



**MINISTÈRE
DES ARMÉES**

*Liberté
Égalité
Fraternité*

**Direction Générale du Numérique
et des Systèmes d'Information
et de communication**

DIRECTIVE DGNUM N° 23/ARM/DGNUM/DG

PORTANT SUR

LA SÉCURITÉ

DE TECHNOLOGIES DE RÉSEAUX SANS FIL

(DIR SS.FIL)

1^{ère} ÉDITION
approuvée le 02 février 2021

Entretenu par la DGNUM



**L'édition en vigueur de ce document est celle accessible via le site
SYNOPTIC : <http://synoptic.intradef.gouv.fr/>. S'assurer de la validité de
toute copie avant usage.**

Rédaction	LV Frédéric Caro	DGNUM/SDSN/BMR
Contribution	GT du 7 janvier 2021 (msg du 03 DEC 2020/430 DGNUM)	Représentants des EMDS
Vérification	CF Stéphane Laugier	DGNUM/SDSN/BMR
Vérification	COL (A) Eric Alardet	DGNUM/SDSN

TABLE DES MATIÈRES

1	PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.....	3
1.1	Présentation	3
1.2	Textes abrogés	3
1.3	Niveaux de préconisation	3
1.4	Gestion des dérogations.....	3
2	CADRE DOCUMENTAIRE.....	4
2.1	Documents applicables	4
2.2	Normes et standards applicables.....	4
2.3	Autres documents et sites de référence.....	4
3	DÉFINITIONS ET PÉRIMÈTRE D'APPLICATION.....	6
3.1	Périmètre d'application de la directive	6
3.2	Constitution d'un système sans fil.....	6
3.3	Sous-systèmes de communication sans fil.....	6
3.4	Sous-systèmes équipement IoT	7
3.5	Sous système équipements et infrastructures dédiés	8
3.6	Aspects protocolaires mis en jeu	8
4	VULNÉRABILITÉS DES TECHNOLOGIES SANS FIL.....	9
4.1	Spécificités des systèmes sans fil intéressant la Cybersécurité	9
4.2	Scénarios de menaces	9
5	MESURES DE SÉCURITÉ RELATIVES AUX SYSTÈMES SANS FIL.....	11
5.1	Réglementaire.....	11
5.2	Analyse de Risques.....	11
5.3	Cartographie des composants	11
5.4	Sécurisation de l'architecture du système sans fil	11
5.5	Sécurité des protocoles	11
5.6	Sécurisation des équipements.....	12
5.7	Sécurisation physique.....	12
	ANNEXE 1: COMPARATIF DE TECHNOLOGIES SANS FIL.....	13
	ANNEXE 2: BLUETOOTH ET BLUETOOTH LOW ENERGY.....	15
	ANNEXE 3: RFID	17
	ANNEXE 4: ZIGBEE.....	20
	ANNEXE 5: WIFI	23
	ANNEXE 6: DE LA 2G A LA 5G.....	25
	ANNEXE 7: LORAWAN	28

1 PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE

1.1 Présentation

La présente directive s'inscrit dans les missions de la direction générale du numérique et des systèmes d'information et de communication (DGNUM), aux termes de l'article 11 du décret n° 2018-532 du 28 juin 2018 portant création de la direction générale du numérique et des systèmes d'information et fixant l'organisation des systèmes d'information et de communication de la défense.

L'objectif de cette directive est d'encadrer l'utilisation des technologies sans fil du domaine civil afin de réduire les risques encourus par le ministère face à une cyber-attaque exploitant les faiblesses de ces technologies. Elle s'adresse principalement aux acteurs participant à la conception, la réalisation, l'exploitation, le maintien en condition opérationnel et de sécurité des systèmes d'information.

Cette directive décrit les principales menaces et au terme d'une analyse de risques précise les règles techniques et procédurales applicables à tout cadre d'usage des technologies sans fil issues du domaine civil. **Des compléments spécifiques à chaque technologie étudiée font l'objet d'annexes applicables dédiées.**

Conformément à la [DIR RETEX], les difficultés rencontrées dans l'application de la directive nourriront les réflexions dans le cadre du retour d'expérience. En particulier, ce processus RETEX visera à intégrer les nouvelles demandes associées à des technologies sans fil du domaine civil non adressées par la présente directive. En fonction des éléments collectés et de leur pertinence, une nouvelle version de la directive sera rédigée dans l'objectif d'en améliorer l'applicabilité.

1.2 Textes abrogés

La directive n° 23/DEF/DGSIC du 6 février 2012 portant sur l'utilisation du WI-FI au sein du MINDEF et le guide n° 9/DEF/DGSIC relatif à la mise en œuvre des réseaux WI-FI du 6 février 2012 sont abrogés.

1.3 Niveaux de préconisation

Les règles définies dans ce document sont conformes à la [RFC 2119] :

OBLIGATOIRE	ce niveau de préconisation signifie que la règle édictée indique une exigence absolue de la directive.
RECOMMANDÉ	ce niveau de préconisation signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ignorer la règle édictée, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente.
DÉCONSEILLÉ	ce niveau de préconisation signifie que la règle édictée indique une prohibition qu'il est toutefois possible, dans des circonstances particulières, de ne pas suivre, mais les conséquences doivent être comprises et le cas soigneusement pesé.
INTERDIT	ce niveau de préconisation signifie que la règle édictée indique une prohibition absolue de la directive.
CONSEILLÉ	ce niveau de préconisation signifie que la règle édictée est une bonne pratique de sécurité des systèmes d'information. Il n'est pas nécessaire d'instruire une dérogation lorsqu'elle n'est pas respectée.

1.4 Gestion des dérogations

Les dérogations aux règles **OBLIGATOIRE** et **INTERDIT** sont du ressort des AQ. Le FSSI et la DGNUM sont tenus informés.

Les dérogations aux règles **RECOMMANDÉ** et **DÉCONSEILLÉ** sont du ressort des AH. L'AQ est tenue informée.

Les dérogations octroyées sont à lister et insérer dans le dossier d'homologation.

2.1 Documents applicables

[PSSI-M]	Instruction ministérielle n° 7326/ARM/CAB relative à la politique de sécurité des systèmes d'information du ministère des armées du 25 juin 2018. https://synoptic.intradef.gouv.fr/securite-des-systemes-dinformation/instruction-ministerielle-ndeg7326armcab-du-25-juin-2018
[PSSI-M-T]	Instruction ministérielle 7326-2/DEF/CAB relative au volet technique de la politique de sécurité des systèmes d'information du ministère de la défense du 8 janvier 2016. https://synoptic.intradef.gouv.fr/sites/synoptic/files/160128_pssi_m_t_dr.pdf
[DIR HSI]	Directive n°27/DEF/DGNUM – 2 ^{ème} édition 19 novembre 2019 portant sur l'homologation des systèmes d'information du ministère des Armées.
[DIR MCS]	Directive n°47/ARM/DGNUM/DR du 4 juin 2020 portant sur le maintien en condition de sécurité des systèmes d'information du ministère. https://synoptic.intradef.gouv.fr/sites/synoptic/files/20200604_dr_dgnum-dg_200-directive-47-relative-maintien-condition-securite-v1_0.pdf
[DIR RETEX]	Directive n°33/DEF/DGSIC/NP du 05 février 2015 relative au retour d'expérience en cybersécurité au sein du ministère de la Défense. https://synoptic.intradef.gouv.fr/sites/synoptic/files/20150205_np_dgsic-sdssi-bmr_033-directive-retex-ed1.pdf
[DIR TRACES]	Directive n° 29/DEF/DGSIC du 12 novembre 2013 relative aux traces et leur gestion au sein du ministère de la Défense. https://synoptic.intradef.gouv.fr/sites/synoptic/files/20131112_np_29_dgsic_directive_traces-et-gestion-au-sein-du-mindef.pdf

2.2 Normes et standards applicables

[RFC 2119]	Mots-clés pour niveaux d'obligation.
[RFF 7228]	Terminologie des réseaux à nœuds contraints.

2.3 Autres documents et sites de référence

[EMA-DGA-RFID]	Note n°D-18-005592 ARM/EMA/DSA/MCO/NP et n°DGA01D18054469 ARM/DGA/DO/SMCO/NP du 15 octobre 2018 relative à la mise en œuvre de la technologie RFID http://www.dga.defense.gouv.fr/mco/system/files/20181015_dga01d18054469_smco_not_diffusion_dtia_rfid_ema-dga_0.pdf
[VM-DGA-RFID]	Vade-mecum de la DGA de 2016 sur la RFID http://www.dga.defense.gouv.fr/mco/system/files/vade_mecum_rfid_v1_0.pdf
[ANSSI WIFI]	Recommandations de sécurité relatives aux réseaux Wi-Fi https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-aux-reseaux-wifi/
[Guide n°6]	Guide n°6/DEF/DGSIC du 02 avril 2013 portant sur les données de caractérisation d'un système d'information. https://synoptic.intradef.gouv.fr/sites/synoptic/files/20130402_np_dgsic_guide-06_valorisationdonneescaracterisation-si.pdf

[ETUDE_JANUS]	<p>Étude JANUS DGA-MI V2</p> <p>http://www.dga.defense.gouv.fr/dga_mi/janus-securisation-des-technologies-wifi-cpl-android%E2%80%A6</p>
[NISTIR 8220]	<p>Étude NIST sur les standards objets connectés.</p> <p>https://csrc.nist.gov/publications/detail/nistir/8200/final</p>
[ENISA]	<p>Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures November 2017</p> <p>https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot</p>
[ENISA 5G]	<p>ENISA THREAT LANDSCAPE FOR 5G NETWORKS</p> <p>https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks</p>
[ENISA_5GTOOLS]	<p>Cybersecurity of 5G networks EU Toolbox of risk mitigating measures January 2020</p> <p>https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures</p>
[API]	<p>Politique et directive DGNUM sur les API</p> <p>https://synoptic.intradef.gouv.fr/sites/synoptic/files/20200724_np_dgnum_po-l-api_politique-generale-echanges-inter-applicatifs-par-api.pdf</p>

3.1 Périmètre d'application de la directive

La présente directive est applicable à tout système d'information utilisant une technologie de radiocommunication du domaine civil.

