Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1364

(03/2020)

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

Applications et services sécurisés (2) – Sécurité de l'Internet des objets (IoT)

Exigences et cadre de sécurité applicables à l'Internet des objets à bande étroite

Recommandation UIT-T X.1364

Union internationale des télécommunications

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	**X.1360–X.1369**
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1429
Sécurité de la technologie des registres distribués	X.1430–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATION QUANTIQUE	X.1700–X.1729

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

Recommandation UIT-T X.1364

Exigences et cadre de sécurité applicables à l'Internet des objets à bande étroite

Résumé

La Recommandation UIT-T X.1364 analyse les modèles de déploiement possibles et les scénarios d'application types de l'Internet des objets à bande étroite (NB-IoT). Elle indique les menaces pour la sécurité et les exigences de sécurité propres aux déploiements de l'IoT à bande étroite et établit un cadre de sécurité permettant aux opérateurs de protéger les nouvelles applications technologiques de l'IoT à bande étroite.

L'évolution actuelle des technologies des télécommunications fait que l'on passe, dans le domaine des communications mobiles, de communications de personne à personne à des communications de personne à objet et d'objet à objet, et rend inévitable l'évolution vers l'IoT.

Par rapport aux technologies de communication à courte distance, par exemple Bluetooth, ZigBee et autres technologies, les réseaux mobiles cellulaires caractérisés par une large couverture, la mobilité et de nombreuses connexions donnant lieu à des scénarios d'application plus riches vont devenir la principale technologie d'interconnexion de l'IoT.

L'IoT à bande étroite s'appuie sur la technologie de réseau mobile cellulaire et utilise une bande passante d'environ 180 kHz seulement. Il peut être déployé directement sur des réseaux GSM (système mondial de communications mobiles), des réseaux UMTS (système universel de télécommunications mobiles) ou sur des réseaux LTE (évolution à long terme) afin de réduire les coûts et d'effectuer une transition progressive.

Du fait de sa faible dissipation d'énergie, de sa large couverture, de son faible coût et de sa grande capacité, l'IoT à bande étroite devrait être largement adopté par les opérateurs avec de nombreuses applications dans plusieurs secteurs verticaux.

En tant que nouvelle technologie, l'IoT à bande étroite possède ses propres caractéristiques qui peuvent poser de nouveaux problèmes de sécurité. Afin de garantir la sécurité des déploiements et des applications NB-IoT, il est nécessaire d'analyser les menaces pour la sécurité et les exigences de sécurité pertinentes propres à l'IoT à bande étroite et d'établir un cadre général pour la sécurité de l'IoT à bande étroite.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1364	26-03-2020	17	11.1002/1000/14088

Mots clés

Cadre, Internet des objets, bande étroite, exigences de sécurité.

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

AVANT-PROPOS

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

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

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

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

NOTE

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

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1364

Exigences et cadre de sécurité applicables à l'Internet des objets à bande étroite

1 Domaine d'application

La présente Recommandation analyse les modèles de déploiement possibles et les scénarios d'application types de l'Internet des objets à bande étroite (IoT à bande étroite) . Elle indique les menaces pour la sécurité et les exigences de sécurité propres aux déploiements de l'IoT à bande étroite et établit un cadre de sécurité permettant aux opérateurs de protéger ces nouvelles applications technologiques de l'IoT à bande étroite.

2 Références

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

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

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

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 authentification [b-UIT-T X.1141]: processus permettant de déterminer si quelqu'un ou quelque chose est ce qu'il déclare être, avec un certain degré de confiance.

3.1.2 capacité [b-UIT-T X.1145]: possibilité qu'un système ou un équipement fournit pour offrir un service.

3.1.3 IoT cellulaire [ETSI TS 123 401]: réseau cellulaire prenant en charge des dispositifs peu complexes et à bas débit pour un réseau d'objets connectés. L'IoT cellulaire prend en charge le trafic IP ainsi que le trafic non IP.

3.1.4 intégrité des données [b-UIT-T X.800]: propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée.

3.1.5 chiffrement [b-UIT-T X.800]: transformation cryptographique de données produisant un cryptogramme.

NOTE – Le chiffrement peut être irréversible. Dans ce cas, le déchiffrement correspondant ne peut pas être effectué.

3.1.6 entité [b-UIT-T X.1252]: élément qui a une existence séparée et distincte et peut être identifié dans un contexte.

NOTE – Une entité peut être une personne physique, un animal, une personne morale, une organisation, une chose active ou passive, un dispositif, une application logicielle, un service, etc., ou un groupe de ces entités. Dans le contexte des télécommunications, il peut s'agir de points d'accès, d'abonnés, d'utilisateurs, d'éléments de réseau, de réseaux, d'applications logicielles, de services et de dispositifs, d'interfaces, etc.

