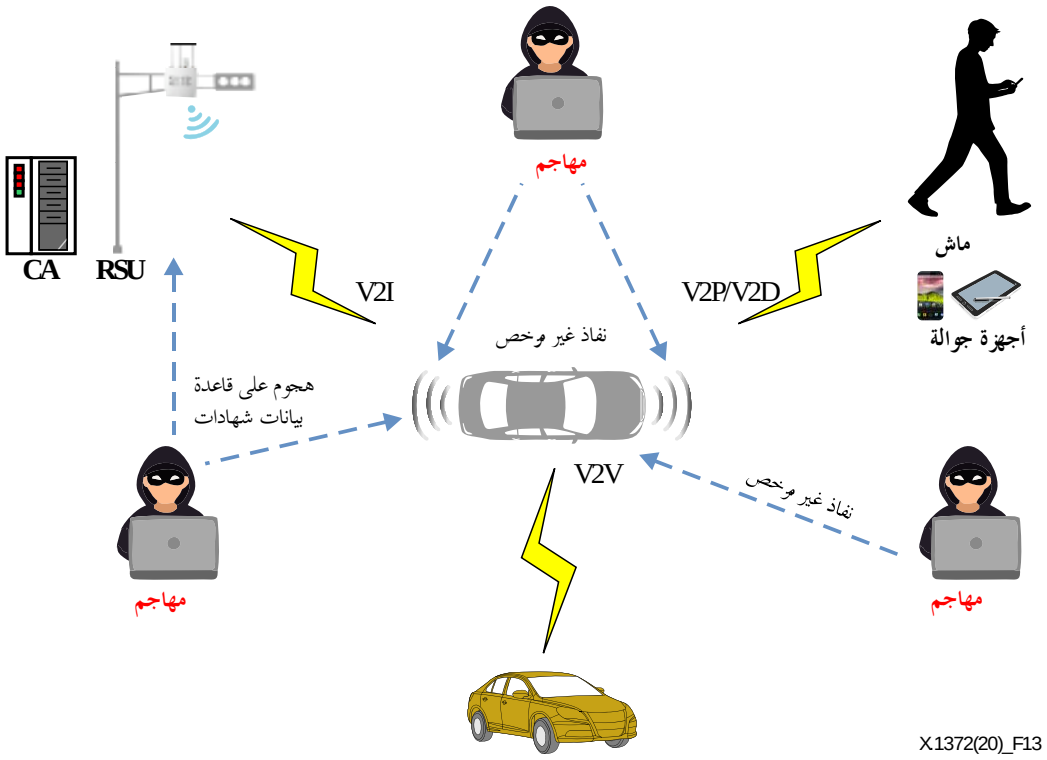
يوضح الشكل 13 التهديدات لعدم الرفض الموصوفة في هذه الفقرة.

- التلاعب في قاعدة بيانات الشهادات:

يمكن للمهاجم التلاعب بقاعدة بيانات الأسماء المستعارة لدى سلطة الشهادات، ويمكنه بعدئذ تعديل العلاقة بين شهادة طويلة الأجل وشهادة اسم مستعار قصيرة الأجل.

- النفاذ غير المرخص به إلى أوراق الاعتماد:

يمكن للمهاجم النفاذ إلى مفتاح خاص وشهادة ما دون ترخيص. فإذا تم الكشف عن المفتاح الخاص، عندئذ لا يمكن توفير عدم الرفض للمركبة، ولا يمكن توفير الوحدة بجانب الطريق والجهاز الجوال.



الشكل 13 – تهديدات لعدم الرفض

5.7 تهديدات الاستيقانية

يوضح الشكل 14 التهديدات الاستيقانية الموصوفة في هذه الفقرة.

- جدول التوجيه وهجوم تعديل الخارطة الدينامية المحلية:

يمكن للمهاجم محاكاة معلومات نظام GPS الخاص بالمركبة وتعديل معلوماته الجغرافية المكانية الأصلية.

- هجوم انتحال الهوية:

يمكن للمهاجم أن يتظاهر بأنه كيان آخر بسرقة معلومات هوية الكيان الآخر. عندئذ يستطيع المهاجم أن يتلقى رسائل ترسل عادةً إلى الكيان الآخر، ويمكنه أيضاً إرسال رسائل يولدها عادةً الكيان الآخر. فإذا كان الكيان الآخر مركبة طوارئ مثلاً، فيمكن للمهاجم إرسال رسالة إلى المركبات المحيطة الأخرى من قبيل "أنا مركبة طوارئ. يرجى إفساح الطريق".

وقد يرسل المهاجم أيضاً إشارة عطل كاذبة بالنيابة عن مركبة بريئة، عندئذ يمكن لسلطة إصدار الشهادات إلغاء تواصل المركبة البريئة.

- هجوم من نمط "Sybil":

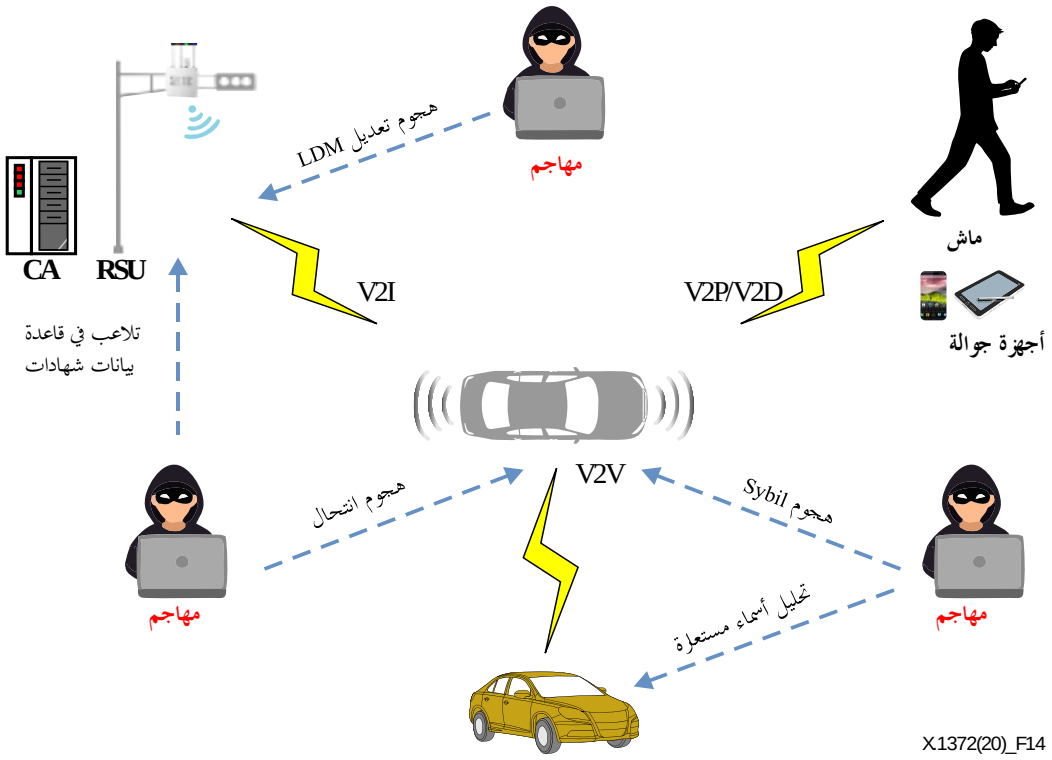
يمكن أن يحدث هجوم Sybil مثلاً عندما تحاكي مركبة ما مركبات متعددة باستخدام معرّفات هوية المركبات المتعددة.

- هجوم تحليل اسم مستعار:

يمكن للمهاجم تحليل العلاقة بين معرّفات هوية المركبة والأسماء المستعارة للعثور على الأسماء المستعارة المتعددة المستخدمة لنفس المركبة.

- التلاعب في قاعدة بيانات الشهادات:

يمكن للمهاجم التلاعب في قاعدة بيانات الأسماء المستعارة لدى سلطة إصدار الشهادات. عندئذ يستطيع المهاجم تعديل العلاقة بين الشهادة طويلة الأجل وشهادة الاسم المستعار قصيرة الأجل.



الشكل 14 – تهديدات الاستيقانية

6.7 تهديدات للمساءلة

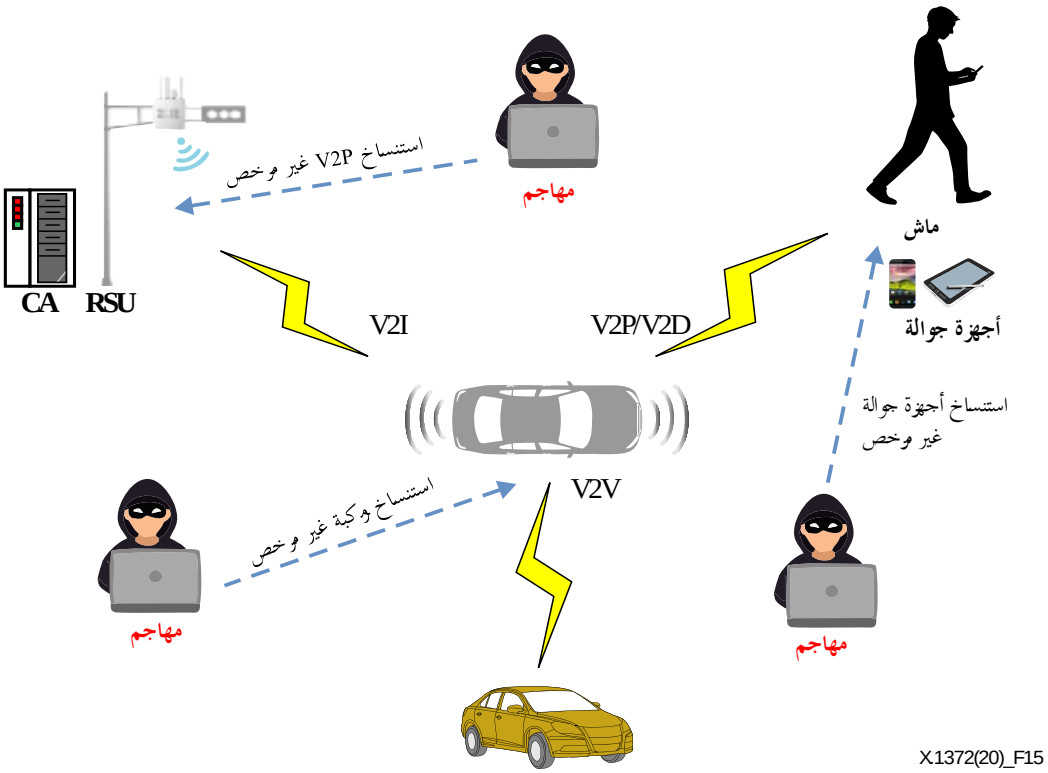
يوضح الشكل 15 التهديدات للمساءلة الموصوفة في هذه الفقرة.

- الاستنساخ غير المرخص له لجهاز جوال:

في إطار بعض الخدمات المعينة، تشخيص المركبات مثلاً، يمكن لجهاز جوال مرخص له النفاذ إلى وحدة الاتصالات المركزية في المركبة. ولكن إذا استنسخ ترخيصه بواسطة أجهزة خبيثة، كما يمكن أن يحصل مثلاً عند استخدام حساب تسجيل الدخول للجهاز المرخص له من قبل جهاز خبيث آخر، عندئذ يمكن لهذا الجهاز الخبيث النفاذ إلى وحدة الاتصالات. ويمكن التلاعب بوحدة الاتصالات المركزية هذه داخل مركبة من جانب جهاز جوال غير مرخص له.

- الاستنساخ غير المرخص له للمركبة والوحدة بجانب الطريق:

عندما يحصل المهاجم على معرّفات هوية المركبة والوحدة RSU (ينسخها)، تفقد المركبة الأصلية والوحدة RSU صفة المساءلة الخاصة بها.



الشكل 15 – تهديدات للمساءلة

7.7 تهديدات للترخيص

يوضح الشكل 16 التهديدات للترخيص الموصوفة في هذه الفقرة.