Elle ne s'applique pas aux liaisons satellitaires, aux liaisons de données tactiques, aux technologies de détection type SONAR/RADAR/LIDAR, aux radiocommunications à technologie militaire. Elle ne s'impose pas aux systèmes d'armes mais peut être retenue comme un guide dès lors que les technologies décrites y sont utilisées.

3.2 Constitution d'un système sans fil

Dans la suite de la directive, un système sans fil est décomposé selon le schéma de principe suivant :

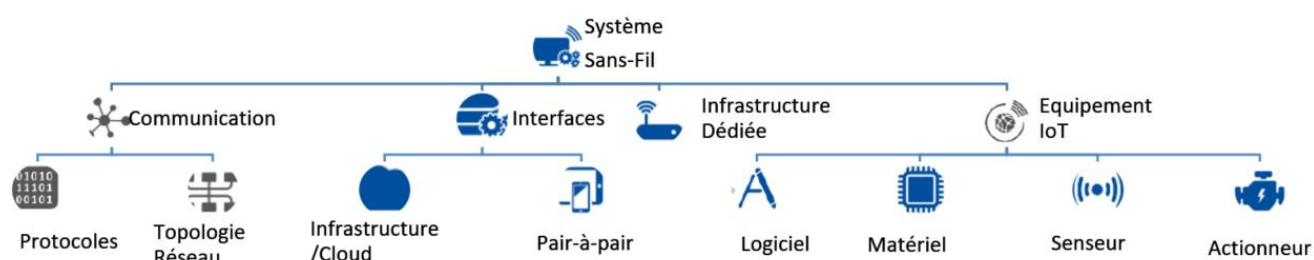


Figure 1 : Schéma de principe d'un système sans fil

Le système sans fil est vu comme une composition :

- d'un Sous-Système « Communication sans fil » défini par des protocoles (WIFI, ZigBee, LORA, ...) et par une taxonomie de réseau sans fil auquel il appartient (LPAN, WPAN, LoPWAN, réseau cellulaire 2G à 5G) ;
- d'un Sous-Système « Equipement IoT » ;
- d'un Sous-Système « Équipements et infrastructures dédiés » assurant la passerelle avec l'infrastructure filaire ou assurant la gestion/administration/supervision dédiée du système sans fil ;
- d'interfaces avec des éléments d'infrastructure filaire et éventuellement non filaire (type équipement ordiphone). Deux cas sont distingués :
 - Infrastructure sous maîtrise dans une emprise du ministère ;
 - Infrastructure non maîtrisée (cas d'un opérateur télécom tiers par exemple).

3.3 Sous-systèmes de communication sans fil

3.3.1 Taxonomie des réseaux sans fil

Les sous-systèmes de communication sans fil, dits réseaux sans fil, font l'objet d'une activité normative prolifique.

On distingue généralement deux grandes natures pour les technologies sans fil :

1. Cellulaires :
 - Normalisés dans le cadre 3GPP ;
 - Infrastructures spécifiques ;
 - Réseaux de type 2G, 3G, 4G, 5G ;
2. ad-hoc :
 - Normalisés par IEEE (802.11, 15, 16) ;
 - Infrastructure et moyens dédiés ;
 - Réseaux de type WPAN, WLAN, LoPWAN (Low-Power Wide Area Network), ...

NB : D'autres technologies fonctionnant sur d'autres domaines spectraux (technologie type LIFI par exemple) ne sont pas listées ici. Comme précisé au §1.1, elles pourront faire l'objet d'une mise à jour de cette directive une fois que le niveau de maturité (cas d'usage au sein du ministère des Armées et études de sécurisation) sur ces technologies sera estimé suffisant.

La présente directive s'intéresse aux technologies suivantes :

- 2G, 3G, 4G, 5G des réseaux cellulaires ;
- ZIGBEE et BLUETOOTH des réseaux WPAN (IEEE 802.15) ;
- RFID/NFC un protocole spécifique avec un faible lien WPAN (IEEE 802.15) ;
- LORA un protocole propriétaire de la catégorie LoPWAN.

3.3.2 Caractéristiques principales

Les communications sans fil sont caractérisées par le débit utile et la portée et leur coût d'accès :

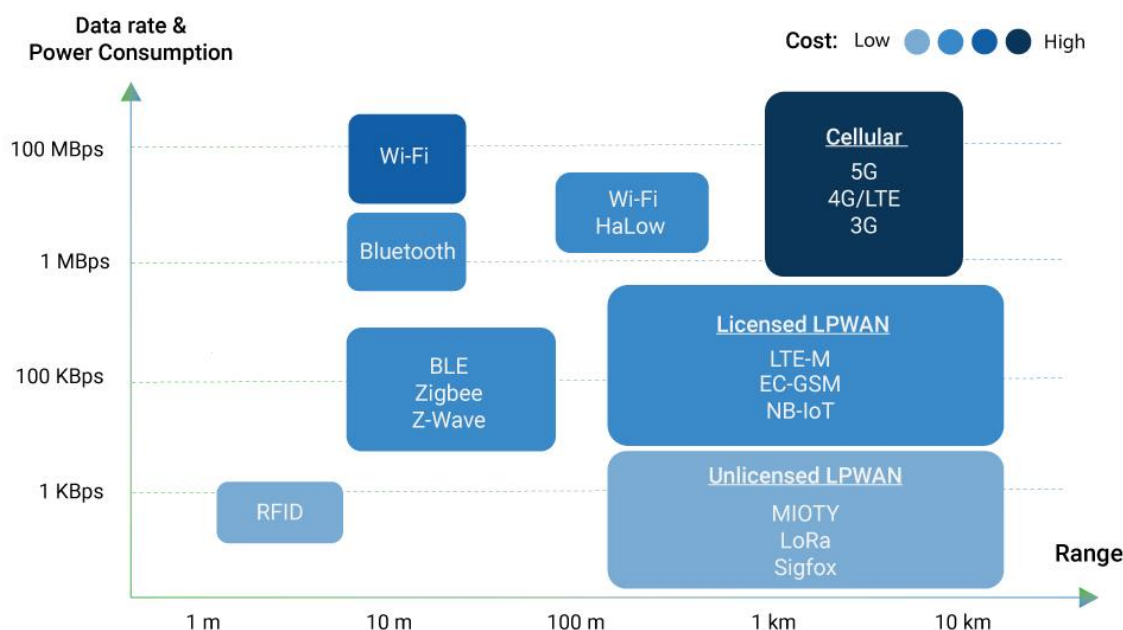


Figure 2 : Comparaison de protocoles sans fil selon leur portée, débit et coût (source : industry.com)

L'annexe I présente une comparaison plus détaillée des technologies sans fil.

3.4 Sous-systèmes équipement IoT

L'IoT (Internet of Things) est communément appelé « internet des objets ». « Objet connecté » est utilisé pour désigner un composant de l'IoT.

La définition d'un objet connecté n'est pas encore normalisée. Dans [NISTIR 8200], le NIST dresse quelques caractéristiques communes et en particulier deux concepts fondamentaux :

- Les composants IoT sont connectés au réseau, offrant une capacité de relation bilatérale ou multilatérale entre eux ou au bénéfice d'autres systèmes, en s'appuyant prioritairement mais pas systématiquement sur des protocoles reposant sur UDP et TCP. Généralement le sens de transmission du capteur vers le réseau et le protocole UDP pour les objets peu évolués sont privilégiés par les constructeurs.
- La plupart des composants IoT possèdent des senseurs et actionneurs leur permettant d'observer et d'agir sur le monde physique.

[ENISA] représente la structure des systèmes embarquant de l'IoT de manière concentrique :

- au centre : le processeur ;
- 1^{er} cercle : la mémoire non volatile, la connectivité (sans fil et filaire), l'alimentation électrique (pile et câble) ;
- 2^{ème} cercle : les capteurs, les actionneurs et la gestion des interfaces.

La plupart des objets connectés dispose d'une capacité de sécurisation réduite qui peut s'expliquer par des ressources et des traitements limités en vue de minimiser la consommation énergétique, et les faibles efforts en R&D.

Un objet connecté peut être rattaché à un réseau par un lien filaire ou sans fil.

Un objet connecté peut disposer de trois types de fonctionnalités :

1. fonction de support permettant de gérer l'objet lui-même (configuration, sécurité, supervision, orchestration dans le cadre d'un réseau d'objet ...);
2. fonction de gestion des données (traitement, stockage, transfert);
3. fonction d'interaction avec le monde physique (Capteurs, actionneurs).

Ce sous-système comprend également les terminaux au sens plus usuel (ordinateur portable, smartphone, ...).

3.5 Sous système équipements et infrastructures dédiés

Ce sous-système regroupe l'ensemble des équipements assurant la passerelle entre le monde sans fil et l'infrastructure filaire, ainsi que les équipements assurant l'administration et la supervision du système sans fil.

Par exemple, cela comprend :

- les points d'accès et les contrôleurs d'accès sans fil dans une infrastructure de type WIFI ;
- les antennes relais (Base Transceiver Station ou E-NodeB) dans le monde des radiocommunications cellulaires.

Des facteurs de non maturité :

- fragmentation des standards et des initiatives de réglementations sur ce sujet (IETF, GSMA, ISA/IEC, OSIDO etc.);
- faible prise en compte de la sécurité numérique par les acteurs de l'Internet des objets (IoT) et inadéquation de la plupart des solutions techniques traditionnelles aux spécificités des objets connectés.

3.6 Aspects protocolaires mis en jeu

Les réseaux utilisant des technologies sans fil implémentent différents protocoles dont notamment ceux concernant les couches physique et l'accès au média radio. Ces derniers sont le plus souvent standardisés. Les couches réseau, transport ou applicatif relèvent généralement de spécifications établies par des consortiums propriétaires.