3.1.7 réseau central évolué en mode paquet [b-UIT-T Q.1743]: cadre d'évolution ou de migration du système 3GPP vers un système à plus haut débit de données, à plus faible latence et optimisé pour le mode paquet, qui prend en charge plusieurs technologies RAT.

3.1.8 système évolué en mode paquet [b-UIT-T Q.1743]: évolution du système UMTS de troisième génération (3G) caractérisée par un système à plus haut débit de données, à plus faible latence et optimisé pour le mode paquet, qui prend en charge plusieurs technologies RAT. Le système évolué en mode paquet comporte le réseau central évolué en mode paquet et le réseau d'accès radioélectrique évolué (E-UTRA et E-UTRAN).

3.1.9 gestion des clés [b-UIT-T X.800]: production, stockage, distribution, suppression, archivage et application de clés conformément à la politique de sécurité.

3.1.10 Internet des objets à bande étroite [ETSI TS 123 401]: technologie d'accès radioélectrique 3GPP qui fait partie de l'IoT cellulaire. Elle permet d'accéder à des services de réseau via un réseau E-UTRAN avec une bande passante limitée à 180 kHz (correspondant à un bloc PRB). Sauf indication contraire, l'IoT à bande étroite est un sous-ensemble du réseau E-UTRAN.

3.1.11 menace [b-UIT-T X.800]: violation potentielle de la sécurité.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 nœud de passerelle de desserte CIoT (C-SGN, *CIoT serving gateway node*): un nœud de passerelle de desserte pour l'Internet des objets cellulaire (CIoT) (C-SGN) est une option de mise en œuvre de réseau central évolué en mode paquet (EPC) à nœud combiné qui réduit au minimum le nombre d'entités physiques en mettant ensemble les entités du système évolué en mode paquet (EPS) sur les trajets dans les plans de commande et utilisateur (par exemple, entité de gestion de la mobilité (MME), passerelle de desserte (S-GW), passerelle de réseau de données en mode paquet (P-GW)), qui pourra être privilégiée dans les déploiements CIoT.

NOTE – Les fonctions indiquées dans cette définition renvoient à la publication [ETSI TS 123 401].

3.2.2 nœud B évolué (eNodeB): nœud d'accès hertzien qui héberge des fonctions de gestion des ressources radioélectriques, de décompression et de chiffrement des données sur la liaison montante pour le flux de données d'utilisateur, d'acheminement des données dans le plan utilisateur, etc.

NOTE – Les fonctions indiquées dans cette définition renvoient à la publication [ETSI TS 123 401].

3.2.3 réseau d'accès hertzien de Terre universel évolué (E-UTRAN, *evolved universal terrestrial radio access network*): réseau d'accès hertzien dont les fonctions comprennent la compression de l'en-tête et le chiffrement du plan utilisateur, la sélection de l'entité MME, le contrôle du débit au niveau du support sur les liaisons montante et descendante, la commande d'admission au niveau du support, le contrôle de l'encombrement, etc.

NOTE – Les fonctions indiquées dans cette définition renvoient à la publication [ETSI TS 123 401].

3.2.4 serveur d'abonné résidentiel (HSS, *home subscriber server*): élément de réseau central mobile doté des fonctions de stockage et de gestion des informations d'abonnement de l'utilisateur.

NOTE – Les fonctions indiquées dans cette définition renvoient à la publication [ETSI TS 123 401].

3.2.5 entité de gestion de la mobilité (MME, *mobility management entity*): élément de réseau central mobile doté des fonctions de gestion de la liste de zones de suivi, de cartographie des emplacements des équipements d'utilisateur (EU), de sélection des passerelles de desserte (S-WG)

et de réseau de données en mode paquet (P-WG), de sélection des transferts, d'authentification, d'autorisation, de gestion du support, etc.

NOTE – Les fonctions indiquées dans cette définition renvoient à la publication [ETSI TS 123 401].

3.2.6 passerelle de réseau de données en mode paquet (P-WG, *packet data network gateway*): élément de réseau central mobile doté des fonctions de filtrage des paquets par utilisateur, d'attribution d'adresse de protocole Internet (IP) d'équipement d'utilisateur (UE), de marquage des paquets au niveau du transport, de facturation au niveau du service, etc.

NOTE – Les fonctions indiquées dans cette définition renvoient à la publication [ETSI TS 123 401].

3.2.7 fonction d'exposition des capacités de service (SCEF, *service capability exposure function*): élément de réseau central mobile doté des fonctions d'authentification et d'autorisation, de découverte des capacités de service exposées, de gestion des politiques, de configuration des paramètres de réseau, etc.