– النفاذ غير المرخص له إلى المعلومات الحساسة من حيث السلامة في المركبة:

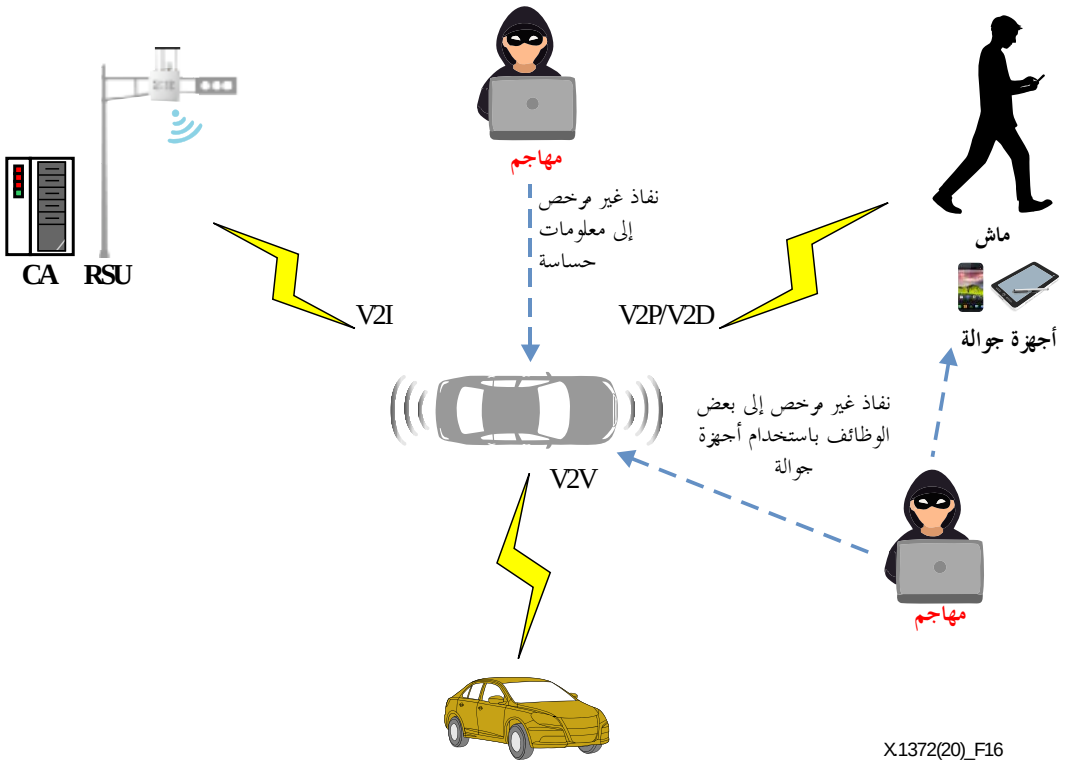
إذا لم يكن هناك تحكم في الترخيص، فيمكن للمستخدم الخبيث أو التطبيق الخبيث التحكم في مركبة ما دون ترخيص. مثال ذلك، ينبغي عدم السماح للتطبيق الذي يشغّل الموسيقى من خلال مكبر صوت في المركبة بالنفاذ إلى المعلومات الحساسة من حيث السلامة، مثل سرعة المركبة والحالة الراهنة للمكابح.

ويمكن للمهاجم غير المرخص له أيضاً التلاعب ببيانات المركبة الحساسة من حيث السلامة ومحوها واستبدالها، بما في ذلك معلمات المركبة، مثل عتبة المكابح والوسادة الهوائية لحالة الطوارئ وسجل النظام.

وفيما يتعلق بالمركبة الكهربائية، يمكن للمهاجم غير المرخص له التلاعب بمعلمات التشكيل لوظائف شحن المركبة.

– النفاذ غير المرخص له إلى وظائف معينة في المركبة باستخدام الأجهزة الجوالة:

من الأهمية بمكان تحديد وظائف التحكم في النفاذ إلى الأجهزة الجوالة الموصولة بمركبة ما. وتستخدم الأجهزة الجوالة عموماً كأدوات الصوت والفيديو والملاحة في المركبة. ويمكنها أن تعرض أيضاً محتويات الأجهزة الجوالة عبر جهاز تشغيل على الرأس متعدد الوسائط. وقد يترتب على الوظائف غير المرخص لها، مثل الاتصال مع بوابة مركزية في المركبة باستخدام هذا الجهاز الجوال، آثار ضارة شديدة على السلامة.



الشكل 16 – تهديدات الترخيص

8 متطلبات الأمن

تصف هذه الفقرة متطلبات الأمان للاتصالات من مركبة إلى كل شيء. وتصف الفقرات من 1.8 إلى 7.8 متطلبات الأمن في الاتصالات من مركبة إلى كل شيء (V2X)، ويرد في الفقرة 8.8 المزيد من التفاصيل عن هذه المتطلبات.

1.8 الكتمان

ينبغي ألا يكون من الممكن لكيان غير مرخص له أن يكشف عن الرسائل بين المركبات، وبين المركبات والبنية التحتية، وبين المركبات والأجهزة الجوالة، وبين المركبات والمشاة.

وينبغي ألا يكون من الممكن لكيان غير مرخص له تحليل تعرّف هوية شخص ما من خلال المعلومات المحدِّدة لهوية الشخص (PII) في رسائل الاتصال، مثل الموقع أو مسار القيادة لشخص معين.

2.8 السلامة

ينبغي حماية الرسائل المرسلة من مركبة ما أو إليها، أو وحدة بجانب الطريق أو جهاز جوال، من التعديل والحذف غير المرخص بهما.

3.8 التيسر

ينبغي أن يكون من الممكن لأي كيان إرسال واستقبال الرسائل في غضون زمن استجابة مناسب. مثال ذلك، ينبغي إرسال رسالة التحذير من اصطدام أمامي إلى مركبة قادمة قبل وصول المركبة إلى مكان الحادث. فإذا تعذر تسليم رسالة التحذير إلى المركبة القادمة بسبب هجوم تشويش، فقد يصبح تطبيق اتصالات السلامة V2V/V2I عديم الفائدة.

وينبغي أن يكون من الممكن لأي كيان معالجة المعلومات المتبادلة في الوقت الفعلي، متطلباً بذلك تنفيذ خوارزميات تجفير بسيطة منخفضة البتات الخدمية.

4.8 عدم الرفض

ينبغي ألا يكون من الممكن لأي كيان أن ينكر أنه قد أرسل رسالة ما. ويمكن تنفيذ هذا المطلب باستخدام التواقيع الرقمية في أنظمة الاتصالات من مركبة إلى كل شيء (V2X).

5.8 الاستيقانية

ينبغي أن تكون الكيانات، مثل الوحدات على متن المركبة والوحدات بجانب الطريق في بيئة اتصالات V2V/V2I، قادرة على البرهان بأنها صاحبة هوية شرعية مرخص لها. ويُعرف هذا المطلب باسم استيقان الكيان. وهو مطلوب أيضاً بين المركبة والجهاز الجوال.

وفي حالة الاتصال الجماعي، لا تحتاج المركبة إلى إثبات هويتها. بل ينبغي أن تثبت المركبة أنها عضو أصيل في المجموعة. ويطلق على هذا المطلب اسم استيقان النعت.

6.8 المساءلة

ينبغي أن يكون من الممكن لأي كيان تحري و/أو منع أي سوء سلوك في الوحدات على متن المركبة أو أجهزة استشعار المركبة عن طريق التحقق من بياناتها.

مثال ذلك، يمكن لوحدة OBU التحقق من بعض المعلومات في رسالة مستلمة بحثاً عن السلامة الحركية مقابل الرسالة المستلمة سابقاً. فإذا أظهرت بيانات الموقع في الرسالة الراهنة تغييرات مستحيلة في السلوك الدينامي للمركبة، فقد يكون ذلك خطأ في سلوك كيان آخر. ومن ثم يمكن نبذ هذه المعلومات أو تجاهلها.

7.8 الترخيص

من الأهمية بمكان تحديد التحكم في النفاذ والترخيص لمختلف الكيانات. وينبغي فرض قواعد محددة لتمكين كيانات محددة من النفاذ إلى وظائف أو بيانات معينة و/أو استخدامها أو منعها من ذلك.

8.8 قابلية تطبيق متطلبات الأمن للاتصالات من مركبة إلى كل شيء V2X

يسرد الجدول 1 متطلبات الأمن الموضحة في الفقرات من 1.8 إلى 7.8، وقابلية تطبيقها على الأشكال المختلفة للاتصالات من مركبة إلى كل شيء (V2X).

الجدول 1 – متطلبات الأمن للاتصالات من مركبة إلى كل شيء V2X

	V2V انتشار التحذير من مركبة إلى مركبة	V2V تواصل الفصائل من مركبة إلى مركبة	V2V المنارات الإلكترونية من مركبة إلى مركبة	V2I التحذير من مركبة إلى بنية تحتية	V2V/V2I تبادل المعلومات من مركبة إلى مركبة وإلى بنية تحتية	V2D التواصل من مركبة إلى أجهزة جوالة	V2P التواصل من مركبة إلى المشاة
الكتمان (عموماً)	–	O	–	–	O	O	O
كتمان (المعلومات المحددة لهوية الشخص)	O	O	O	▲	O	O	O
السلامة (PII)	O	O	O	O	O	O	O
التيسر	O	O	O	O	O	▲	O
عدم الرفض	O	O	O	O	O	O	O
الاستيقانية	O	▲	O	O	O	O	O
المساءلة	O	O	O	O	O	O	O
الترخيص	–	O	–	–	O	O	–

O: مطلوب؛ –: غير مطلوب؛ ▲: مطلوب جزئياً

وفي حالة انتشار تحذير V2V، لا تكون الخصوصية مطلوبة إلزاماً نظراً لأن الرسائل المتبادلة بين مركبة وأخرى تحتوي على معلومات مشاع أصلاً، مثل حوادث المرور نحو الأمام أو اقتراب مركبات طوارئ. وفي حالة انتشار تحذير V2V، لا تتضمن الرسائل المنشورة أي معلومات متعلقة بالترخيص.

وفي سيناريو الاتصالات V2V ضمن الفصيل، يكون استيقان المركبة مطلوباً جزئياً مما يعني أن كل مركبة لا يطلب منها بالضرورة استيقان كل مركبة في الفصيل. ويعني استيقان الكيان العملية التي يتأكد من خلالها كل كيان من هوية الكيان الآخر المشارك في الاتصال. ولكن في سيناريو V2V ضمن الفصيل لا تتطلب كل مركبة على وجه الدقة استيقان الكيان في المجموعة. وفي هذه الحالة، يكفي البرهان على أن كل مركبة هي عضو في المجموعة. أي أن هوية المركبة غير مضمونة وإنما المضمون فقط هو أن المركبة عضو في المجموعة. ويمكن أن يطلق على هذا النوع من الاستيقان اسم استيقان النعت. وتحتوي الرسائل في هذا السيناريو أيضاً على معلومات ترخيص من قبيل قائد الفصيل أو عضوية الفصيل.

وفي سيناريو الاتصالات V2V بواسطة المنارات الراديوية، ينبغي حماية معلومات البث من التعديل والحذف غير المرخص بهما. ومع ذلك، وإذا لم تتضمن الرسالة معلومات تعريف المركبة، فلا حاجة إلى تجفير الرسالة. وعلاوةً على ذلك، لا حاجة إلى الترخيص في سيناريو V2V بواسطة المنارات الراديوية لأن المعلومات المرسلة لن تستخدم لأغراض التحكم.

وفي سيناريو التحذير V2I، تكون المعلومات بين المركبة والبنية التحتية، مثل الوحدات بجانب الطريق، عادة معلومات حركة مرور في متناول عامة الناس. ولذلك فإن الخصوصية في بيئة التحذير V2I غير مطلوبة. وتعني العلامة المطلوبة جزئياً لحماية المعلومات المحدِّدة لهوية الشخص في حالة التحذير V2I أن المركبة تتطلب حماية هذه المعلومات، لكن الوحدة بجانب الطريق لا تتطلب حماية هذه المعلومات. وينبغي حماية الموقع الراهن للمركبة وتاريخ الرحلة إذا كان السائق مرتبطاً بالمركبة. ولكن ليس لدى الوحدة RSU أي معلومات محدِّدة لهوية الشخص لأن الوحدة RSU ليست مرتبطة بالأشخاص.