Ci-après une liste de quelques protocoles disponibles dans [ENISA].

SESSION		AMQP, CoAP, DDS, MQTT, XMPP
NETWORK	ENCAPSULATION	6LowPAN, Thread
	ROUTING	CARP, RPL
DATALINK		Bluetooth / BLE, Wi-Fi / Wi-Fi HaLow, LoRaWAN, Neul, SigFox, Z-Wave, ZigBee,

À l'instar de ce qui a été fait pour les protocoles du web, l'IETF est en train de définir des versions sécurisées de protocoles de l'Internet des objets dont un exemple est donné ci-après :

Layer	Sdt. Internet	Secure Std. Internet	IoT	Secure IoT
Application	HTTP	HTTPS	CoAP,CBOR	OSCOAP,COSE
Transport	TCP	TLS	UDP	DTLS
Network	IP	IKEv2+IPsec(ESP)	6LoWPAN	Min.IKEv2+ESP

4.1 Spécificités des systèmes sans fil intéressant la Cybersécurité

Les systèmes qui utilisent des technologies sans fil sont exposés aux risques intrinsèques de ces dernières. Ils convient d'analyser ces risques en fonction du contexte d'emploi. Parmi ces risques, on retrouve selon la technologie utilisée tout ou partie des points ci-dessous :

- les systèmes de communications sans fil sont conçus pour minimiser la consommation électrique afin de s'intégrer dans l'environnement embarqué. Il en résulte des capacités limitées de calcul (vitesse), de stockage (volume), de connectivité (portée) et de sécurité (mécanismes simplifiés) ;
- les systèmes sans fils portent en général un risque cyber plus élevé que les systèmes filaires du fait de leur exposition ;
- les systèmes de connexions sans fil comportent les risques intrinsèques de disponibilité du service (interférences, brouillage, accès au support de communication/authentification) et de confidentialité (discrétion, interception).

La mobilité et l'itinérance des équipements apportés par le système sans fil est un risque qui doit être pris en compte.

4.2 Scénarios de menaces

Dix scénarios de menace de [ENISA]) sont proposés lors des analyses de risque des systèmes utilisant les technologies sans fil. Ces scénarios sont à adapter au contexte d'emploi du SI et peuvent être reconsidérés comme des événements redoutés,

Nmr	Libelle du scénario	DICT impacté	Vulnérabilités associées	Biens supports Impactés	Source d'attaques
S1	Attaque par déni de service sur les équipements IoT ou S/S de Communication liés au système sans fil	D	Sensibilité au brouillage Faiblesse protocolaire Dépassement de capacité mémoire, ressource CPU, énergie ...	Communications Equipements IoT Infra. dédiées	
S2	Attaque des relais sans fil vers l'infrastructure en interface	D	Manipulation protocolaire (rejeu, injection, ...) Maturité faible en termes de sécurité des développement, processus de sécurité (gestion des vulnérabilités ...)	Communications Equipements IoT Infra. dédiées Interfaces	
S3	Attaque de type ransomware sur système sans fil ou comme relais vers l'infrastructure en interface	DIC	Défaut d'implémentation des protocoles Vulnérabilité COTS Faiblesse protection intégrité mémoire Faible maturité de la sécurité des développement, processus de sécurité (gestion des vulnérabilités ...)	Equipements IoT Infra. dédiées Interfaces	Kit d'exploit, malware
S4	Attaque sur l'intégrité/modification des paramètres d'un équipement du système sans fil en vue d'altérer son fonctionnement	DICT	Manipulation protocolaire (rejeu, injection, ...) Défaut d'implémentation des protocoles Vulnérabilité COTS Faiblesse protection intégrité Faible maturité de la sécurité des développement, processus de sécurité (gestion des vulnérabilités ...)	Communications Equipements IoT	Kit d'exploit, malware,

Nmr	Libelle du scénario	DICT impacté	Vulnérabilités associées	Biens supports Impactés	Source d'attaques
S5	Attaque permettant de compromettre les informations de localisation sur un équipement du système sans fil en vue d'usurper ou de divulguer l'identité de l'équipement et de son propriétaire	C	Manipulation protocolaire (rejeu, injection, ...) Défaut d'implémentation des protocoles Vulnérabilité COTS Faiblesse protection intégrité ou confidentialité Faible maturité de la sécurité des développement, processus de sécurité (gestion des vulnérabilités ...)	Communications Equipements IoT	Écoute passive ou active Kit d'exploit, malware,
S6	Attaque via usurpation ou « leurrage » sur l'identité des équipements du système sans fil	C	Manipulation protocolaire (rejeu, injection, ...) Faiblesse protocolaire Défaut d'implémentation des protocoles Faible maturité de la sécurité des développement, processus de sécurité (gestion des vulnérabilités ...)	Communications Equipements IoT Infra. dédiées	Écoute passive ou active Kit d'exploit, malware IMSI Grabber
S7	Attaque sur l'administration ou la supervision des systèmes sans fil en vue d'attenter à l'intégrité, la confidentialité ou à la disponibilité d'un équipement le constituant, ou à détourner la finalité de la liaison	DICT	Manipulation protocolaire (rejeu, injection, ...) Défaut d'implémentation des protocoles Vulnérabilité COTS Faiblesse protection en confidentialité ou intégrité mémoire Faible maturité de la sécurité des développement, processus de sécurité (gestion des vulnérabilités ...)	Infra. dédiées Communications Équipement IoT	Écoute passive ou active Kit d'exploit, malware
S8	Atteinte à la confidentialité des données transitant depuis ou à destination du système sans fil	C	Faiblesse ou défaut d'implémentation des protocoles Faible maturité de la sécurité des développement, processus de sécurité (gestion des vulnérabilités ...)	Infra. dédiées Communications Equipements IoT Interfaces	Écoute passive ou active
S9	Atteinte à la confidentialité des données stockées sur le système sans fil	C	Manipulation protocolaire (rejeu, injection, ...) Défaut d'implémentation des protocoles Vulnérabilité COTS Faiblesse protection en confidentialité ou intégrité mémoire Faible maturité de la sécurité des développement, processus de sécurité (gestion des vulnérabilités ...)	Infra. dédiées Communications Équipement IoT	
S10	Atteinte à l'intégrité des données transitant depuis ou à destination du système sans fil	I	Rejeu Man in the middle (lien avec S6)		

5.1 Réglementaire

Le corpus réglementaire est applicable pour les systèmes d'information utilisant des technologies sans fil (chiffrement, cloisonnement, journalisation, interconnexion...).

SSFIL 01: Il est **OBLIGATOIRE** d'utiliser les bandes de fréquences et les densités de puissances autorisées par la réglementation nationale ou, pour des cas particuliers, celles validées par le bureau de la gouvernance des fréquences du ministère (DGNUM).

Les recommandations liées aux fréquences peuvent différer de la réglementation nationale interministérielle en temps de paix. En effet, elles tiennent compte d'un usage dans un contexte opérationnel, qui prend en compte la présence de réseaux de communication militaires et de systèmes d'arme.

Les recommandations liées aux fréquences peuvent différer en fonction de la zone géographique. Ce point est important pour les systèmes ayant vocation à être projetés hors du territoire national.

5.2 Analyse de Risques

SSFIL 02: Il est **OBLIGATOIRE**, lorsque la démarche d'homologation du système impose une analyse des risques, de tenir compte des vulnérabilités des technologies sans fil utilisées.

5.3 Cartographie des composants

SSFIL 03: Il est **RECOMMANDÉ** d'indiquer dans le référentiel de configuration (paramétrages, version de firmware, version logicielle ...) du système sans fil déployé les fréquences et puissances d'émission.

5.4 Sécurisation de l'architecture du système sans fil

SSFIL 04: Il est **OBLIGATOIRE**, lors de l'interconnexion d'un système sans fil avec un autre système d'information de maîtriser les protocoles d'échanges, d'authentifier les interfaces d'échanges.

SSFIL 05: Il est **OBLIGATOIRE**, lors de l'interconnexion d'un système sans fil avec un système d'informations diffusion restreinte ou classifié, de sécuriser cette interconnexion (et les flux échangés) par des dispositifs agréés par l'ANSSI au moins au même niveau que le système d'information interconnecté et conformément aux dispositions de l'agrément. Cette sécurisation est complémentaire à celle fournie par le protocole natif de communication sans fil.

SSFIL 06: Il est **OBLIGATOIRE** de cloisonner au moins logiquement (VLAN) un système sans fil des autres installations auxquelles il est raccordé.

SSFIL 07: Il est **OBLIGATOIRE** d'appliquer les règles suivantes pour le filtrage en interface du système sans fil:

- Identification des flux par exemple le quadruplet (adresse IP source, adresse IP destination, protocole de transport, ports de communication) ;
- Refus par défaut des flux (politique de liste blanche) ;
- Autorisation accordée seulement aux flux nécessaires au fonctionnement du système sans fil.

SSFIL 08: Il est **RECOMMANDÉ** d'utiliser une connexion filaire avec des interfaces physiques et/ou logiques (VLANs) dédiées pour administrer et superviser les infrastructures et leurs interfaces.

5.5 Sécurité des protocoles

SSFIL 09: Il est **DÉCONSEILLÉ** d'utiliser des protocoles de sécurité propriétaires.

NB: En règle générale, la sécurité par l'obscurité des algorithmes et des sources est peu fiable dans le domaine civil. Nombre de protocoles utilisés dans l'internet des objets s'appuient sur des mécanismes et algorithmes propriétaires non documentés et souvent peu robustes.

SSFIL 10: Il est **OBLIGATOIRE** d'utiliser des protocoles sécurisés pour administrer et superviser les infrastructures et les interfaces d'un système sans fil.