NOTE – les fonctions indiquées dans cette définition renvoient à la publication [ETSI TS 123 401].

3.2.8 passerelle de desserte (S-WG, *serving gateway*): élément de réseau central mobile doté des fonctions de point d'ancrage local de mobilité pour les transferts entre nœuds B évolués, d'ancrage de la mobilité pour la mobilité entre réseaux 3GPP, d'acheminement et de retransmission des paquets, de marquage des paquets au niveau du transport, de comptabilité pour la facturation entre opérateurs, etc.

NOTE – Les fonctions indiquées dans cette définition renvoient à la publication [ETSI TS 123 401].

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

3G	troisième génération
3GPP	projet de partenariat de troisième génération (*3rd generation partnership project*)
AMRC	accès multiple par répartition en code
CIoT	Internet des objets cellulaire (*cellular Internet of Things*)
C-SGN	nœud de passerelle de desserte CIoT (*CIoT serving gateway node*)
DDoS	déni de service réparti (*distributed denial of service*)
eNodeB	nœud B évolué (*evolved node B*)
EPC	réseau central évolué en mode paquet (*evolved packet core*)
EPS	système évolué en mode paquet (*evolved packet system*)
E-UTRAN	réseau d'accès hertzien de Terre universel évolué (*evolved universal terrestrial access network*)
GSM	système mondial de communications mobiles (*global system for mobile communication*)
HSS	serveur d'abonné résidentiel (*home subscriber server*)
IMEI	identité internationale d'équipement mobile (*international mobile equipment identity*)
IP	protocole Internet (*Internet protocol*)
LTE	évolution à long terme (*long term evolution*)
MME	entité de gestion de la mobilité (*mobility management entity*)
NB-IoT	Internet des objets à bande étroite (*narrow band Internet of Things*)

P-GW passerelle de réseau de données à commutation par paquets (*packet data network gateway*)

RAT technologie d'accès radioélectrique (*radio access technology*)

SCEF fonction d'exposition des capacités de service (*service capability exposure function*)

S-GW passerelle de desserte (*serving gateway*)

SIM module d'identification de l'abonné (*subscriber identification module*)

SMS service de messages courts (*short message service*)

UE équipement d'utilisateur (*user equipment*)

UMTS système de télécommunications mobiles universelles (*universal mobile telecommunications system*)

UTRA accès radioélectrique de Terre universel (*universal terrestrial radio access*)

5 Conventions

Aucune.

6 Aperçu de l'Internet des objets à bande étroite

L'évolution actuelle des technologies des télécommunications fait que l'on passe, dans le domaine des communications mobiles, de communications de personne à personne à des communications de personne à objet et des communications d'objet à objet, et rend inévitable l'évolution vers l'Internet des objets.

Par rapport aux technologies de communication à courte distance, par exemple Bluetooth ou ZigBee, entre autres, les réseaux mobiles cellulaires caractérisés par une large couverture, la mobilité et de nombreuses connexions pouvant donner lieu à des scénarios d'application plus riches vont devenir la principale technologie d'interconnexion de l'IoT.

L'IoT à bande étroite (NB-IoT) s'appuie sur un réseau mobile cellulaire qui utilise une bande passante d'environ 180 kHz seulement Il pourrait être déployé directement sur les réseaux GSM (système mondial de communications mobiles), les réseaux UMTS (système universel de télécommunications mobiles) ou sur les réseaux LTE (évolution à long terme) afin de réduire les coûts et d'effectuer une transition progressive.

Les caractéristiques propres à l'IoT à bande étroite sont les suivantes:

– faible dissipation d'énergie: les dispositifs NB-IoT pourraient être utilisés pendant cinq à dix ans;
– large couverture: dans la même bande, l'IoT à bande étroite offre un gain de 15 à 20 dB par rapport au réseau actuel et une zone de couverture jusqu'à 100 fois plus grande;
– grande capacité: un seul secteur NB-IoT pourrait prendre en charge quelque 100 000 dispositifs; et
– faible coût: un dispositif NB-IoT coûte environ 5 USD.

Du fait de sa faible dissipation d'énergie, de sa large couverture, de son faible coût et de sa grande capacité, l'IoT à bande étroite devrait être largement adopté par les opérateurs avec de nombreuses applications dans plusieurs secteurs verticaux.

7 Modèle de déploiement et scénarios d'application types

7.1 Modèle de déploiement

7.1.1 Déploiement avec le réseau central mobile existant

Dans ce scénario de déploiement, les opérateurs déploient l'IoT à bande étroite en utilisant les réseaux centraux mobiles 2/3/4G déjà déployés.