وفي سيناريو الاتصال V2D، يُستخدم الجهاز الجوال في المركبة. وعندما يتواصل الجهاز الجوال مع المركبة، لن يكون للتيسر نفس أثر سيناريو الاتصال V2V لأن عدد الأجهزة في المركبة أصغر عملياً من عدد المركبات على الطريق في بيئة الواقع.

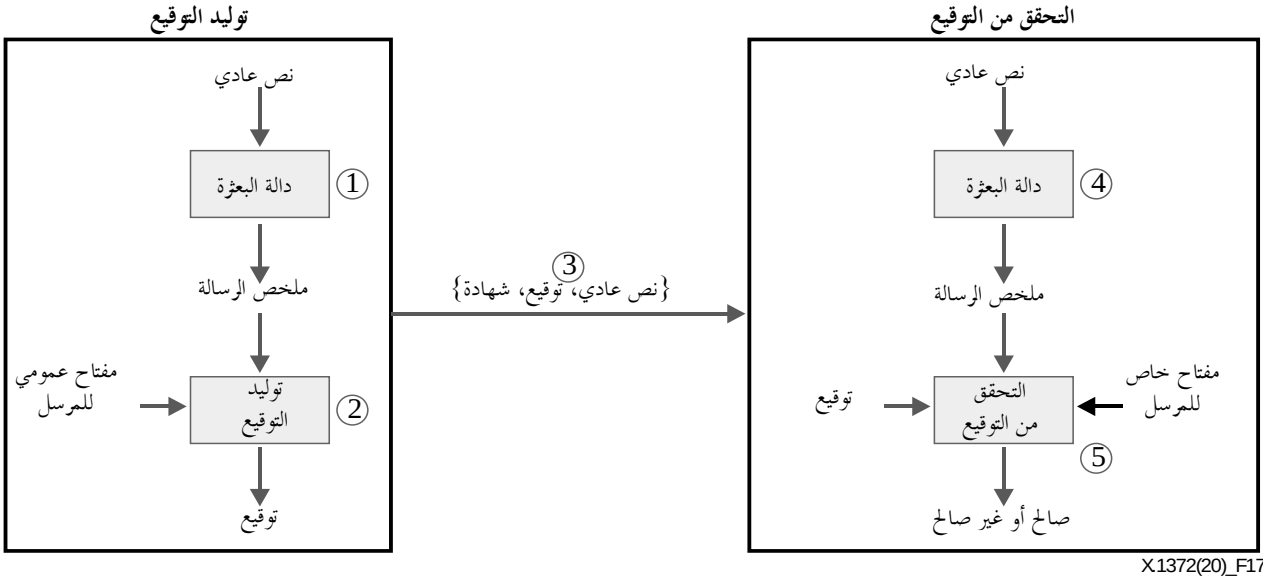
وفي سيناريو الاتصال V2P، لا يمكن أن يكون للجهاز الجوال لدى المشاة أو مستخدمي الطريق المستضعَفين (VRU) أي وظيفة تتطلب الترخيص من المركبة.

9 تنفيذ الاتصالات V2X مع توفير الأمن

يوفر هذا البند تطبيقات ممكنة للاتصالات V2X للوفاء بمتطلبات الأمن مثل الخصوصية وسلامة المعلومات والتيسر وما إلى ذلك، والتي ورد وصفها في الفقرة 8. ويقدم البند نظرة عامة موجزة لخوارزميات التجفير الأساسية المناسبة لبيئات الاتصالات الخاصة بالمركبات، يليها وصف لكيفية استخدامها في سيناريوهات الاتصالات V2X مثل الإنذار في حالات الطوارئ والتواصل بين الفصائل.

1.9 التجفير من أجل استيقان الكيان وخصوصية الرسائل

يمكن تنفيذ وظيفة استيقان الكيانات V2X باستخدام خوارزميات التوقيع الرقمي. ويمكن تنفيذ وظيفة خصوصية الرسائل باستخدام خوارزميات التجفير المتناظرة وخوارزميات تجفير المفاتيح العمومية. وتقدم هذه التوصية أمثلة على كيفية تنفيذ هذه الوظائف. ويتوقف تكييف واختيار الآليات والمعلمات المرتبطة بوظيفة استيقان الكيانات ووظيفة خصوصية الرسائل على سياسة النشر.



الشكل 17 – توليد التواقيع والتحقق منها

تشتمل خوارزمية التواقيع الرقمية على عملية توليد التواقيع وعملية التحقق من التواقيع كما هو موضح في الشكل 17. ويستخدم الموقّع عملية التوليد لتوليد توقيع رقمي على البيانات. ويستخدم المدقق عملية التحقق للتحقق من صحة التوقيع. ولدى كل موقّع مفتاح عمومي ومفتاح خاص. وكما هو مبين في الشكل 17، يستخدم المفتاح الخاص في عملية توليد التوقيع، ويستخدم المفتاح العمومي للموقّع في عملية التحقق من التوقيع.

والإجراء الإجمالي لتوليد التواقيع والتحقق منها هو كما يلي:

- الخطوة 1: باستخدام دالة اختزال (مثل دالة البعثرة الآمنة 256 (SHA-256)، يتم حساب ملخص الرسالة عبر رسالة النص العادي. مثال ذلك، يحسب الملخص بالنسبة لصيغة البروتوكول والرأسية والحمولة النافعة وطول الذيلية.
- الخطوة 2: يتم توليد توقيع ملخص الرسالة باستخدام المفتاح الخاص للمرسل؛
- الخطوة 3: يرسل النص العادي والتوقيع وشهادة المرسل إلى جهاز الاستقبال؛
- الخطوة 4: يحسب المتلقي ملخص الرسالة باستخدام النص العادي الوارد من المرسل؛
- الخطوة 5: يحسب المتلقي قيمة التحقق باستخدام ملخص الرسالة في الخطوة 4، والتوقيع المستلم، والمفتاح العمومي للمرسل. فإذا كانت قيمة التحقق هي نفس القيمة في التوقيع، يكون التوقيع المستلم صالحاً. وإذا كانت قيمة التحقق مختلفة عن القيمة في التوقيع المستلم يكون التوقيع غير صالح.

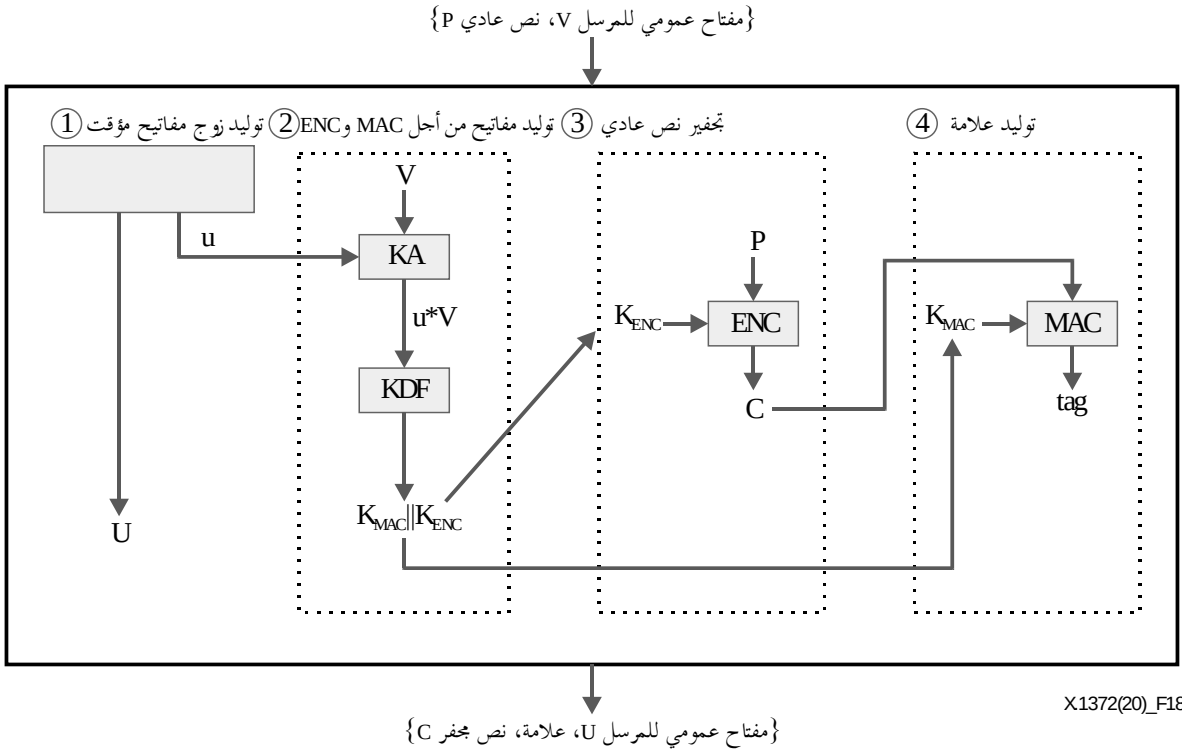
ويمكن استخدام خوارزمية التوقيع الرقمي للمنحنى الإهليلجي (ECDSA) بمثابة خوارزمية توقيع رقمي في الاتصالات V2X؛

وتُستخدم خوارزميات التجفير لدعم خصوصية رسائل الاتصالات V2X. وتُستخدم خوارزمية تجفير لاتناظري، مثل مخطط تجفير متكامل للمنحنى الإهليلجي (ECIES)، لنقل مفتاح لخوارزمية مفتاح تناظري، مثل معيار التجفير المتقدم (AES). ويصف الشكل 18 إجراء التجفير الخاص بالمخطط ECIES. ويستخدم المخطط ECIES في الشكل 18 الوظائف التالية:

- اتفاق المفاتيح (KA): الوظيفة المستخدمة لتوليد سر مشترك بين كيانين؛
- وظيفة اشتقاق المفتاح (KDF): آلية تنتج مجموعة من المفاتيح من مادة تكوين المفاتيح وبعض المعلمات الخيارية؛
- التجفير (ENC): خوارزمية تجفير المفاتيح التناظرية؛
- شفرة استيقان الرسائل (MAC): خوارزمية توليد شفرة استيقان الرسائل.

وتستخدم في الشكل 18 الرموز التالية:

- ***u***: مفتاح المرسل الخاص
- ***U***: مفتاح المرسل العمومي
- ***v***: مفتاح المستقبل الخاص
- ***V***: مفتاح المستقبل العمومي



الشكل 18 – إجراءات التجفير بمخطط تجفير متكامل للمنحنى الإهليلجي

كما هو مبين في الشكل 18، فإن مدخلات إجراء التجفير هي المفتاح العمومي للمستقبل ***V*** والنص العادي ***P***. ومخرجات إجراء التجفير هي المفتاح العمومي للمرسل ***U*** والعلامة ونص التجفير ***C***. ويتكون إجراء تجفير الرسائل من الخطوات التالية:

- الخطوة 1: توليد زوج مفاتيح مؤقت:

يولد المرسل المفتاح الخاص ***u*** والمفتاح العمومي ***U***. يوصى بتوليد المفتاح العمومي ***U*** حديثاً لكل عملية تجفير؛

- الخطوة 2: توليد المفتاح من أجل شفرة استيقان الرسائل والتجفير:

تولد وظيفة اتفاق المفتاح سراً مشتركاً بواسطة المفتاح الخاص ***u*** المؤقت للمرسل والمفتاح العام ***V*** للمستلم. وتأخذ وظيفة اشتقاق المفتاح القائمة على البعثرة SHA-256 هذا السر المشترك لتوليد مفتاح تسلسل شفرة استيقان الرسالة أي (***K_{MAC}***) ومفتاح التجفير (***K_{ENC}***)؛