5.6 Sécurisation des équipements

SSFIL 11: Il est **OBLIGATOIRE**, lorsque possible, d'appliquer sur les équipements des réseaux sans fil les mesures suivantes :

- suppression des comptes par défaut ;
- suppression des clés de chiffrement par défaut ou non utilisées ;
- changement des mots de passe par défaut ;
- changement des noms des équipements ;
- désactivation des ports physiques inutilisés dont ports de maintenance ;
- désactivation ou suppression des services non nécessaires (protocoles d'administration non sécurisés, service web ...).
- désactivation des protocoles cryptographiques obsolètes ou non-conformes au RGS

SSFIL 12: Il est **RECOMMANDÉ** de contrôler, au chargement, l'intégrité du système d'exploitation, des *firmware* et des paramètres de configuration.

SSFIL 13: Il est **OBLIGATOIRE** de configurer les puissances émises, d'identifier les portées et zones couvertes pour appréhender la sécurité de l'environnement physique et identifier des scénarios de menace.

SSFIL 14: Il est **RECOMMANDÉ** d'utiliser des certificats d'authentification/chiffrement délivrés et gérés par le ministère.

SSFIL 15: Il est **OBLIGATOIRE** d'utiliser des composants du système sans fil (firmware, logiciels) soutenus dont les fournisseurs communiquent sur les vulnérabilités et assurent la délivrance de correctifs de sécurité.

5.7 Sécurisation physique

SSFIL 16: Il est **RECOMMANDÉ** de contrôler l'accès physique des équipements d'infrastructure dédiés au système sans fil (hors antenne déportée).

SSFIL 17: Il est **OBLIGATOIRE**, à défaut de contrôler l'accès physique, de protéger physiquement l'intégrité de l'équipement d'infrastructure dédiés au système sans fil (scellé ...) et de le contrôler périodiquement.

ANNEXE 1 : COMPARATIF DE TECHNOLOGIES SANS FIL

Caractéristiques	Bluetooth LE	Bluetooth (classique)	Zigbee	Z-wave	NFC	RFID	WIFI	LORA
Débit utile (Kb/s)	> 100	1000	20 à 250	9,6 à 100	106 à 424	/	10 000 à 900 000 (7 000 000 pour 802.11ad)	0.25 à 11
Portée	100 m	10 à 100 m	10 à 20 m	30 à 100 m	10 cm	1 cm à 10 m	10 m à 250m selon standard	0,5 à 20 Km
Domaine Fréquence (MHz)	2400	2400	868/915/2400	868.42 (Europe) 908.42 (US).	13,56	125-135 Khz 13,56 MHz (inclus NFC) 860/908 MHz	2400 et 5000 (45 GHz pour 802.11ad)	868 (Europe)
Capacité de franchissement obstacle	Faible	Faible	Moyenne	Élevée	Très faible	Faible	Élevée	Très élevée
Consommation	Faible	Élevée	Très faible	Faible	Faible	Faible	Élevée	Très faible
Normalisation	IEEE 802.15.1	IEEE 802.15.1	IEEE 802.15.4 (PHY+MAC) Zigbee alliance pour protocole réseau/transpo rt/application	ITU-T G.9959 (PHY + MAC) Z-wave alliance pour protocole réseau/transpo rt/application	ISO14443 (radio) NFC Forum pour protocole réseau/transpo rt/application	ISO14443 ISO18000	IEEE 802.11.(x) avec nombreuses évolutions	LORA Alliance Brevet SEMTECH pour couche PHY

Caractéristiques	Bluetooth LE	Bluetooth (classique)	Zigbee	Z-wave	NFC	RFID	WIFI	LORA
Usage domaine civil	Smartphone Domotique Résidences intelligentes Santé	Smartphone Domotique Résidences intelligentes Santé	Domotique Smart Energy Smart Grid Applications low energy	Envoi d'informations en temps-réel, domotique : alarmes interrupteurs capteurs...	Contrôle d'accès (PRODEF) Paielements Billetterie et ticketing (transports, loisirs...),	Identification Logistique Télécommande (UHF) Étiquetage (BF) Capteurs, systèmes anti-démarrage, alarme Suivi d'objets,... (BF)	Large dans le domaine SIC (entreprise, usage personnel ...)	Envoi de mesures à intervalles réguliers : consommation eau/gaz/élec., températures, humidité, données de fréquentation ...

La technologie Bluetooth repose sur la pile protocolaire suivante :



Mode de sécurité Bluetooth classique :

La spécification propose 3 modes de sécurité. Ces modes de sécurité sont déployés ou non dans les équipements selon la décision prise par les fabricants. Les modes de sécurité sont les suivants :

- Mode 1 : non sécurisé :
 - Permet d'offrir à un appareil d'offrir ces services à tout dispositif à portée.
- Mode 2 : sécurisé au niveau applicatif :
 - Permet de sécuriser de façon logicielle le dispositif en paramétrant les profils applicatifs.
- Mode 3 : sécurisé au niveau de la liaison :
 - Permet d'établir une connexion avec authentification et chiffrement au moyen d'une clé.

Mode de sécurité Bluetooth LE

- Mode 1 : Ajout de sécurité en rajoutant une couche de chiffrement et d'authentification.
 - **Niveau 1 :** Pas d'authentification, ni de chiffrement requis. Un niveau à proscrire évidemment puisqu'il ne signifie aucune sécurité pour votre objet.
 - **Niveau 2 :** Communication chiffrée (AES-CMAC), mais pas d'authentification de l'objet.
 - **Niveau 3 :** Communication chiffrée (AES-CMAC) et authentification de l'objet.
 - **Niveau 4 :** Communication chiffrée (avec la méthode ECDH et BLE 4.2) et authentification de l'objet.
- Mode 2 : Ce mode ajoute une signature de la donnée pendant la communication entre les objets.
 - **Niveau 1 :** Pas d'authentification, mais la donnée est signée.
 - **Niveau 2 :** Authentification et la donnée signée.

Appairage :

Deux dispositifs destinés à communiquer ensemble devront être couplés au moyen d'une clé symétrique. Cette étape permet aux deux appareils de partager une clé secrète utilisée pour chiffrer et déchiffrer les données. Cette clé secrète est conçue au moyen d'un algorithme mettant en œuvre l'adresse physique des dispositifs appairés, de nombres aléatoires et d'un sésame fourni par l'utilisateur (code PIN, mot de passe, etc...).

Vulnérabilités liées à la conception du protocole :

Ces vulnérabilités sont notamment décrites dans le « *Guide To Bluetooth Security* » du NIST.

- Un *PassKey* statique pourrait faciliter une attaque de l'homme du milieu (MITM).
- Les tentatives d'authentification ne sont pas limitées.
- Il n'y a pas nativement de délai entre deux challenges d'authentification. Un attaquant pourrait recueillir un nombre important de réponses pour récupérer des informations sur la clé de liaison. La norme Bluetooth (Bluetooth Core Spec V5.0, Vol.2, Part H, 5.1) décrit des parades.
- L'ajout d'un délai exponentiel après les tentatives d'authentification n'est pas natif mais implémentable.
- Le mode « sécurité 1 niveau 1 » ne fournit aucun mécanisme de sécurité.
- La robustesse du générateur de nombres aléatoires n'est pas connue. Il pourrait générer des nombres statiques ou périodiques.

Menaces liées à l'implémentation (cas académique ou scénarios d'attaques existants) :

- Bluesnarfing ;
- Bluejacking ;
- Bluebugging ;
- Car Whisperer ;
- Fuzzing attacks ;
- Pairing Eavesdropping ;
- Secure Simple Pairing attacks.

Mesures de sécurité pour les systèmes sans fil utilisant la technologie Bluetooth

SSFIL-BTH 01 : Il est **RECOMMANDÉ** d'utiliser des versions *Bluetooth* disposant de protection contre l'écoute passive (telles que les versions 4.2 et 5.0).

SSFIL-BTH 02 : Il est **OBLIGATOIRE** d'utiliser le mode de sécurité « mode 3 » avec la technologie *Bluetooth* classic et « mode 1 niveau 3 » avec la technologie *Bluetooth LE*.

SSFIL-BTH 03 : Il est **RECOMMANDÉ** d'utiliser une méthode d'appairage sécurisé hors bande. À défaut, il est **OBLIGATOIRE** d'utiliser la méthode « Numeric Comparison » avec la technologie *Bluetooth LE Secure Connections* et la méthode « Passkey Entry » avec la technologie *Bluetooth LE Legacy Pairing*.

SSFIL-BTH 04 : Il est **RECOMMANDÉ** d'utiliser l'algorithme « AES-128-CCM » avec la technologie *Bluetooth*. À défaut, il est **OBLIGATOIRE** d'utiliser un chiffrement de niveau applicatif en complément de « E0-SAFER » prévu par la norme.

ANNEXE 3 : RFID

La note [EMA-DGA-RFID] et le vadémécum de la DGA [VM-DGA-RFID] reste des documents de référence pour les projets utilisant les technologies RFID.