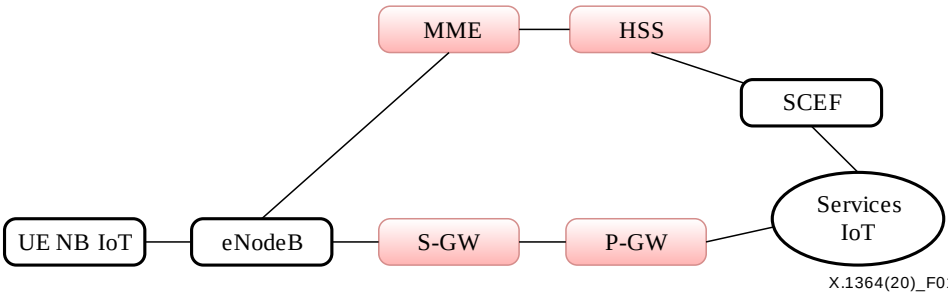
Il est nécessaire d'optimiser les éléments d'un réseau central mobile, notamment l'entité de gestion de la mobilité (MME), la passerelle de desserte (S-GW) et la passerelle de réseau de données en mode paquet (P-GW) pour l'IoT à bande étroite, afin qu'ils puissent prendre en charge les caractéristiques [ETSI TS 123 401] suivantes:

– très faible consommation d'énergie des équipements d'utilisateur (UE);

– grand nombre de dispositifs par cellule;

– technologies d'accès radioélectrique (RAT) à bande étroite, par exemple réseau d'accès hertzien de Terre universel évolué (E-UTRAN), accès radioélectrique de Terre universel (UTRA), GSM, CDMA2000; et

– couverture étendue.



NOTE – Les éléments du réseau central mobile existant sont indiqués en rose.

Figure 1 – Déploiement avec un réseau central mobile existant

En plus de ces éléments de réseau optimisés, les éléments de réseau apparaissant dans la Figure 1, comme indiqué dans la publication [ETSI TS 123 401], sont les suivants:

– Nœud B évolué (eNodeB): ce nœud d'accès hertzien héberge des fonctions de gestion des ressources radioélectriques, de décompression et de chiffrement des données sur la liaison montante pour le flux de données d'utilisateur, d'acheminement des données dans le plan d'utilisateur, etc.

– Serveur d'abonné résidentiel (HSS): stocke les informations d'abonnement de l'utilisateur, par exemple les paramètres d'authentification, les informations de localisation, etc.

– Fonction d'exposition des capacités de service (SCEF): services et capacités exposés de manière sécurisée qui sont fournis par les interfaces de réseau 3GPP.

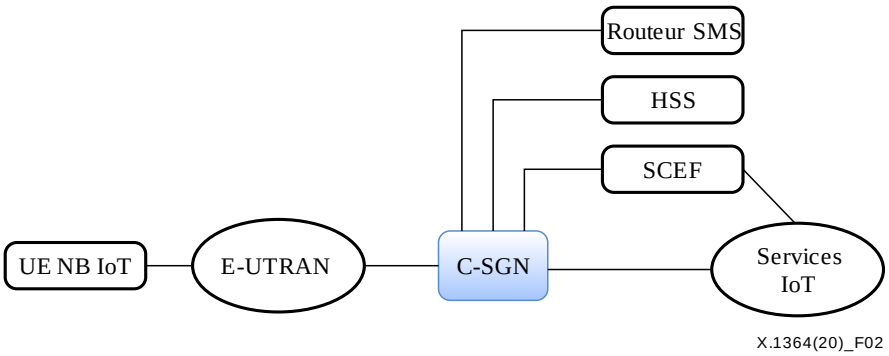
Ces éléments de réseau, de même que leurs fonctions, prennent en charge des services NB-IoT via le réseau de télécommunication mobile.

7.1.2 Déploiement avec un réseau central mobile dédié nouvellement établi

Dans ce scénario de déploiement, les opérateurs établissent un réseau central mobile dédié pour les services NB-IoT.

Le nœud de passerelle de desserte pour l'Internet des objets cellulaire (CIoT) (C-SGN) est défini par la publication [ETSI TS 123 401].

Un nœud C-SGN prend en charge un sous-ensemble des fonctionnalités nécessaires des éléments de réseau central existant à un système évolué en mode paquet (EPS). Il s'agit d'un nœud combiné pour réseaux évolués en mode paquet (EPC). Il offre la possibilité de réduire au minimum le nombre d'entités physiques EPS et regroupe des fonctions d'entités EPS sur les trajets dans le plan de commande et dans le plan utilisateur. Un nœud C-SGN combine les fonctions MME, P-GW et S-GW pour fournir une solution CIoT très optimisée. Une mise en œuvre C-SGN prend en charge les options de ses interfaces externes. Ces interfaces correspondent aux interfaces des entités EPC respectives, comme les fonctions MME, S-GW et P-GW.