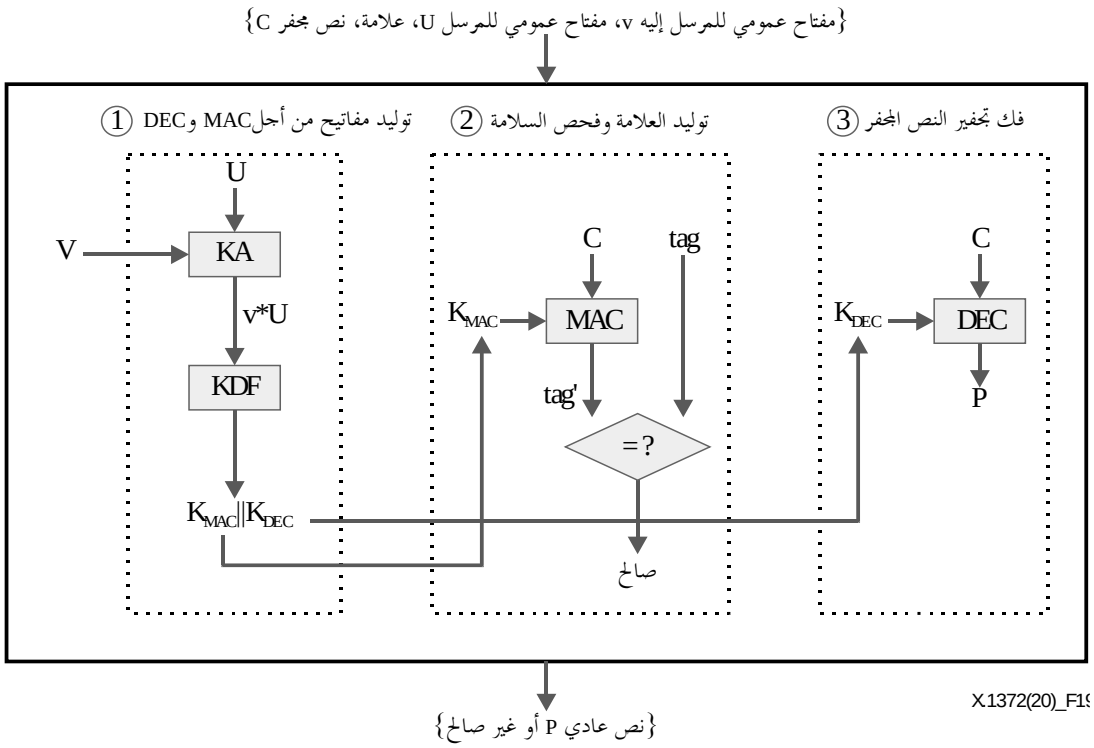
- الخطوة 3: تجفير النص العادي:

يتم تجفير النص العادي ***P*** بواسطة ***K_{ENC}*** باستخدام خوارزميات التجفير التناظري:

يستخدم المخطط ECIES لتجفير مفتاح تناظري لتجفير رسائل V2X باستخدام معيار التجفير المتقدم – أسلوب معاكس مع شفرة استيقان من رسالة تسلسل كتل التجفير (AES-CCM). لذلك فإن النص العادي هو في الواقع مفتاح التجفير من أجل المعيار AES-CCM؛

- الخطوة 4: توليد العلامة

تقوم وظيفة شفرة استيقان الرسالة (MAC) مع بعثرة SHA-256 بتوليد علامة لنص التجفير، وهو المفتاح التناظري للمعيار AES-CCM، لدعم سلامة الرسائل.



الشكل 19 – إجراءات فك التجفير بمخطط تجفير متكامل للمنحنى الإهليلجي

يصف الشكل 19 إجراءات فك التجفير الخاص بالمخطط ECIES. وكما هو موضح في الشكل، فإن مدخلات إجراءات فك التجفير هي المفتاح الخاص ***v*** للمستقبل، والمفتاح العمومي ***U*** للمرسل والعلامة ونص التجفير. ومخرجات إجراءات فك التجفير هما النص العادي ***P*** أو نتائج اختبار سلامة الرسالة. ويعني فك التجفير (DEC)، في الشكل 19، إجراء فك التجفير لخوارزمية المفتاح التناظري. ويتكون إجراء فك تجفير الرسائل من الخطوات التالية:

– الخطوة 1: توليد مفتاح لشفرة استيقان الرسالة وفك التجفير:

تقوم وظيفة اتفاق المفتاح (KA) بتوليد سر مشترك عن طريق المفتاح العمومي المؤقت ***U*** للمرسل والمفتاح الخاص ***v*** للمستقبل. وتأخذ وظيفة اشتقاق المفتاح (KDF) القائمة على البعثرة SHA-256 هذا السر المشترك لتوليد تسلسل مفتاح شفرة استيقان الرسالة (MAC) أي ***K_{MAC}*** ومفتاح فك التجفير ***K_{DEC}***. ويلاحظ أن قيم ***K_{ENC}*** و***K_{DEC}*** متماثلة في خوارزميات المفتاح التناظري؛

– الخطوة 2: توليد العلامة والتحقق من السلامة:

تقوم وظيفة شفرة استيقان الرسالة بتوليد العلامة لنص التجفير ***C*** المستلم بواسطة ***K_{MAC}***. وتقارن العلامة المحسوبة بالعلامة المستلمة. فإذا كانت القيم غير متماثلة، تهمل الرسالة المستلمة بسبب فشل التحقق من سلامة الرسالة؛

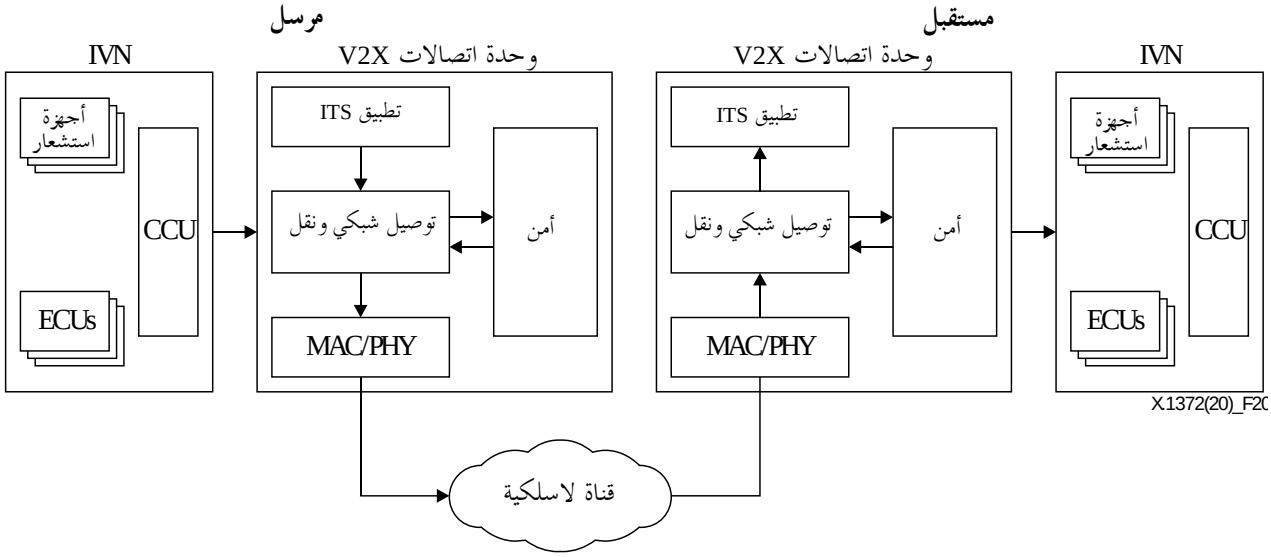
– الخطوة 3: فك تجفير النص المجفر:

يتم فك تجفير نص المجفر ***C*** بواسطة ***K_{DEC}*** باستخدام خوارزميات تجفير تناظري.

يُستخدم ECIES لتجفير مفتاح تناظري لتجفير رسائل V2X باستخدام العملية AES-CCM. لذلك، فإن النص العادي هو في الواقع مفتاح التجفير الخاص من أجل العملية AES-CCM.

2.9 خصوصية رسائل التحذير بشأن السلامة على الطرق في حالة الطوارئ

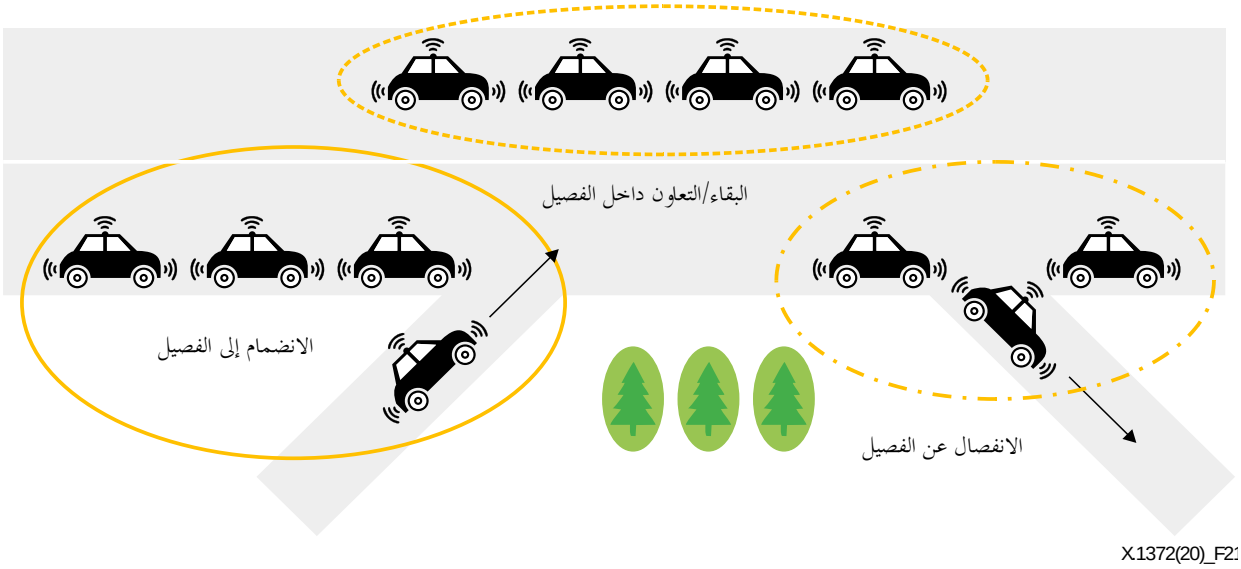
يبين الشكل 20 حالة استخدام عمومية للإنذار في حالات الطوارئ. حيث ترسل وحدة التحكم الإلكتروني في المكابح رسالة إلى وحدة الاتصالات V2X في المركبة من خلال وحدة الاتصالات المركزية (CCU). ويتلقى تطبيق أنظمة النقل الذكية المقابل في وحدة الاتصالات V2X الرسالة من وحدة التحكم ECU في المكابح ويقوم بتوليد رسالة تحذير V2X. وترسل الرسالة المتولدة إلى طبقة توصيل الشبكات والنقل. وينبغي توقيع هذه الرسالة أو تجفيرها بواسطة طبقة الأمان. ثم ترسل الطبقة المادية الرسالة الموقعة أو المجفرة إلى قناة اتصالات لاسلكية. وباستخدام قناة الاتصالات اللاسلكية ترسل الرسالة إلى المستقبل. وفي المستقبل، يتم التحقق من الرسالة أو فك تجفيرها بواسطة طبقة الأمان وتنقل أخيراً إلى الطبقة العليا، وهي تطبيق أنظمة النقل الذكية المقابل. ويمكن لتطبيق الأنظمة ITS المقابل تحديث الخارطة الدينامية المحلية أو تنبيه السائق بواسطة جهاز ذي واجهة بشرية وقد يرسل رسالة تحكم إلى وحدة التحكم ECU في المكابح لتخفيف سرعة المركبة.