Les technologies RFID sont spécialisées pour les usages dits « sans contact » formant des familles et des protocoles distincts :

Famille RFID	Description	Cas d'usage civil	Type de mémoire	Distance (mètre)
Propriétaire 125 KHz	Basic RFID Passif	Contrôle d'Accès, Inventaire/logistique	ROM EPROM	~ 1
EPC Global/ISO18000 900 MHz à 2.45GHz	Basic RFID Passif	Autoroutier, Inventaire/logistique	ROM EPROM	~ 10
ISO/IEC 15693 13.56 MHz	Étiquette intelligente Passif	Contrôle d'Accès, Inventaire/logistique, Billets Électroniques	ROM RAM EEPROM FRAM	~ 1
ISO/IEC14443 A/ 13.56 MHz	Microcontrôleur Passif	Contrôle d'Accès, Paiement, Passeport électronique	ROM RAM EEPROM FRAM	~ 0.01
Actif RFID 303 MHz à 2400 MHz	Microcontrôleur Actif	Autoroutier, Inventaire/logistique	ROM RAM EEPROM	~ 100

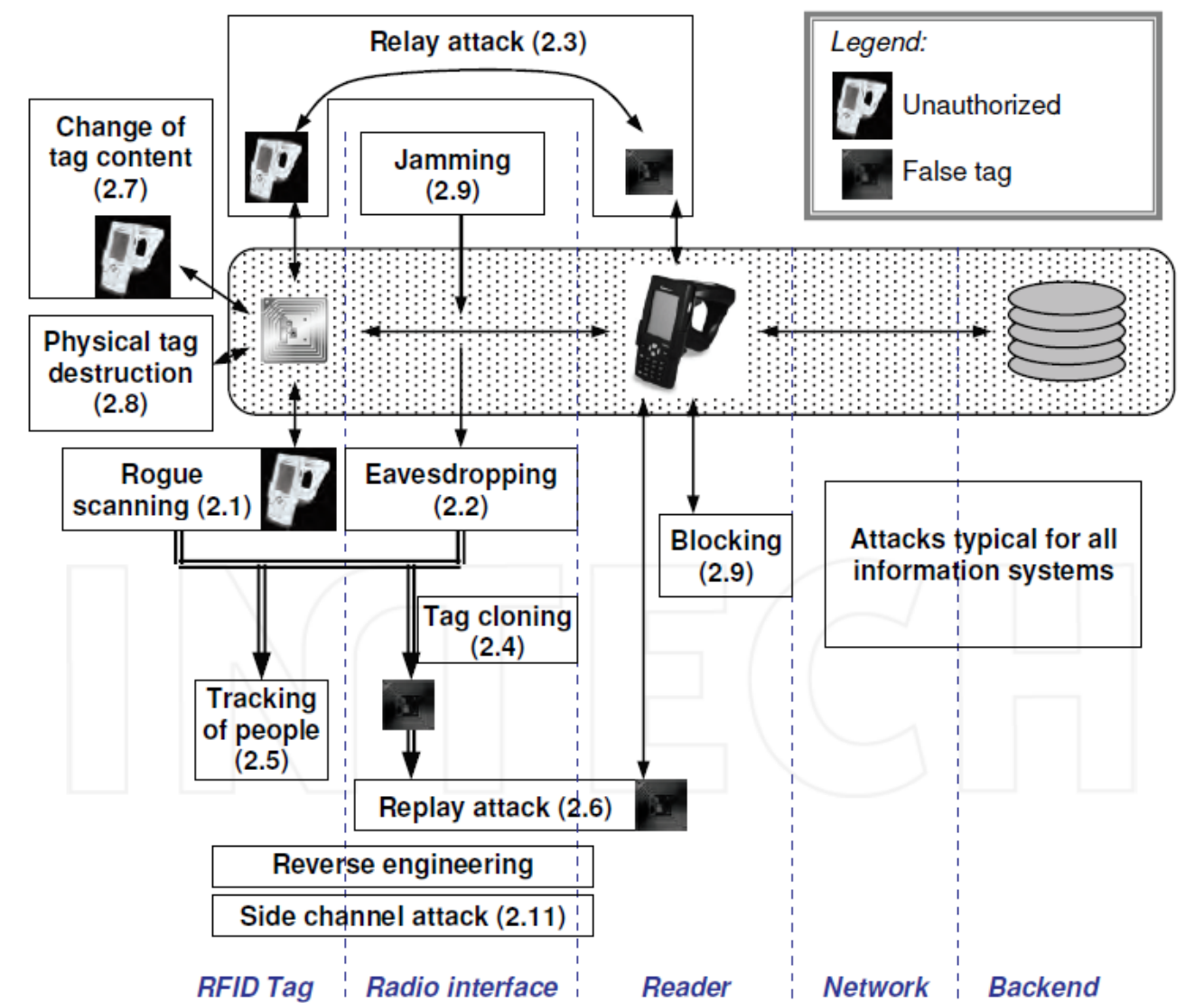
Menaces liées à la conception du protocole

Des outils pour exploiter les vulnérabilités et menaces génériques précitées existent et sont disponibles (RFDump, RFIDwasher) Des travaux académiques¹ détaillent ces *exploits*.

Le schéma suivant² liste les principales possibilités d'attaque sur un système RFID :

¹ ex. IEEE PerCom in March 2006 RFID malware: Design principles and examples

² Source : Paweł Rotter (2009). Security and Privacy in RFID Applications, ISBN: 978-3-902613-54-7



- (2.1) Usurpation d'identité du lecteur en vue d'attenter à l'intégrité/confidentialité des données sur le tag.
- (2.2) Vol d'informations lors des échanges entre un lecteur et un tag
- (2.3) Attaque en relais permettant d'usurper et d'attenter à l'intégrité/confidentialité du contenu du tag sur une distance bien supérieure à celle nominale (cas NFC) prévue par la norme (via faux lecteur en mode proxy)
- (2.4) Contrefaçon de tag par la copie de données valides vers un tag non contrôlé.
- (2.5) Localisation de tag par ses données ou identifiants afin de tracer l'objet à l'insu de son propriétaire.
- (2.7) Modification du contenu du tag par un lecteur usurpé ou non légitime.
- (2.8) Déni de service du tag par désactivation à distance ou destruction physique.
- (2.9) Déni d'accès et d'échanges entre le lecteur et le tag via brouillage.
- (2.9) Déni de service par le ciblage d'un lecteur ou d'une base de données support.

Mesures de sécurité pour un système sans fil utilisant la technologie RFID

- SSFIL-RFID 01:** Il est **OBLIGATOIRE**, avec les technologies RFID de la famille *NFC/ISO 14443*, d'utiliser des mécanismes cryptographiques standardisés pour protéger les fonctions d'authentification, et l'intégrité et la confidentialité des échanges.
- SSFIL-RFID 02:** Il est **RECOMMANDÉ** d'utiliser des mécanismes cryptographiques de type *Lightweight Cryptographic Function* pour les technologies RFID qui ne sont pas de la famille *NFC/ISO 14443* pour protéger les fonctions d'authentification et l'intégrité et la confidentialité des échanges.

- SSFIL-RFID 03 :** Il est **RECOMMANDÉ** d'utiliser des mécanismes de sécurité évalués par l'ANSSI ou par le centre expert de la SSI du ministère (DGA/MI).
- SSFIL-RFID 04 :** Il est **RECOMMANDÉ** d'utiliser un algorithme de type *Distance Bounding Protocol* permettant d'évaluer la distance de communication entre émetteur et récepteur et déjouer les attaques de type relais.
- SSFIL-RFID 05 :** Il est **RECOMMANDÉ** d'utiliser des mécanismes de verrouillage mémoire (« permalock ») conforme à *EPC Global/ ISO 18000-3*.

ANNEXE 4 : ZIGBEE

La norme ZigBee se base sur le standard 802.15.4 de l'organisme IEEE dédié au Low Rate Wireless PAN pour ses couches physiques et logiques (OSI 1 à 2). Il est à noter que d'autres protocoles dans le domaine industriel (ISA 100 ou Wireless HART) s'appuient également sur cette couche standardisée 802.15.4 mais ont développé des couches protocolaires supérieures différentes.

ZigBee fait l'objet d'un regroupement d'industriels, sous le nom Zigbee Alliance, concernant sa normalisation et sa certification.

Zigbee s'appuie sur la pile protocolaire (équivalence couche OSI 1 à 7) suivante :

Application Profile	ZRC	ZID	ZLL	ZHA	ZBA	ZTS	ZRS	ZHC	ZSE 1.x	ZSE 2.0
Network	RFC4CE		PRO							Zigbee IP
MAC	IEEE 802.15.4 – MAC									
PHY	IEEE 802.15.4 – 2,4GHz									

Nota : Zigbee existe aussi sur la bandes ISM 800-900 MHz.

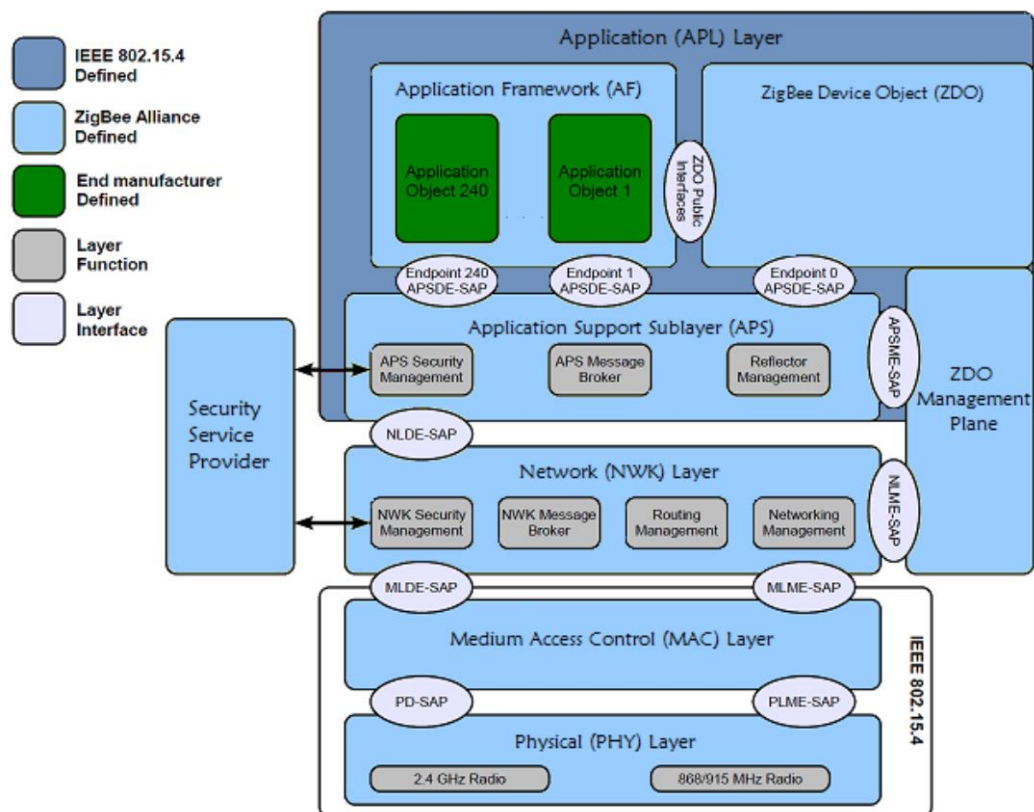
Chaque profil d'application est orienté pour un domaine métier particulier régi par la Zigbee Alliance (par exemple ZSE concerne le smart Energy fonctionnant sur IP).