NOTE – Les éléments du nouveau réseau central mobile sont indiqués en bleu.

Figure 2 – Déploiement avec un nouveau réseau central mobile dédié

En plus de ces éléments du nouveau réseau, les éléments de réseau apparaissant dans la Figure 2 sont les suivants [ETSI TS 123 401]:

– Réseau E-UTRAN: héberge des fonctions telles que la compression de l'en-tête et le chiffrement du plan utilisateur, la sélection de l'entité MME, le contrôle du débit au niveau du support, le contrôle de l'encombrement, le marquage des paquets au niveau du transport sur la liaison montante, etc.

– Serveur HSS: stocke et gère les informations d'abonnement de l'utilisateur, par exemple les paramètres d'authentification, les informations de localisation, etc.

– Fonction SCEF: donne les services et capacités exposés de manière sécurisée fournis par les interfaces de réseau 3GPP.

– Routeur de service de messages courts (SMS): prend en charge le transfert de demande d'attachement sans attachement EPS combiné (demande de services EPS et non EPS). Cette fonctionnalité est disponible pour les équipements UE ne prenant en charge que l'IoT à bande étroite.

Ces éléments de réseau, de même que leurs fonctions, prennent en charge des services NB-IoT via le réseau de télécommunication mobile.

7.2 Applications types

7.2.1 Relevé de consommation à distance

Dans ce scénario d'application, un dispositif NB-IoT est utilisé pour recevoir les relevés de consommation pour un service collectif, par exemple pour la consommation d'eau, de gaz, etc., et pour les envoyer au fournisseur de services correspondant via le réseau hertzien.

Grâce à la technologie NB-IoT, on établit les relevés de consommation de manière plus simple, plus fiable et plus efficace qu'avec les techniques manuelles traditionnelles.

7.2.2 Stationnement intelligent

Dans ce scénario d'application, on déploie dans un parking des dispositifs NB-IoT qui servent de capteurs permettant de détecter si une place de stationnement est disponible ou non. Les conducteurs ont ainsi la possibilité d'utiliser une application de stationnement intelligent qui leur recommandera tel ou tel parking et leur permettra en outre de s'acquitter en ligne du montant de leur stationnement.

L'utilisation de la technologie NB-IoT peut contribuer à aider les conducteurs à trouver des parkings ouverts et des places de stationnement ainsi qu'à effectuer le paiement correspondant.

7.2.3 Agriculture intelligente

Dans ce scénario d'application, les dispositifs NB-IoT servent de capteurs permettant d'enregistrer des paramètres utiles pour l'agriculture, comme la salinité, l'humidité, la température, etc. Sur la base des valeurs enregistrées, un agriculteur peut bénéficier de recommandations concernant des solutions pour l'irrigation et la fertilisation.

L'utilisation de la technologie NB-IoT facilite une agriculture plus intelligente grâce à une analyse d'informations en temps réel plutôt que sur des pratiques agricoles traditionnelles.

8 Menaces concernant l'IoT à bande étroite

L'analyse des menaces concernant la sécurité de l'IoT à bande étroite est effectuée suivant deux points de vue: les caractéristiques de l'IoT à bande étroite et le cadre fonctionnel des couches de l'IoT à bande étroite, qui sont décrits dans les § 8.1 et 8.2 respectivement.

8.1 Caractéristiques de l'IoT à bande étroite

Les caractéristiques types de l'IoT à bande étroite comprennent une faible dissipation d'énergie, une grande capacité, un faible coût et une large couverture.

8.1.1 Faible dissipation d'énergie

1) Description de la caractéristique

Les dispositifs NB-IoT se caractérisent par une faible consommation d'énergie, une grande autonomie et, partant, un besoin de recharges moins fréquentes, une faible capacité de calcul, etc. Les systèmes intégrés sont également légers et plus simples.

En général, l'une des caractéristiques des systèmes fonctionnant sur des terminaux IoT traditionnels est leur très grande capacité de calcul. Ces systèmes utilisent des protocoles de transmission complexes et des solutions strictes de renforcement de la sécurité. Parce qu'ils consomment beaucoup d'énergie, ils doivent être rechargés fréquemment.

2) Menaces pour l'IoT à bande étroite

Un dispositif NB-IoT pourrait être la cible d'attaques par déni de service par la simple consommation de ses ressources. Les coûts pour mener une telle attaque contre un logiciel et un équipement sont relativement faibles.