الشكل 20 – إجراءات التحذير في حالة الطوارئ

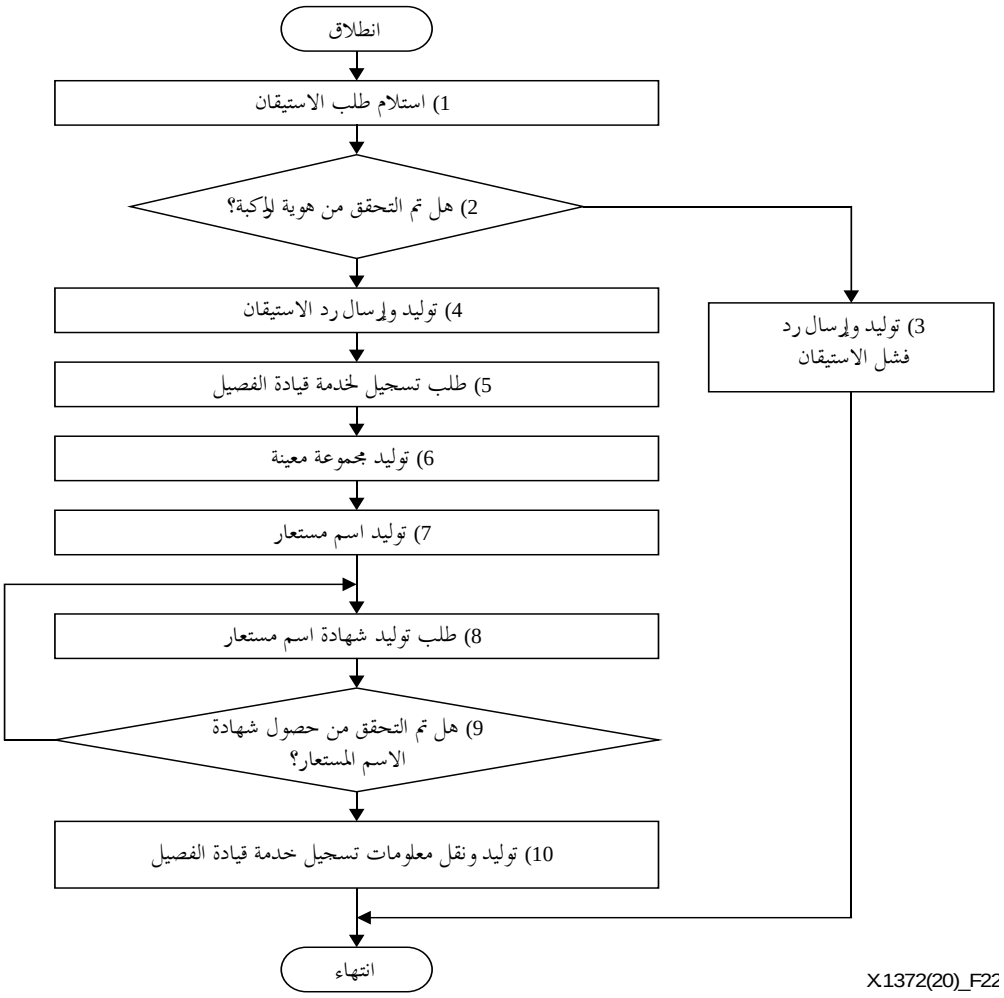
3.9 استيقان الكيان لفصيل من المركبات

يعتبر نهج الفصائل نهج فعال ينطوي على تغيير نمط القيادة من القيادة الفردية إلى القيادة القائمة على أساس الفصيل. والقيادة القائمة على أساس الفصيل هي عبارة عن مجموعة من المركبات ذات اهتمامات مشتركة، حيث تتبع كل مركبة الأخرى وتحافظ على مسافة صغيرة شبه ثابتة من المركبة المتقدمة، وتشكل فصائل كما هو مبين في الشكل 21. وفيما يتعلق بالفصائل هناك ثلاث عمليات رئيسية: الاندماج في الفصيل، والتعاون/البقاء فيه، والانفصال عنه.



الشكل 21 – حالة الانقسام إلى فصائل

- الالتحاق بالفصيل: تتحرك المركبة، التي ليست عضواً في فصيل، وتلتحق بالفصيل عند تقاطع الطريق المقبل؛
- التعاون/البقاء داخل الفصيل: يتعين على المركبات داخل نفس الفصيل التواصل والتعاون فيما بينها للبقاء ضمن الفصيل وتحقيق المهام، مثل إفساح المجال للمركبات ذات الأولوية الأعلى، وتعديل مواقعها بناءً على تخطيط المسار، وعبور تقاطع المرور وتبديل الممرات؛
- الانفصال عن الفصيل: تنفصل المركبة عن فصيلها إلى ممر آخر عند تقاطع الطرق المقبل.



الشكل 22 – إجراءات تسجيل الفصائل

يوضح الشكل 22 مثال استيقانٍ لخدمة القيادة ضمن الفصيل. وفي هذا الشكل، إذا ورد طلب استيقان لتسجيل خدمة قيادة جماعية، أي طلب استيقان مركبة، من مركبة في أسلوب تنفيذ خدمة في الخطوة 1، عندئذ ينبغي التحقق من معرّف هوية المركبة، ومثال ذلك باستخدام خوارزمية توقيع رقمي لنظام تجفير مفتاح عمومي، في الخطوة 2. وهنا يمكن تنفيذ طلب الاستيقان من المركبة بإرسال رسالة موقعة بواسطة مفتاح خاص للمركبة إلى نظام خدمة القيادة الجماعية. ونتيجة للتحقق في الخطوة 2، وإذا تبين أن هوية المركبة غير صالحة، يقوم نظام خدمة القيادة الجماعية بتوليد رد مقابل يفيد بفشل الاستيقان ويرسل الرد إلى المركبة على النحو المبين في الخطوة 3.

ونتيجة للتحقق في الخطوة 2، وإذا تبين أن هوية المركبة صالحة، يقوم نظام خدمة القيادة الجماعية بتوليد رد استيقان للمركبة ويرسل هذا الرد إلى المركبة في الخطوة 4.

وبعد ذلك، وعند استلام رد الاستيقان، أي أن استيقان المركبة قد تحقق، وبعد إدراج مدخلات المستخدم واختيار معلومات تسجيل القيادة الجماعية، بما في ذلك التأهيل للقيادة الجماعية ومكان الانطلاق والوجهة المقصودة والوقت المقدر للمغادرة والوقت المقدر للوصول ومكان الاستراحة المرغوب، ترسل المركبة معلومات تسجيل القيادة الجماعية إلى نظام خدمة القيادة الجماعية، وبذلك تطلب تسجيل خدمة القيادة الجماعية على النحو المبين في الخطوة 5.

ومن ثم، إذا ورد طلب لتسجيل خدمة القيادة الجماعية، يتضمن معلومات تسجيل القيادة الجماعية، من المركبة، فإن نظام خدمة القيادة الجماعية يولد مجموعة معينة باستخدام معلومات تسجيل القيادة الجماعية، من قبيل نفس الوجهة ونفس مكان الانطلاق ونفس الوقت المقدر للوصول وهكذا، ثم يخزن/يسجل المعلومات بشأن مجموعة معينة في معلومات المجموعة على النحو المبين في الخطوة 6.

وهنا، قد تتضمن المجموعة المعينة قائداً واحداً على الأقل، أي مركبة رائدة وعضواً واحداً على الأقل، أي مركبة عضو. وبعد ذلك، يخصص نظام خدمة القيادة الجماعية اسماً مستعاراً لكل مركبة في مجموعة معينة على النحو المبين في الخطوة 7، ويقوم بتوليد رسالة طلب شهادة يطلب فيها توليد شهادة اسم مستعار للاسم المستعار المخصص لكل مركبة في المجموعة المعينة، ويرسل رسالة طلب الشهادة إلى مركز الاستيقان على النحو المبين في الخطوة 8.

ويراقب نظام خدمة القيادة الجماعية ما إذا قد تم الحصول على شهادة اسم مستعار أم لا من مركز الاستيقان في الخطوة 9. ونتيجة لهذه المراقبة، وإذا تم الحصول على شهادة الاسم المستعار، يعمد نظام خدمة قيادة المجموعة إلى تخزين شهادة الاسم المستعار في قاعدة بيانات المجموعة. وقد تكون شهادة الاسم المستعار رسالة موقعة رقمياً من مركز الاستيقان. ومن الممكن ضمان تبرير الاسم المستعار من خلال شهادة الاسم المستعار. والاسم المستعار هو مفتاح عمومي يخصص لكل مركبة من جانب نظام خدمة القيادة الجماعية.

ومن الممكن تخصيص عدد كبير من الأسماء المستعارة لكل مركبة. وبما أن الاسم المستعار لا يحتوي على معلومات مرتبطة بمعرّف هوية كل مركبة، فإن معرّف المركبة المشاركة في مجموعة القيادة يبقى مكتوماً، بحيث يمكن حماية المعلومات المحدِّدة للهوية لكل مركبة مشاركة في مجموعة القيادة.

وإذا تم استلام الإخطار بذلك، يقوم نظام خدمة القيادة الجماعية بتوليد معلومات تسجيل خدمة القيادة الجماعية لمجموعة معينة، ويخزنها في قاعدة بيانات المجموعة، ويرسلها إلى كل مركبة في المجموعة المعينة في الخطوة 10. وهنا قد تتضمن معلومات تسجيل خدمة القيادة الجماعية معرّف هوية المجموعة والاسم المستعار المخصص لكل مركبة وشهادة الاسم المستعار وما إلى ذلك. ويمكن لكل مركبة، أي مستخدم كل مركبة، في المجموعة المحددة التي تم تسجيل خدمة قيادة المجموعة لها، أن تشارك في القيادة الجماعية بإجراء الاتصالات بين المركبات في المجموعة المحددة باستخدام معلومات تسجيل خدمة القيادة الجماعية الواردة من خدمة القيادة الجماعية.

4.9 البنية التحتية للمفاتيح العمومية في المركبات

إن البنية التحتية للمفاتيح العمومية (PKI)، التي تسهل وتدير الشهادات الرقمية، ضرورية لبناء الثقة بين المشاركين في بيئة اتصالات المركبات. وتمتاز البنية PKI في المركبات عن البنية PKI التقليدية في العديد من الجوانب. وأكثر هذه الجوانب أهمية هو استخدام الأسماء المستعارة بغية حماية تعرض موقع المركبة المرتبط بموقع المالك. وعدد الشهادات في هذه البنية ضخم مقارنةً بمثيله في البنية PKI التقليدية. لذلك، فإن الهدف الرئيسي من البنية PKI للمركبات هو توفير أساليب فعالة لطلب الشهادات ومعالجة حالات الإلغاء.

ويصف التذييل II النماذج المرجعية للبنية PKI للمركبات بمزيد من التفاصيل.

التذييل I

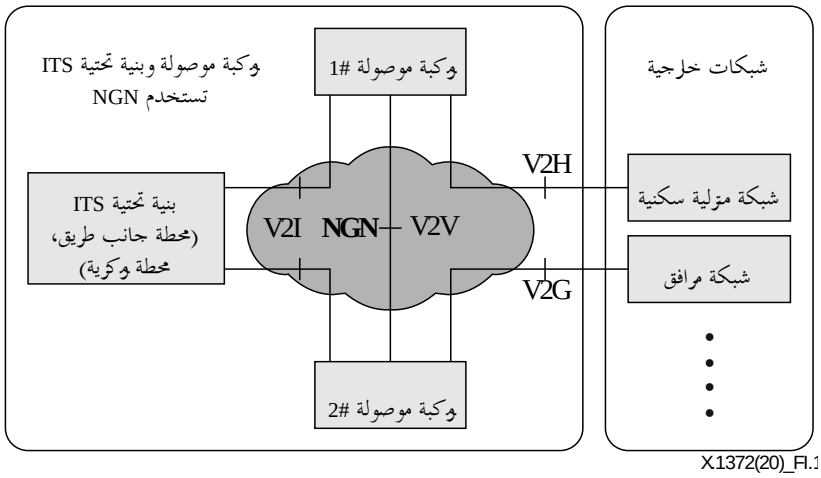
نماذج مرجعية للتواصل بين المركبات

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.I إطار قطاع تقييس الاتصالات لخدمات وتطبيقات المركبات الموصولة التي تستخدم شبكات الجيل التالي

يرد وصف إطار خدمات وتطبيقات المركبات الموصولة في سياق شبكات الجيل التالي (NGN) في التوصية [b-ITU-T Y.2281]. وتعتبر المركبة واحدة من المكونات الهامة التي تستخدم إمكانات الشبكة من حيث الاتصالات بين البنية التحتية (V2I) والمركبة وبين مركبة وأخرى (V2V) وبين المركبة والمنزل (V2H). وفي هذا السياق، يمكن للمركبة الموصولة أن تتعاون مع شبكات الجيل التالي لدعم الخدمات والتطبيقات الأكثر تقدماً، من قبيل تطبيقات السلامة على الطرق والتطبيقات المتعلقة بحركة المرور وخدمات الوسائط المتعددة والتنفيذ القائم على الموقع لهذه الخدمات.