ZigBee se caractérise par ailleurs par des topologies réseau différenciées de type maillée, en arbre ou en étoile.

À ce titre, au sein d'un réseau Zigbee, on distingue trois grands rôles :

- coordinateur : c'est l'équipement le plus évolué, il est unique pour chaque réseau ZigBee. Typiquement, le coordinateur est connecté à une passerelle réseau et est responsable de l'élaboration du réseau ZigBee et de sa maintenance. En terme de sécurité, il peut agir comme un centre de confiance (Trust Center) pour l'établissement et la gestion des clés, ainsi que l'authentification de chaque équipement ;
- routeur : il agit comme un équipement intermédiaire capable de transmettre des paquets à d'autres équipements ;
- end device : il ne participe pas au routage. Il s'agit en général des équipements avec le moins de capacités.

La figure suivante montre l'empilement de protocoles de ZigBee, réparties sur les couches précédemment décrites :



La sécurité dans ZigBee :

Le niveau de sécurité offert par l'architecture de sécurité ZigBee dépend de la protection des clés symétriques, des mécanismes de protection utilisés, ainsi que de la bonne mise en œuvre des mécanismes cryptographiques et des politiques de sécurité.

ZigBee utilise certains éléments de sécurité de la norme 802.15.4. Il étend les fonctionnalités de cette norme en utilisant :

- des clés de chiffrement AES d'une taille de 128 bits ;
- définition de différentes clés pour sécuriser les communications : Master, Link, Network ;
- utilisation de l'algorithme CCM ;
- utilisation d'un Trust Center (TC) ;
- sécurité qui peut être personnalisée par application.

Les 3 types de clés pour assurer la sécurité des échanges :

- **Link Key** : entre 2 équipements pour protéger les trames sur la couche APS ;
- **Network Key** : pour les actions de la couche réseau (routage, requête pour joindre le réseau, etc.) et pour prévenir l'insertion illégitime d'un équipement ;
- **Master Key** : pour partager le secret initial entre deux équipements lorsqu'ils effectuent la procédure d'établissement de clé (SKKE) pour générer la Link Key.

Afin de distribuer les clés, plusieurs méthodes peuvent être utilisées par les constructeurs :

- pré-installation sur l'équipement ;
- transport ;
- établissement : les équipements négocient avec le centre de confiance pour établir les clés sans qu'elles soient transportées en utilisant l'une de ces trois techniques :
 - o SKKE (Symmetric-Key Key Establishment) ;
 - o CBKE (Certificate-based Key Establishment) ;
 - o ASKE (Alpha-secure Key Establishment).

Menaces associées

Des outils pour exploiter les vulnérabilités et menaces génériques précitées existent et sont disponibles (killerbee, secbee).

Dès lors qu'un attaquant est en portée, la découverte et la cartographie des nœuds ne peut être empêchée car cette visibilité participe au fonctionnement du protocole.

Une attaque de type sniffing permet la récupération passive d'informations (identifiants PAN, adresse MAC réelle du Trust Center Link Key, etc.). Aussi, dans le cas où le chiffrement n'est pas utilisé, il est possible pour un attaquant de capturer le trafic en clair.

Si le trafic est chiffré, et dans le cas d'une implémentation par défaut de certains profils d'application ZigBee comme ZHA, il est possible de déchiffrer l'ensemble des trames réseau. Ceci est réalisable, car la clé (Trust Center Link Key) par défaut est connue « ZigBeeAlliance09 ».

Enfin, bien que certains mécanismes de chiffrement soient considérés comme robustes pour résister à différentes attaques existantes, ils ne sont pas forcément tous implémentés par les constructeurs ce qui engendre de multiples menaces sur les équipements utilisant ce protocole.

Mesures de sécurité pour les systèmes sans fil utilisant la technologie ZigBee

- SSFIL-ZB 01 :** Il est **OBLIGATOIRE** de mettre en œuvre les mécanismes d'authentification des nœuds prévus par la norme ZigBee.
- SSFIL-ZB 02 :** Il est **OBLIGATOIRE** d'utiliser le mécanisme de chiffrement AES-128 CCM pour communiquer.
- SSFIL-ZB 03 :** Il est **OBLIGATOIRE** de définir le coordinateur en mode dit « commercial » ou « haute sécurité » dans la norme.
- SSFIL-ZB 04 :** Il est **RECOMMANDÉ** d'affecter le rôle *Trust Center* à un équipement redondé de type *Coordinateur* dédié aux aspects sécurité.
- SSFIL-ZB 05 :** Il est **OBLIGATOIRE** de préconfigurer tous les équipements d'un réseau ZigBee avec l'adresse du *Trust Center*.
- SSFIL-ZB 06 :** Il est **OBLIGATOIRE** d'utiliser les mécanismes de *Network Key* prévus par la norme. En particulier, gestion des clés par le Trust Center et mises à jour à chaque ajout/suppression d'un équipement/nœud.
- SSFIL-ZB 07 :** Il est **RECOMMANDÉ** de privilégier des mécanismes dits « *out-of band* » pour charger les clés sur les équipements. À défaut, il est **RECOMMANDÉ** le mécanisme *CBKE*.
- SSFIL-ZB 08 :** Il est **OBLIGATOIRE** de pré-assigner un identifiant PAN et de restreindre la connectivité des nœuds.
- SSFIL-ZB 09 :** Il est **OBLIGATOIRE** de mettre en place les mécanismes de filtrage des adresses MAC.

ANNEXE 5 : WIFI

La technologie Wi-Fi a fortement évolué depuis 1999 en produisant de nombreux protocoles :

Famille Protocole	Date de sortie	Fréquence / Largeur de bande	Débit théorique maximal
802.11a	1999	5GHz / 20MHz	54Mbits/s
802.11b	1999	2,4GHz / 22MHz	11Mbits/s
802.11g	2003	2,4GHz / 22MHz	54Mbits/s
802.11n	2009	2,4GHz/20MHz 5GHz / 40MHz	Jusqu'à 600Mbits/s (dans une configuration de 4x4 MIMO et de 40MHz de largeur de bande)
802.11ac	2012	5GHz / 20, 40, 80, 160 MHz	Jusqu'à 6,77Gbits/s (dans une configuration de 8x8 MIMO et de 160MHz de largeur de bande)
802.11ax (WIFI 6)	2018	2,4GHz / 20, 40, 80, 160 MHz 5GHz / 20, 40, 80, 160 MHz	Jusqu'à 9,60 Gbits/s (dans une configuration de 8x8 MIMO et de 160MHz de largeur de bande) Des latences réduites de 70% par rapport à 802.11ac sont annoncées

Menaces associées

Des outils pour exploiter les vulnérabilités et menaces génériques précitées existent et sont disponibles (trousse à outils de Metasploit).

Parmi les vulnérabilités d'envergure récentes, citons notamment KRACK en 2017 qui constitue une attaque par réinstallation de la clef de session et réinitialisation du l'IV (initial vector) sur le protocole Wi-Fi. Cela a conduit le consortium « WIFI Alliance » à lancer le WPA3 en 2018 supportant entre autre l'AES CCM en 192 bits.

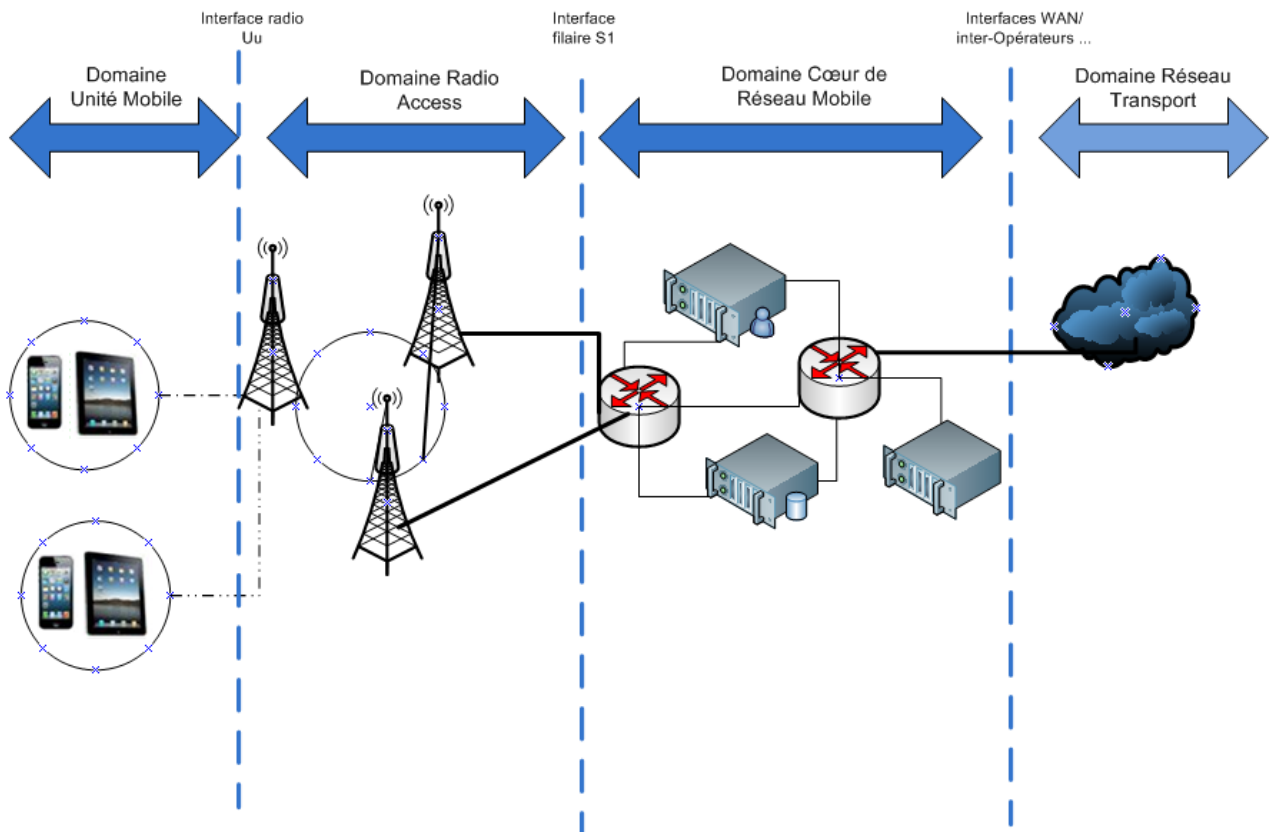
Mesures de sécurité pour les systèmes sans fil utilisant la technologie WIFI