Étant donné que les dispositifs NB-IoT sont légers, consomment peu d'énergie et ont une capacité de calcul limitée, il n'est pas possible de garantir le chiffrement des données lors des transmissions pour assurer la sécurité. Les données seront parfois transmises en clair. Par conséquent, l'authentification et la validation des données pourraient faire l'objet de graves menaces. Par exemple, l'auteur d'une attaque pourrait utiliser des dispositifs non autorisés pour communiquer avec une station de base afin d'envoyer des données falsifiées.

8.1.2 Grande capacité

1) Description de la caractéristique

L'IoT à bande étroite offre une capacité bien plus grande que l'IoT traditionnel. Par exemple, un seul secteur NB-IoT pourrait prendre en charge quelque 100 000 dispositifs.

2) Menaces pour l'IoT à bande étroite

En raison du grand nombre de dispositifs, même une petite vulnérabilité pourrait avoir des conséquences dramatiques pour la sécurité du réseau. Par exemple, un cheval de Troie pourrait infecter d'autres terminaux et rendre le réseau indisponible.

Dans le cas d'un scénario de déploiement avec des dispositifs NB-IoT qui peuvent utiliser le réseau central mobile existant, le terminal pourrait infecter des éléments du réseau central mobile, comme l'entité de gestion de la mobilité, le serveur d'abonné résidentiel et d'autres dispositifs en vue d'atteindre les usagers des communications mobiles. Dans ce cas, l'accès au réseau pourrait être refusé aux utilisateurs ou les informations concernant les abonnés pourraient être modifiées afin que, par exemple, le coût des appels téléphoniques, des messages courts ou du trafic de données ne leur soit pas facturé.

8.1.3 Faible coût

1) Description de la caractéristique

Les dispositifs NB-IoT sont généralement peu coûteux.

2) Menaces concernant l'IoT à bande étroite

Les coûts peu élevés des dispositifs s'expliquent notamment par l'utilisation de protocoles simplifiés, dont les vulnérabilités pourraient par conséquent être utilisées par les auteurs d'attaques à l'encontre des dispositifs et du réseau.

8.1.4 Large couverture

1) Description de la caractéristique

L'IoT à bande étroite offre une couverture bien plus grande que l'IoT traditionnel. Par exemple, dans la même bande, par rapport aux réseaux actuels, l'IoT à bande étroite offre un gain de 15 à 20 dB et une zone de couverture jusqu'à 100 fois plus grande.

2) Menaces pour l'IoT à bande étroite

L'auteur d'une attaque peut facilement s'approprier et exploiter des dispositifs déployés à un emplacement éloigné.

8.2 Couche NB-IoT

8.2.1 Couche dispositif

Il est possible de mener une attaque en dupliquant des cartes SIM (module d'identification de l'abonné) à des fins illégales, par exemple pour accéder gratuitement au réseau.

Les piles de protocoles des nouveaux modules terminaux légers mis au point peuvent présenter des vulnérabilités relatives à la sécurité.

Les fabricants des terminaux IoT existants peuvent utiliser des éléments matériels prenant en charge les technologies WiFi, Bluetooth, ZigBee et d'autres protocoles lorsqu'ils mettent au point de nouveaux équipements prenant en charge l'IoT à bande étroite. Étant donné qu'ils peuvent se contenter d'ajouter à ces équipements la prise en charge de l'IoT à bande étroite, le risque est que ce processus engendre des vulnérabilités et des menaces pour la sécurité, avec par exemple, des ports de débogage mal protégés, l'utilisation d'algorithmes de chiffrement faibles, l'échec de la mise à jour d'éléments matériels et l'absence des contrôles d'intégrité réguliers nécessaires.

8.2.2 Couche réseau

Il serait possible d'utiliser des outils de détournement des communications d'un réseau de données pour surveiller des sessions entre un terminal et des stations de base afin d'intercepter des paquets de données échangés entre ces composants. Par conséquent, la communication est détournée, ce qui permet à l'auteur de l'attaque d'analyser les vulnérabilités concernant la sécurité grâce aux données extraites des messages détournés.

Compte tenu du grand nombre de dispositifs et du fait que les abonnés aux télécommunications mobiles utilisent les mêmes réseaux, les dispositifs NB-IoT ayant subi une altération volontaire pourraient être à l'origine de perturbations de la signalisation.

Il pourrait y avoir un risque de divulgation des données en raison des nombreuses données qui sont collectées par les services NB-IoT, transférées au réseau et traitées par de nombreux éléments de réseau.

La signalisation du réseau central NB-IoT pourrait être falsifiée ou altérée, ou faire l'objet d'une attaque par rejeu, faute de mécanismes d'authentification entre éléments de réseau.