وتحدد التوصية [b-ITU-T Y.2281] العلاقة بين شبكات الجيل التالي ومركبة موصولة وكذلك المتطلبات التي تراعي ضرورة دعم خدمات وتطبيقات المركبات الموصولة التي تستخدم شبكات الجيل التالي. وإضافة إلى ذلك، يرد وصف معمارية إطار للبنية التحتية لأنظمة النقل الذكية للمركبات المتمكنة من شبكات الجيل التالي وذلك لدعم مزايا الاتصالات في شبكة منسقة من شبكات الجيل التالي مع المركبة الموصولة شبكياً.



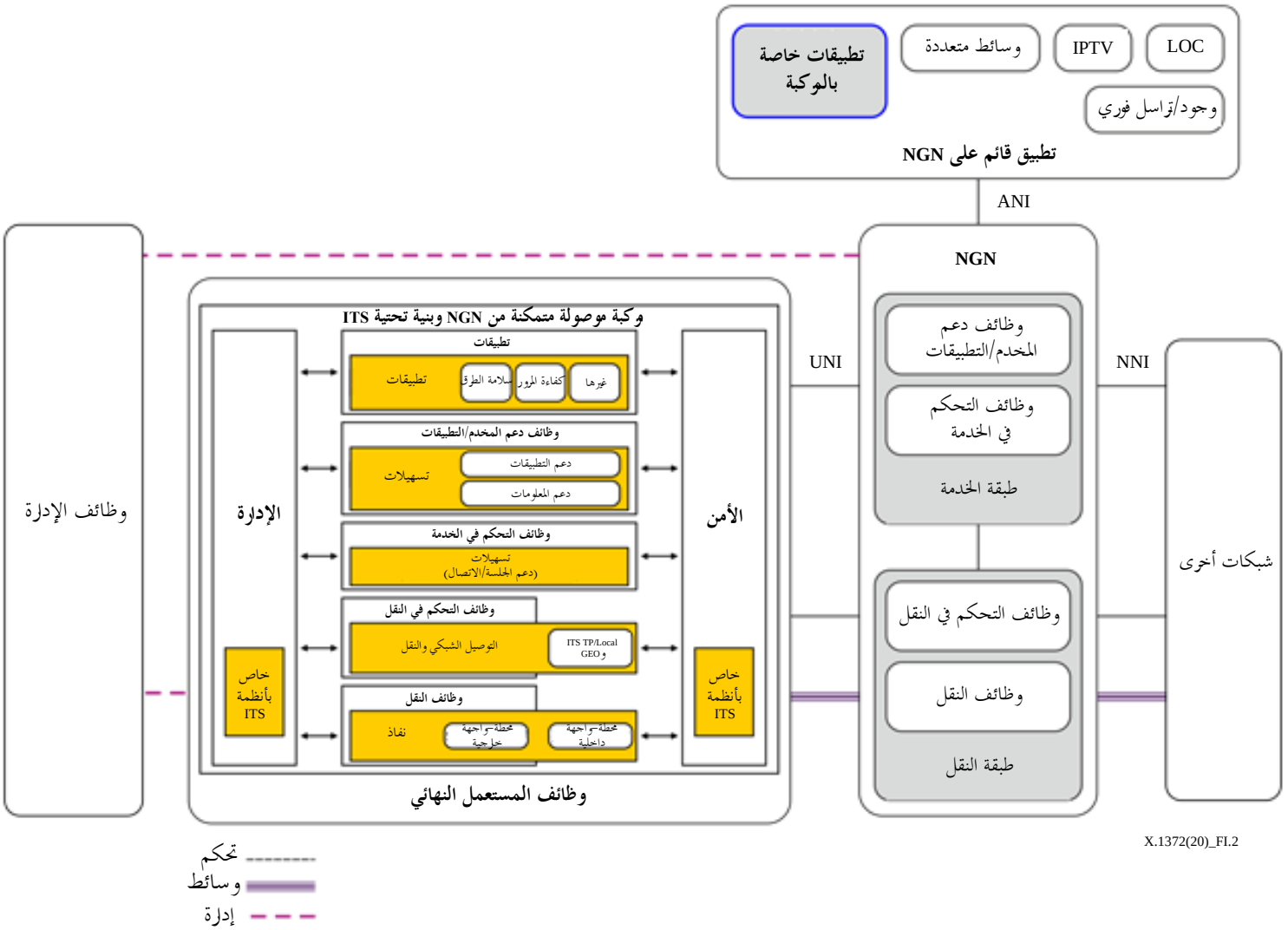
ملاحظة – يعود مصدر الشكل إلى التوصية [b-ITU-T Y.2281].

الشكل 1.I – نموذج التشكيل الإجمالي للمركبة الموصولة والبنية التحتية لأنظمة النقل الذكية

يبين الشكل 1.I نموذج تشكيلٍ بموجب التوصية ITU-T Y.2281 ويوضح كيفية ارتباط المركبات الموصولة بالبنية التحتية لأنظمة النقل الذكية وكذلك بالشبكات الخارجية التي تشمل الشبكات المنزلية وشبكة المرافق لنقل الطاقة باستخدام شبكات الجيل التالي. وبالمقارنة مع المعايير الأخرى لأنظمة النقل الذكية، تركز التوصية [b-ITU-T Y.2281] على استخدام شبكات الجيل التالي في بيئات أنظمة النقل الذكية. وتحدد التوصية [b-ITU-T Y.2281] استخدام شبكات الجيل التالي في بيئات أنظمة النقل الذكية للحد من مشكلات قابلية التشغيل بين اتصالات أنظمة النقل الذكية من الند إلى الند واتصالات شبكة عمومية. وتتسم قابلية التشغيل البيني هذه بأهمية خاصة في دعم جودة الخدمة (QoS) والتنقلية والأمان مع مختلف خدمات الوسائط المتعددة.

ويعرض الشكل 2.I معمارية إجمالية للبنية التحتية للمركبات الموصولة وأنظمة النقل الذكية المتمكنة من شبكات الجيل التالي بالتعاون مع هذه الشبكات. وتتكون شبكات الجيل التالي في هذا الصدد من "وظائف المستخدم النهائي" و"طبقة الخدمة" و"طبقة النقل" و"طبقة الإدارة" و"التطبيقات القائمة على شبكات الجيل التالي". وتقع وظيفة البنية التحتية للمركبات الموصولة

شبكياً وأنظمة النقل الذكية المتمكنة من شبكات الجيل التالي ضمن وظائف المستخدم النهائي في منظور شبكة الجيل التالي. وتصف التوصية [b-ITU-T Y.2281] كيف يتم دعم تطبيقات شبكات الجيل التالي الخاصة بالمركبة، مثل نداء الطوارئ، من خلال هذه الشبكات.



ملاحظة – يعود مصدر الشكل إلى التوصية [b-ITU-T Y.2281].

الشكل 2.I – نظرة مجملة للبنية التحتية للمركبات الموصولة المتمكنة من شبكات الجيل التالي وأنظمة النقل الذكية بالتعاون مع شبكات الجيل التالي

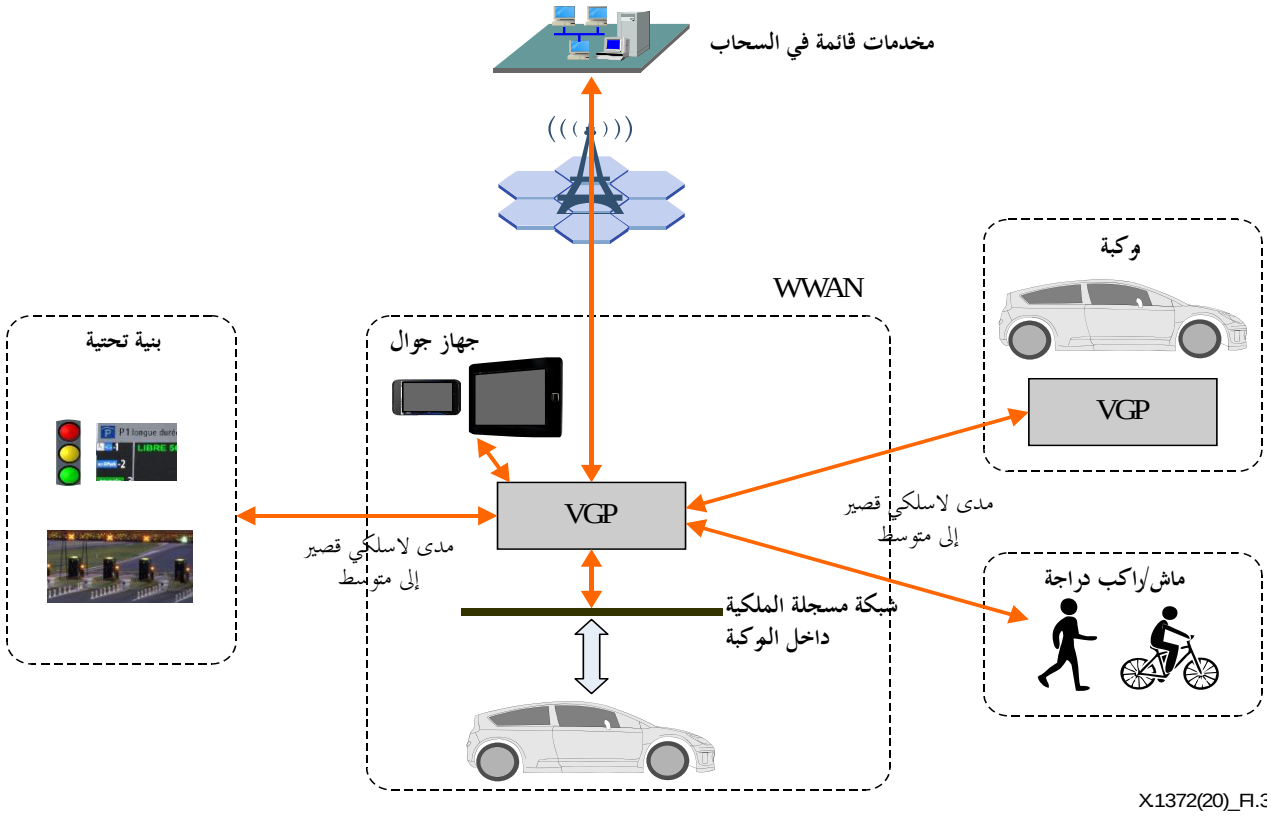
تشير اعتبارات الأمن في التوصية [b-ITU-T Y.2281] إلى التوصية [b-ITU-T Y.2201]. واعتبارات الأمان مطلوبة وفقاً للشبكة الموصولة بالمركبة. ولكن التوصية [b-ITU-T Y.2281] لا تحدد سوى الاعتبارات الأمنية لشبكات الجيل التالي، أما الحالات الأخرى لمتطلبات الأمن فهي خارج نطاق التوصية [b-ITU-T Y.2281].

ويركز إطار قطاع تقييس الاتصالات لخدمات وتطبيقات المركبات الموصولة باستخدام شبكات الجيل التالي على تكييف شبكات الجيل التالي مع بيئة المركبات. ولا تحدد التوصية [b-ITU-T Y.2281] الجوانب الأمنية لبيئة المركبات. وتركز معمارية IEEE بشأن النفاذ اللاسلكي في بيئة المركبات (WAVE)، الموصوفة في المعيار [b-IEEE WAVE]، على واجهة راديوية بمقدار GHz 5,9 لأنها لا تتضمن صراحةً تطبيقاً للتواصل مع شبكة أخرى. وتشير معمارية ETSI ITS، الموصوفة في المعيار [b-ETSI EN 302 665]،

إلى طبقة التطبيق التي هي مكدس من بروتوكولات للاتصال. وبما أن طبقة النفاذ تشتمل على المعيار IEEE 802.x وعلى 3G خلوية وبلوتوث، فإن معمارية ETSI ITS مصممة لدعم مكدسات متعددة لبروتوكولات الشبكات.

2.I معمارية قطاع تقييس الاتصالات والكيانات الوظيفية لمنصات بوابات المركبات

جرت دراسة المعمارية والكيانات الوظيفية لمنصة بوابة المركبات (VGP) في إطار لجنة الدراسات 16 لقطاع تقييس الاتصالات. ويرد وصف المعمارية وإطار المعمارية الوظيفية والكيانات الوظيفية لمنصات بوابة المركبات في التوصية [b-ITU-T H.550]. ويرد تعريف المصطلح VGP في التوصية [ITU-T F.749.1]. والمنصة VGP هي مجموعة من أجهزة وبرمجيات تكنولوجيا المعلومات والاتصالات في مركبة تعمل كمنصة مفتوحة لتوفير بيئة زمن تشغيل متكاملة لتقديم خدمات الاتصالات لبوابة مركبات. وقد توفر المنصة VGP أيضاً خدمات اتصالات لطبقة أعلى، من قبيل التفاعل من خلال خدمات النفاذ مع سائق المركبة وما إلى ذلك. ولا تعتبر الأنظمة الفرعية المخصصة فقط لتشغيل المركبات جزءاً من المنصة VGP.