- SSFIL-WIFI 01 :** Il est **OBLIGATOIRE** de désactiver le mode de connexion automatique aux réseaux WIFI sur les équipements terminaux. Il est **OBLIGATOIRE** de désactiver le mode WPS sur les équipements d'accès.
- SSFIL-WIFI 02 :** Il est **OBLIGATOIRE** d'activer, a minima, le mode WPA-2 avec l'algorithme de chiffrement AES CCMP et d'un firmware à jour non vulnérable à KRACK pour les équipements terminaux et points d'accès sous emprise ministérielle, et d'utiliser le management frame protection (802.11w),
- SSFIL-WIFI 03 :** Il est **OBLIGATOIRE** d'utiliser le standard 802.1X avec les protocoles robustes (type EAP-TLS, EAP-TTLS) pour l'authentification, auprès de l'infrastructure, des points d'accès sous emprise ministérielle. Ces mécanismes d'authentification doivent s'appuyer sur une infrastructure d'authentification filaire adressant des services type RADIUS, AD et provisionnant des certificats d'une autorité reconnue par le Ministère des Armées. Cette mesure est **RECOMMANDE** pour les équipements terminaux.

- SSFIL-WIFI 04 :** Il est **OBLIGATOIRE**, de séparer, entre le point d'accès et le réseau filaire interfacé, la partie donnée de la partie supervision et administration et de la partie contrôle (RADIUS) lorsqu'une infrastructure d'authentification est mise en œuvre. Cette séparation est effectuée au moyen de VLANs ou d'interfaces filaires séparées).
- SSFIL-WIFI 05 :** Dans le cas spécifique d'un réseau WIFI de nature public/invité (qui ne doit pas être interconnecté à d'autres réseaux du Ministère) et pour les terminaux WIFI accueillis, à défaut de l'implémentation de la règle SSFIL-WIFI-03 :
- il est **OBLIGATOIRE** d'utiliser, a minima, une méthode authentification à base de clé pré-partagée (WPA-PSK) ;
 - il est **OBLIGATOIRE** de choisir une clé WPA-PSK avec un mot de passe long (vingt caractères par exemple) et complexe ;
 - il est **OBLIGATOIRE** de renouveler cette dernière avec une fréquence en adéquation avec l'analyse de risques menée ;
 - il est **OBLIGATOIRE** pour les personnels utilisateurs de ces terminaux d'être authentifié par un mode portail captif avec login/mot de passe à usage unique et délivré à chaque utilisateur.
- SSFIL-WIFI 06 :** Il est **RECOMMANDÉ** d'utiliser une configuration Private VLAN invité en mode *isolated* au niveau du point d'accès hormis pour les besoins ToIP.
- SSFIL-WIFI 07 :** Il est **OBLIGATOIRE** de définir et mettre en place des politiques de sécurité pour les différents équipements terminaux (politique de chiffrement, cloisonnement VLAN, affectation aux VLANs infrastructure ...). Il est **RECOMMANDÉ** de centraliser la gestion et le contrôle de ces politiques. *Par exemple on visera à différencier les terminaux mobiles utilisant de la VoIP sur wifi des équipements portables échangeant des données bureautiques.*
- SSFIL-WIFI 08 :** Il est **RECOMMANDÉ** de mettre en œuvre des techniques de détection d'intrusion type WIDS/WIPS au niveau des équipements d'accès et de contrôle sans fil.
- SSFIL-WIFI 09 :** Il est **OBLIGATOIRE** d'anonymiser, si ce dernier n'a pas pour finalité l'accès au public, l'identifiant ou le nom du réseau sans fil en veillant à ne faire aucune mention permettant l'identification d'un organisme du Ministère, **RECOMMANDÉ** du constructeur de l'équipement, et du service offert.
- SSFIL-WIFI 10 :** Il est **DÉCONSEILLÉ** de diffuser l'identifiant ou le nom du réseau sans fil hormis pour les réseaux sans fil du ministère dont la finalité est l'accès au public.

Principe directeur des réseaux cellulaires mobiles

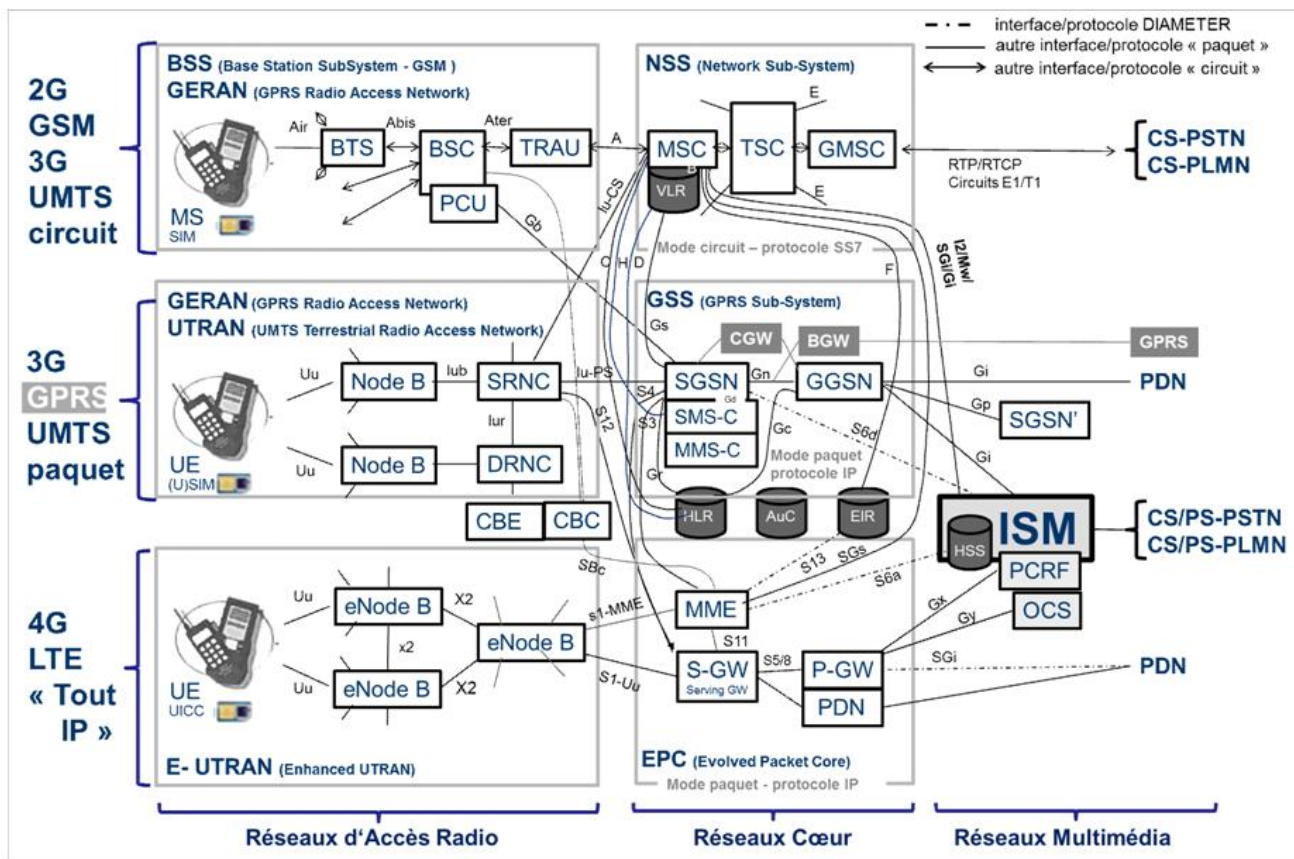
Schéma de principe de l'architecture en couches des réseaux :



Le réseau est constitué :

- L'unité mobile (UE) ou équipement utilisateur : terminaux multi-usage (data/voix) de type ordiphone, téléphone mobile (*tout équipement doté d'une carte SIM*) ;
- Les stations de radiocommunications (BTS, NodeB ou eNodeB en fonction des générations) qui constituent la couche d'accès radio ;
- Le réseau de cœur (MSC, EPC en fonction des générations) qui constitue la couche de cœur de réseau gérant les abonnés et les communications entre éléments de la couche radio et à destination d'autres infrastructures (WAN, communication voix inter-opérateur ...) ;
- Le réseau de transport est généralement hors périmètre.

Cette architecture simplifiée ne considère pas les infrastructures et les interconnexions avec d'autres réseaux opérateurs.



Pour la 5G (en cours de normalisation) le schéma de principe va probablement évoluer vers une approche distribuée à destination des composants dits d'extrémités (Edge Network) pour des fonctions qui sont à ce jour concentrées et situées dans l'infrastructure de cœur.

Celles-ci seraient moins centralisées et plus orientées « logiciel » (fonction dite Network Function Virtualize ou Software Defined Network).

Cela constitue de nouveaux risques en termes d'architecture de sécurité.

Menaces et Vulnérabilités

Des outils pour exploiter les vulnérabilités et menaces génériques précitées existent et deviennent plus facile d'accès avec le développement de la radio logicielle (Software Defined Radio).