De multiples attaques menées depuis l'Internet pourraient endommager l'interface entre le réseau central mobile et l'Internet; par exemple, dans le cas d'un système 5G, l'interface entre le réseau central mobile et l'Internet est appelée interface N6 [ETSI TS 123 501]. Cette interface N6 assure la connexion entre les fonctions du plan utilisateur et l'Internet.

8.2.3 Couche application

L'IoT à bande étroite convient aux scénarios d'exploitation avec des fonctionnalités statiques, une faible sensibilité au temps de latence, des mouvements discontinus et une transmission des données en temps réel.

Des omissions ou des fausses alertes peuvent se produire lors des opérations de signalement automatique des anomalies (par exemple, détecteur de fumée) ou de l'opération de rapport régulier (par exemple, un système de surveillance de l'état de l'environnement). Par exemple, en cas de détournement du relevé de consommation électrique d'un utilisateur, l'auteur de l'attaque pourrait modifier ou falsifier les chiffres indiqués sur le relevé au détriment de l'utilisateur.

De plus, des instructions malveillantes pourraient permettre de déclencher une opération à distance (par exemple, dans le cas d'appareils domestiques intelligents pouvant être allumés ou éteints à distance par les utilisateurs).

Les opérations possibles avec l'IoT à bande étroite sont véritablement intégrées dans les différents secteurs d'activité et, de ce fait, exposées à des vulnérabilités telles que celles inhérentes à des logiques opérationnelles complexes et à de multiples protocoles d'application.

Il est possible d'utiliser de manière abusive des services NB-IoT, par exemple en séparant l'appareil et la carte au moyen de l'insertion de la carte NB-IoT d'un abonné dans un dispositif autre qu'un dispositif NB-IoT ou encore de l'envoi d'un spam par message court.

9 Exigences de sécurité

9.1 Exigences de sécurité du dispositif terminal

9.1.1 Sécurité physique

La protection physique des interfaces et des puces est assurée par le dispositif terminal NB-IoT, qui veille à ce que l'auteur d'une attaque ne puisse pas accéder aux données, même en cas de détournement du matériel.

Pour différentes interfaces, le dispositif terminal NB-IoT prend en charge les fonctions d'authentification et d'autorisation.

9.1.2 Sécurité des mises à jour

Le système, les logiciels, les éléments matériels, etc. du dispositif NB-IoT doivent pouvoir être mis à jour afin de garantir la sécurité des systèmes et des applications.

La protection de la confidentialité et de l'intégrité pour la mise à jour des fichiers est requise pour éviter les altérations volontaires.

9.1.3 Protection de la vie privée

Le dispositif terminal NB-IoT doit comprendre des mécanismes souples de protection de la vie privée pour prendre en charge cette protection sur la base des exigences du service NB-IoT.

9.2 Exigences de sécurité des réseaux

9.2.1 Authentification

L'authentification est requise pour confirmer l'identité de l'entité NB-IoT qui utilise un service NB-IoT. L'authentification permet de garantir la validité de l'identité déclarée par l'entité et de garantir que l'entité ne tente pas d'usurper l'identité d'une entité autorisée.

Une authentification pour environnements contraints est nécessaire compte tenu des caractéristiques de l'IoT à bande étroite.

9.2.2 Prévention des attaques DDoS

Il faut déployer au préalable des mécanismes de sécurité pour empêcher et traiter sans délai les attaques par déni de service réparti (DDoS).

9.2.3 Sécurité des entités de réseau

Les entités du réseau central NB-IoT doivent prendre en charge les capacités de sécurité, afin d'empêcher les falsifications, les altérations volontaires et les attaques par rejeu.

9.3 Exigences de sécurité des applications

9.3.1 Surveillance de la conformité de l'utilisation/du fonctionnement du service

La surveillance de la conformité de l'utilisation/du fonctionnement du service est requise pour surveiller les valeurs maximales et le nombre de flux total, afin de déceler une utilisation/un fonctionnement anormal du service conformément aux exigences des services NB-IoT.

9.3.2 Prévention de l'utilisation abusive du service

Il faut empêcher l'utilisation abusive du service découlant d'une séparation de l'appareil et de la carte en surveillant les caractéristiques d'un changement d'identité internationale d'équipement mobile (IMEI).

9.3.3 Capacités d'identification, d'analyse et d'élimination des menaces concernant la sécurité

Il faut identifier, analyser et éliminer les menaces concernant la sécurité en se fondant sur l'analyse des mégadonnées associées au comportement du dispositif terminal NB-IoT.