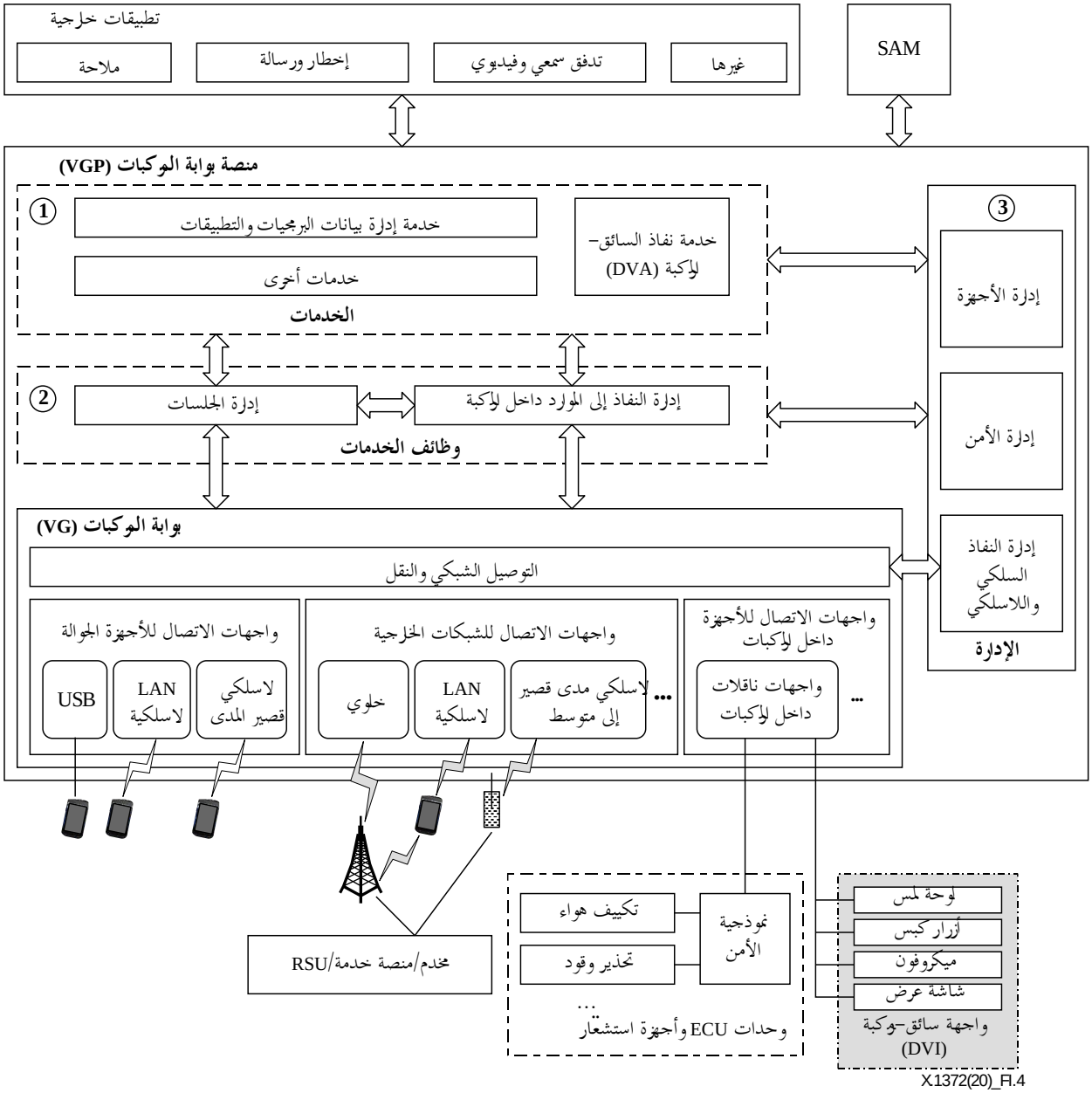
ملاحظة – يعود مصدر الشكل إلى التوصية [b-ITU-T H.550].

الشكل 3.I – موقع منصة بوابة المركبات في النموذج المرجعي لأنظمة النقل الذكية

يبين الشكل 3.I موقع المنصة VGP في النموذج المرجعي لأنظمة النقل الذكية (ITS): هناك ستة سيناريوهات رئيسية للاتصالات وهي من مركبة إلى مركبة، ومن مركبة إلى بنية تحتية، ومن مركبة إلى مخدم في سحابة، ومن مركبة إلى جهاز جوال، ومن مركبة إلى أحد المشاة أو راكب دراجة، والتفاعل مع شبكة داخل المركبة.

- يصف سيناريو الاتصالات من مركبة إلى مركبة (V2V) أساساً سيناريوهات السلامة والقيادة التلقائية التي تتواصل فيها المركبات فيما بينها؛
- يصف سيناريو الاتصالات من مركبة إلى البنية التحتية (V2I) أساساً سيناريوهات السلامة وتحصيل الرسوم إلكترونياً (ETC) وتبادل معلومات المرور التي تتواصل فيها المركبات مع البنية التحتية على جانب الطريق؛

- يصف سيناريو الاتصالات من المركبة إلى مخدم في سحابة أساساً سيناريوهات نداءات الطوارئ والتليماتية التي تتواصل فيها المركبات مع الخدمات القائمة في سحابة؛
- يصف سيناريو الاتصالات من المركبة إلى الجهاز الجوال أساساً سيناريوهات الاتصالات السلكية واللاسلكية وواجهة المستخدم (UI) عن بُعد التي تتواصل بها المركبات بالأجهزة الجوالة؛
- يصف سيناريو الاتصالات من المركبة إلى المشاة أو راكبي الدراجات أساساً سيناريوهات تحذير السلامة التي تتواصل فيها المركبات مع الأجهزة التي يحملها المشاة أو راكبو الدراجات؛
- يصف سيناريو التفاعل مع الشبكة داخل المركبة أساساً تشخيصات المركبة وجمع البيانات عن بُعد والتحكم عن بُعد في المركبة التي تتواصل فيها المنصة VGP بشبكة مسجلة الملكية داخل المركبة.



ملاحظة – يعود مصدر الشكل إلى التوصية [b-ITU-T H.550].

الشكل 4.I – معمارية رفيعة المستوى لمنصة بوابة المركبات

يعرض الشكل 4.I معمارية الطبقة العالية للمنصة VGP. وتتضمن خدمات المنصة VGP البرمجيات وخدمة إدارة بيانات التطبيق، وخدمة النفاذ إلى سائق المركبة، والخدمات الأخرى (انظر الإطار (1) في الشكل 4.I). وتشمل وظائف الخدمة إدارة الجلسة وإدارة النفاذ إلى الموارد داخل المركبة (انظر الإطار (2) في الشكل 4.I). وتشمل الإدارة إدارة الأجهزة وإدارة الأمن وإدارة النفاذ السلكي واللاسلكي (انظر الإطار (3) في الشكل 4.I). وتدعم الخدمات التطبيقات الخارجية مثل الملاحة والإعلام والتسلية من أجل إقامة الجلسة وتحويل نسق البيانات والمعالجة المحددة.

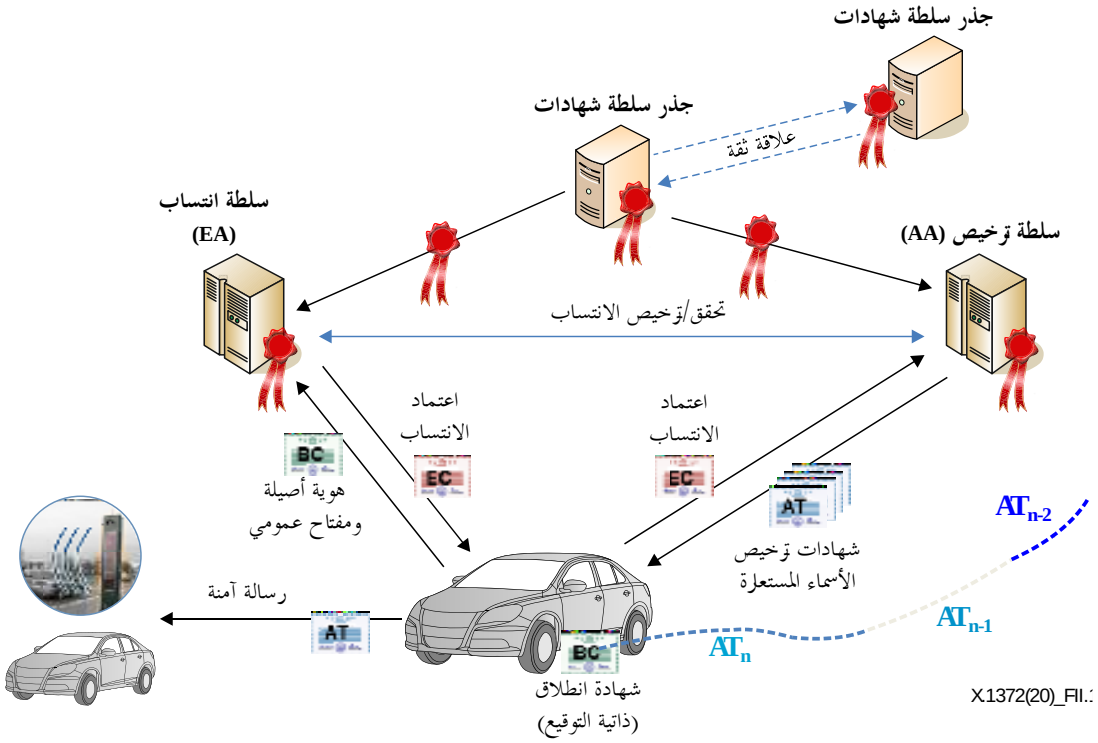
ويرد وصف جانب الأمن في المنصة VGP كجزء من طبقة الإدارة في التوصية [b-ITU-T H.550]. ويرد وصف عمومي لوظيفة الأمن في الفقرة 4.8.I من التوصية [b-ITU-T H.550] بشأن "إدارة الأمن". وهو يتألف من إدارة الأمان لطبقة النفاذ، التي تشمل طبقة النقل والشبكة، وإدارة الأمن للخدمات/التطبيقات.

التذييل II

نماذج مرجعية للبنية التحتية للمفاتيح العمومية في المركبات

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

تشمل وظائف أمن اتصالات أنظمة النقل الذكية الراهنة استيقان الرسائل، التي لها أثر على خصوصية المركبات والرحلات. وعلى المستوى الأوروبي، عرّف المعهد الأوروبي لمعايير الاتصالات (ETSI) آلية استيقان الرسائل التي تعتمد على البنية التحتية للمفاتيح العمومية بأنها بنية تحتية للمفاتيح العمومية للمركبات كما هو موضح في الشكل 1.II.



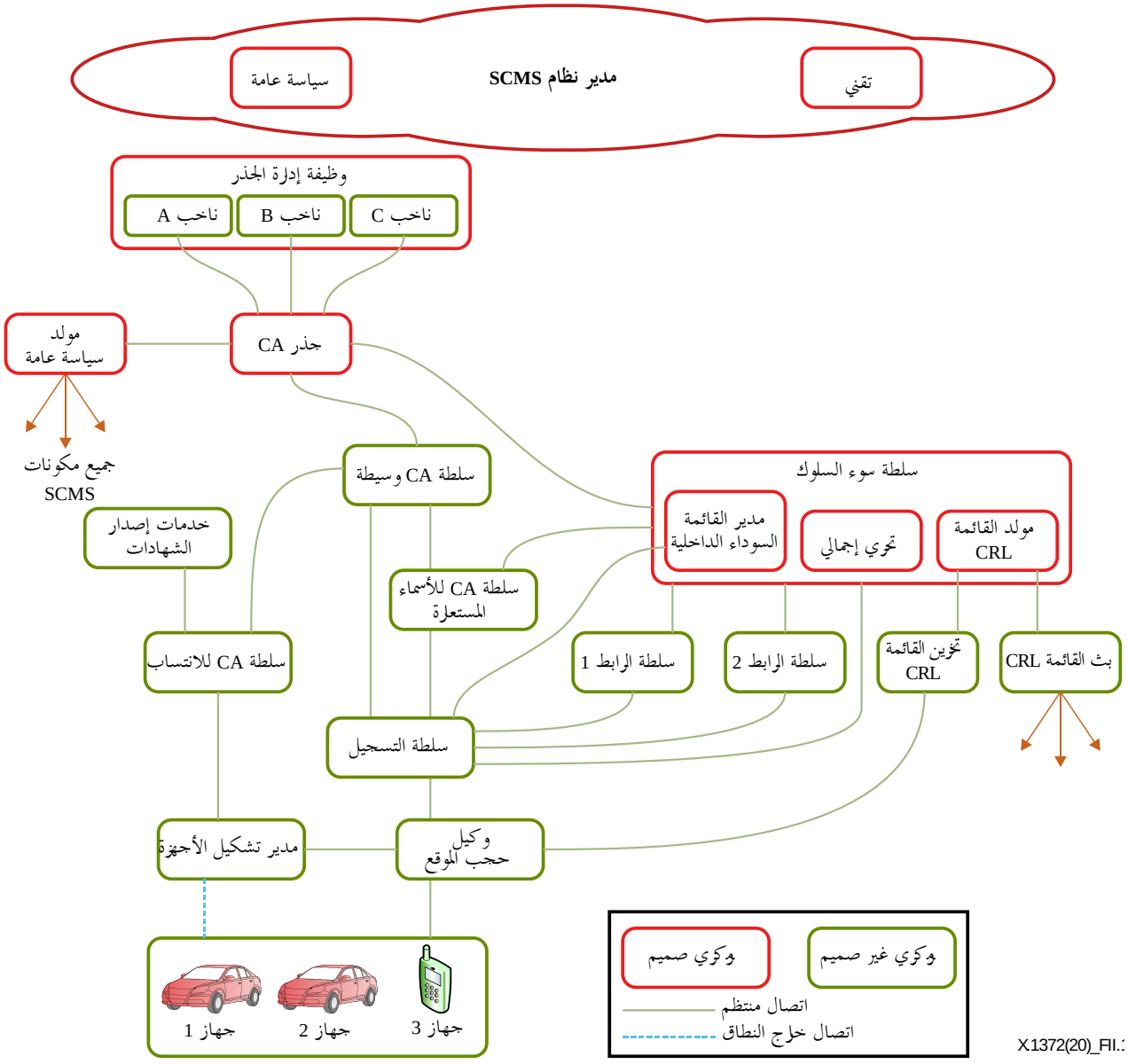
الشكل 1.II – البنية التحتية للمفاتيح العمومية للمركبات بحسب ETSI (المصدر: [b-ETSI TS 102 940])

إن سلطة الشهادات الجذرية (RCA) هي نقطة البداية لسلسلة موثوقية الشهادات، وهي توقع شهادات السلطتين الأخريين (من قبيل سلطة الترخيص (AA) وسلطة الانتساب (EA)) وتنظم قائمة إبطال الشهادات (CRL) وتحافظ عليها، وقائمة التراخيص المبطلة. وفي السياق التشغيلي، تدار السلطة RCA من قبل جهة فاعلة يمكنها ضمان سوية عالية ومستقرة من الثقة وتكون جامعة بدرجة كافية، من قبيل دولة أو مجموعة من الدول. وسلطة الانتساب هي الجهة التي تصدر شهادات الانتساب (EC) وتتحقق من صحة طلبات تذاكر الترخيص. وسلطة الترخيص هي طرف ثالث موثوق به يوفر تذاكر الترخيص (AT) لمحطات أنظمة النقل الذكية. ولا تعرف السلطة AA هوية محطة ITS وتعتمد على سلطة الانتساب للتحقق مما إذا كانت المحطة مرخص لها أم لا للحصول على تذكرة الترخيص. ويتضمن طلب تذكرة الترخيص هوية سلطة الانتساب حيث يتم تسجيل المحطة ITS.

والغرض من هذه المعمارية هو توفير الخصوصية لمحطات ITS وتجنب التتبع: فسلطة الانتساب تعرف هوية المحطة ولكنها لا تعرف شهادات الأسماء المستعارة التي تستخدمها، بينما تعرف سلطة الترخيص شهادة الاسم المستعار للمحطة ولكنها لا تعرف هويتها. وتسجل المحطة نفسها لدى سلطة الانتساب وتحصل على شهادة انتساب. وتستخدم شهادة الانتساب لطلب هويات الأسماء المستعارة من أجل سلطة الترخيص: عندما تطلب المحطة تذكرة ترخيص، ترسل في رسالة الطلب هويتها المجفرة مع شهادة الانتساب وهوية سلطة الانتساب. وتتلقى سلطة الترخيص طلب اسم مستعار، وتقرأ معرّف هوية سلطة الانتساب وتتحقق من نقطة نفاذ سلطة الانتساب

للتحقق من صحة طلب تذكرة الترخيص. وتحقق سلطة الانتساب من شهادة الانتساب لمحطة ITS وتصادق (أو لا تصادق) على صحة الطلبات. وإذا تم التحقق من صحة الطلب، تقوم سلطة الترخيص بتوليد تذكرة الترخيص وترسلها إلى المحطة.

ومن ناحية أخرى، تقدم شراكة قياسات تجنب التصادم (CAMP) نظام إدارة بيانات اعتماد الأمان (SCMS) لضمان الاتصالات من المركبة إلى كل شيء (انظر المرجع [b-SCMS]). وهذا يعتمد على البنية التحتية للمفاتيح العمومية لضمان الاتصالات V2X وهي تنتقل حالياً من مرحلة البحوث إلى مرحلة برهان المفهوم. ويدعم النظام SCMS عملية الانطلاق وتوفير الشهادات والإبلاغ عن سوء السلوك والإلغاء.



ملاحظة – يعود المصدر إلى المرجع [b-SCMS].

الشكل 2.II – البنية التحتية للمفاتيح العمومية للمركبات (V-PKI) في إطار الشراكة CAMP

يقدم الشكل 2.II نظرة عامة لمعمارية نظام إدارة بيانات اعتماد الأمان (SCMS). ويتم التعبير عن العلاقات بين مكونات النظام SCMS المختلفة في شكل خطوط، وهي تشير إلى كل مكونة ترسل معلومات أو شهادات إلى المكونات الأخرى.

والمكونات الرئيسية للنظام SCMS هي كما يلي:

- سلطة شهادات الانتساب (ECA): تصدر شهادات الانتساب لجهاز ما ويمكن استخدامها لطلب شهادات أسماء مستعارة لمناطق جغرافية مختلفة أو مصنّعين أو أنواع من الأجهزة؛
- سلطة الشهادة الوسيطة (ICA): هي سلطة إصدار شهادات ثانوية لتخفيف العبء على سلطة شهادات الجذر جراء حركة مرور كثيفة، وتصدر هذه الشهادة عن سلطة شهادات الجذر؛
- سلطة الربط (LA): تقوم بتوليد قيم ما قبل الربط لتشكيل قيم الارتباط التي توضع في الشهادات لضمان كفاءة الإلغاء. وعلاوةً على ذلك، فإن الغرض من تقسيم سلطات الربط هو منع مشغل سلطة ربط ما من ربط الشهادات التابعة لجهاز معين؛
- وسيط حجب الموقع (LOP): يقوم بتغيير عنوان المصدر لإخفاء موقع الجهاز الطالب ومنع ربط عناوين الشبكة بالمواقع؛
- سلطة سوء السلوك (MA): تتلقى وتعالج تقارير سوء السلوك من الأجهزة لتحديد سوء السلوك أو الخلل الوظيفي المحتمل. وبالإضافة إلى ذلك، تقوم بإلغاء شهادة الجهاز وتضعها في قائمة إبطال الشهادات. وتستهل سلطة سوء السلوك أيضاً عملية ربط معرف الشهادة بشهادات الانتساب المقابلة ووضعها في القائمة السوداء الداخلية لسلطة التسجيل؛
- مولّد السياسة (PG): يحتفظ بتحديثات ملف السياسة الإجمالية لسلطة التسجيل. ويحتوي ملف السياسة الإجمالية على معلومات التشكيل الإجمالية، وملف سلسلة الشهادات الإجمالية، الذي يحتوي على جميع سلاسل الثقة في النظام SCMS؛
- سلطة شهادات الاسم المستعار (PCA): تصدر شهادات الاسم المستعار على المدى القصير وشهادات الهوية والتطبيق للأجهزة. وتقتصر كل سلطة PCA على منطقة جغرافية معينة أو شركة تصنيع معينة أو نوع جهاز؛
- سلطة التسجيل (RA): تقوم بالتحقق من الطلبات الواردة من الجهاز ومعالجتها، وتضمن أن الأجهزة المبطلة غير قادرة على إصدار شهادات أسماء مستعارة جديدة. وبالإضافة إلى ذلك، لا تصدر السلطة RA أكثر من مجموعة واحدة من الشهادات لفترة زمنية معينة لجهاز ما. وعلاوةً على ذلك، تقوم السلطة RA بتخليط الطلبات أو التقارير قبل إرسال طلبات توقيع شهادة الأسماء المستعارة إلى السلطة PCA أو إعادة توجيه المعلومات إلى السلطة MA؛
- سلطة الشهادات الجذرية (RCA): هي جذر وأعلى سلسلة شهادات في النظام SCMS. وهي تصدر شهادات من أجل كل من سلطة الشهادة الوسيطة ومولد السياسة وسلطة سوء السلوك.

بيبليوغرافيا

[b-ITU-T F.749.1] Recommendation ITU-T F.749.1 (2015), *Functional requirements for vehicle gateways*.

[b-ITU-T H.550] Recommendation ITU-T H.550 (2017), *Architecture and functional entities of vehicle gateway platforms*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.641] Recommendation ITU-T X.641 (1997), *Information technology – Quality of service: framework.*

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

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

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

[b-ITU-T X.1371] Recommendation ITU-T X.1371 (2019), *Security threats to connected vehicles*.

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN*.

[b-ITU-T Y.2281] Recommendation ITU-T Y.2281 (2011), *Framework of networked vehicle services and applications using NGN*.

[b-ETSI EN 302 665] ETSI EN 302 665 V1.1.1 (2010-09), *Intelligent Transport Systems (ITS); Communications Architecture*.
<https://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf>

[b-ETSI TS 102 940] ETSI TS 102 940 V1.3.1 (2018-04), *Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management*.
<https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf>

[b-IEEE WAVE] IEEE Std. 1609.2 (2016), *IEEE Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages*.

[b-ISO 13185-1] ISO/TR 13185-1:2012, *Intelligent transport systems – Vehicle interface for provisioning and support of ITS services – Part 1: General information and use case definition*.

[b-OVERSEE] Open Vehicular Secure Platform, OVERSEE Project. (Website).
<https://www.oversee-project.com/>

[b-RITA] United States Department of Transportation, FHWA-JPO-11-130 (2011), *An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues*.
<https://rosap.ntl.bts.gov/view/dot/3334/Share>

[b-SCMS] Crash Avoidance Metrics Partners (CAMP LLC) Vehicle Safety Communications 5 (VSC5) Consortium, *Security Credential Management System Proof-of-Concept Implementation, EE Requirements and Specifications Supporting SCMS Software Release 1.1, 04*. May. 2016.
<https://www.its.dot.gov/pilots/pdf/SCMS_POC_EE_Requirements.pdf>

[b-UNECE GRVA] United Nations Secretary of the Informal document GRVA-01-17, *Draft recommendation on cyber security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA*.

[b-US DOT] United States Department of Transportation, Safety Pilot Program. <https://www.its.dot.gov/research_archives/safety/safety_pilot_plan.htm>

[b-USDOTHS812014] United States Department of Transportation, National Highway Traffic Safety Administration, DOT HS 812 014 (2014), *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*. <https://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf>

[b-US GOV] United States Senator for Massachusetts, Edward J, Markey, Staff Report (2015), *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*. <http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf>

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