10 Capacités de sécurité pour l'IoT à bande étroite

10.1 Capacités de sécurité du dispositif terminal

Un dispositif terminal NB-IoT devrait avoir les capacités de sécurité suivantes:

– SC_terminal 1: capacité de gestion des clés;

– SC_terminal 2: capacité de négociation de l'algorithme de chiffrement;

– SC_terminal 3: capacité de chiffrement des données;
– SC_terminal 4: capacité de protection de l'intégrité des données;
– SC_terminal 5: capacité de mise à jour sécurisée, notamment pour les systèmes, logiciels, éléments physiques, etc.;
– SC_terminal 6: capacité pour mettre en œuvre des protocoles sécurisés fondés sur une cryptographie pour environnements contraints.

10.2 Capacités de sécurité du réseau

Un réseau NB-IoT devrait avoir les capacités de sécurité suivantes:
– SC_réseau 1: capacité de gestion des clés;
– SC_réseau 2: capacité de négociation de l'algorithme de chiffrement;
– SC_réseau 3: capacité de chiffrement des données;
– SC_réseau 4: capacité de protection de l'intégrité des données;
– SC_réseau 5: capacité de contrôle d'accès pour garantir que seules les entités autorisées peuvent accéder aux éléments de réseau NB-IoT, aux informations stockées, aux flux d'informations, aux services et aux applications;
– SC_réseau 6: capacité de détection et/ou de prévention des altérations volontaires;
– SC_réseau 7: capacité pour résister aux attaques DDoS;
– SC_réseau 8: capacité pour mettre en place des configurations sécurisées;
– SC_réseau 9: capacité de détection des séparations appareil/carte.

10.3 Capacités de sécurité des applications

Les applications devraient être dotées des capacités de sécurité suivantes:
– SC_applications 1: capacité de protection contre les infections par des logiciels malveillants grâce à l'utilisation de logiciels de protection contre les logiciels malveillants;
– SC_applications 2: capacité de surveiller la conformité de l'utilisation/du fonctionnement du service au moyen de la surveillance des indicateurs essentiels relatifs au réseau (par exemple, valeur maximale, nombre de flux total);
– SC_applications 3: capacité de sécurité au niveau de l'application pour éliminer les menaces concernant la sécurité en se fondant sur l'analyse des mégadonnées associées au comportement du dispositif terminal NB-IoT.

10.4 Relations entre les capacités de sécurité et les exigences de sécurité

Les différentes capacités de sécurité décrites dans la partie 10 sont utilisées pour répondre à certaines des exigences de sécurité définies dans la partie 9. Le Tableau 1 montre la correspondance entre les capacités de sécurité et les exigences de sécurité.

Dans le Tableau 1, le symbole "√" figurant dans une case indique que l'exigence de sécurité est liée à une capacité de sécurité particulière. Plus précisément, l'exigence de sécurité concernée devrait être prise en charge grâce à la mise en œuvre de la capacité correspondante indiquée.

Tableau 1 – Illustration des relations entre les exigences de sécurité et les capacités de sécurité

Exigences / Capacité	Sécurité physique	Sécurité des mises à jour	Protection de la vie privée	Authenti-fication	Prévention des attaques DDoS	Surveillance de la conformité de l'utilisation/du fonctionnement des services	Prévention de l'utilisation abusive du service	Capacités d'identification, d'analyse et d'élimination des menaces concernant la sécurité
SC_terminal 1	√			√				
SC_terminal 2	√							
SC_terminal 3			√					
SC_terminal 4		√						
SC_terminal 5	√	√						
SC_terminal 6			√	√				
SC_réseau 1				√				
SC_réseau 2		√	√					
SC_réseau 3		√	√					
SC_réseau 4		√						
SC_réseau 5			√	√				
SC_réseau 6						√		
SC_réseau 7					√			
SC_réseau 8		√						
SC_réseau 9							√	
SC_applications 1		√						
SC_applications 2					√	√	√	
SC_applications 3			√					√

Bibliographie

[b-UIT-T Q.1743] Recommandation UIT-T Q.1743 (2016), *Références IMT évoluées à la version 11 du réseau central évolué en mode paquet LTE-advanced*.

[b-UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

[b-UIT-T X.1141] Recommandation UIT-T X.1141 (2006), *Langage de balisage d'assertion de sécurité (SAML 2.0)*.

[b-UIT-T X.1145] Recommandation UIT-T X.1145 (2017), *Cadre et exigences de sécurité pour les capacités ouvertes des services de télécommunication*.

[b-UIT-T X.1252] Recommandation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité*.

SÉRIES DES RECOMMANDATIONS UIT-T

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

Imprimé en Suisse
Genève, 2020