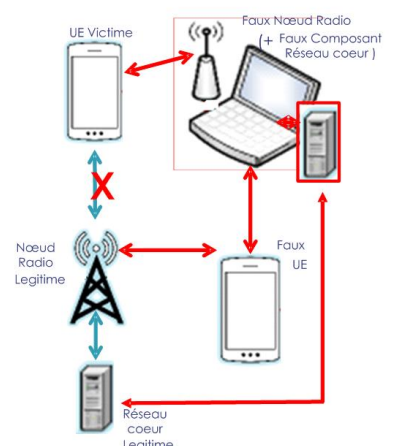
Sources : [ENISA 5G] – [JANUS]

Les classes de vulnérabilités inhérentes à ces technologies :

- Les attaques et vulnérabilités propres au mode de fonctionnement de la couche radio qui s'intéresse à la signalisation et à la gestion des identités par le réseau (divulgaration précoce des identités sans protection de la 2G par exemple).

À ce titre Les attaques permettant à l'attaquant de se faire passer pour un nœud réseau d'accès radio (dite de type « homme du milieu ») sont les plus courantes. Elles permettent de :

- forcer les procédures d'itinérance et d'identification (IMSI grabber);
- forcer les modes de communication affaiblis (bascule 2G ou 3G, intégrité et chiffrement les plus faibles etc.);
- solliciter l'opérateur légitime pour réémettre les informations de l'abonné: identifiants, les clés de sessions, voire clés natives.



Ces attaques sont facilitées lorsque les protocoles de sécurité (chiffrement / authentification) sont obsolètes.

- Les vulnérabilités et attaques propres aux réseaux cœurs et aux interfaces avec les réseaux tiers: écoutes des interfaces, analyse des flux (sonde DPI) ou détournement de flux de signalisation (en particulier SS7 dans les protocoles 2G/3G).
Elles permettent de :
 - forcer l'itinérance ;
 - récupérer les informations de sessions utilisateurs (clés, identités sur le réseau) ;
 - forcer les bascules de 5G/4G vers 3G/2G et profiter ainsi des faiblesses (avec ou sans réauthentification de l'abonné selon les cas par exemple) des protocoles associés ;
 - dénier l'accès à certains services.
- Les vulnérabilités et attaques qui concernent les terminaux UE et leur gestion/cycle de vie :
 - les attaques permettant le clonage ou l'exfiltration de données des (U)SIM et l'exploitation de vulnérabilités dans les outils tels que les SIM Toolkit (STK) ou les faiblesses dans les protocoles d'échange OTA (over the air) utilisés par les opérateurs pour mettre à jour les applicatifs hébergés sur les cartes USIM ;
 - les attaques type spyware, trojan, activation des services de géolocalisation à l'insu de l'utilisateur.
- Les vulnérabilités et attaques propres à la couche physique radio :
 - quasi-absence de protection TRANSEC et faiblesse inhérente à certaines techniques d'utilisation du spectre radio (telle qu'OFDM dans la 4G par exemple) sensibles au brouillage et leurrage ;
 - défauts d'implémentation des protocoles par les équipementiers ou fabricants de terminaux ;
 - défauts dans les processus de sécurité des opérateurs (absence d'usage de passerelle de sécurité pourtant prévue par les normes 3GPP entre opérateurs de « même niveau de confiance », faiblesse de la gestion des vulnérabilités/correctifs).

Mesures de sécurité pour les systèmes sans fil utilisant la technologie 2G, 3G, 4G et 5G

Pour la 5G, la recommandation pour le moment est de s'appuyer sur le document cadre [ENISA_5GTOOLS] comprenant des mesures génériques de nature technique.

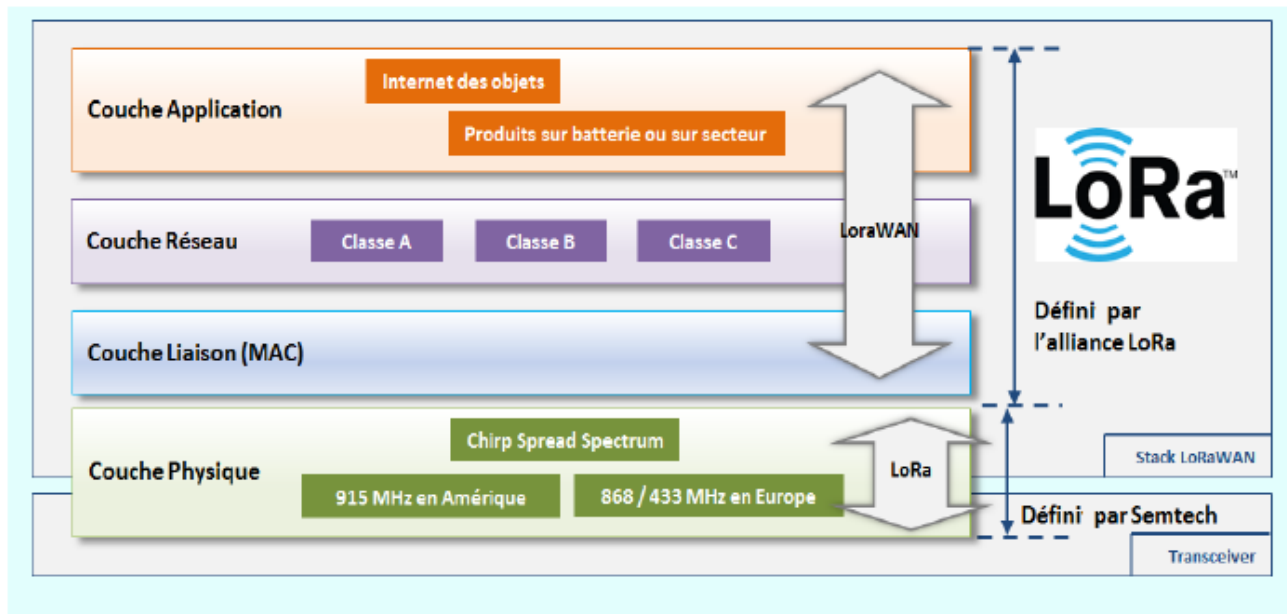
Cas déploiement environnement non maîtrisé (Opérateur Réseau Mobile, Opérateur Virtuel Réseau Mobile) :

- SSFIL- XG 01 :** Il est **OBLIGATOIRE** de maîtriser la gestion et les configurations des équipements déployés. Pour y parvenir, il est **RECOMMANDÉ** d'utiliser une solution de type MDM (Mobile Device Management).
- SSFIL- XG 02 :** Il est **CONSEILLÉ** d'utiliser le mode accès 4G et limiter l'itinérance vers des réseaux 2G/3G. NB : le protocole DIAMETER mis en œuvre en 4G/5G est réputé plus sûr que Radius mis en œuvre dans infrastructure 2G/3G.

Cas déploiement environnement maîtrisé ou devant être maîtrisé pour des besoins opérationnels

- SSFIL- XG 03 :** Il est **OBLIGATOIRE** de conduire une analyse de risque spécifique pour les déploiements en environnement maîtrisé ou devant faire être maîtrisé pour des besoins opérationnels.

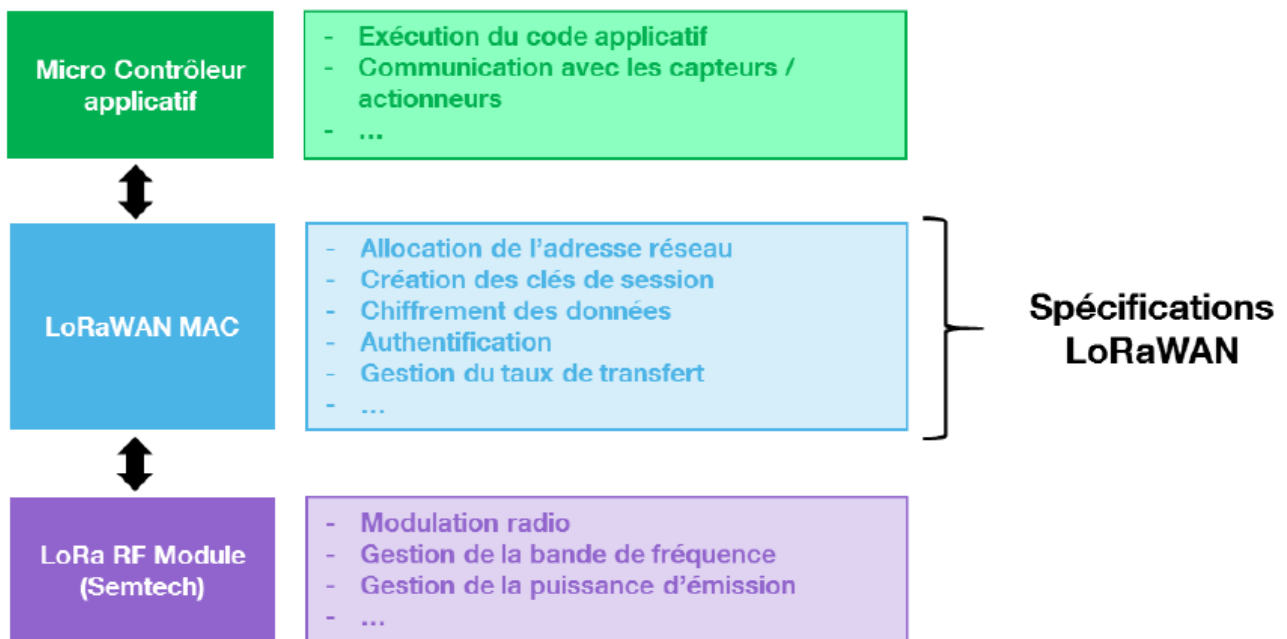
ANNEXE 7 : LORAWAN



La technologie LoRA repose sur une couche propriétaire définie par la société Semtech.

L'interopérabilité et la standardisation pour les couches logiques LoraWAN en termes d'implémentation est garantie par l'« alliance LoRA » consortium de plusieurs industriels.

Au sein d'un équipement IoT sur un réseau LORAWAN, ce dernier se définit par les couches de fonctions suivantes :



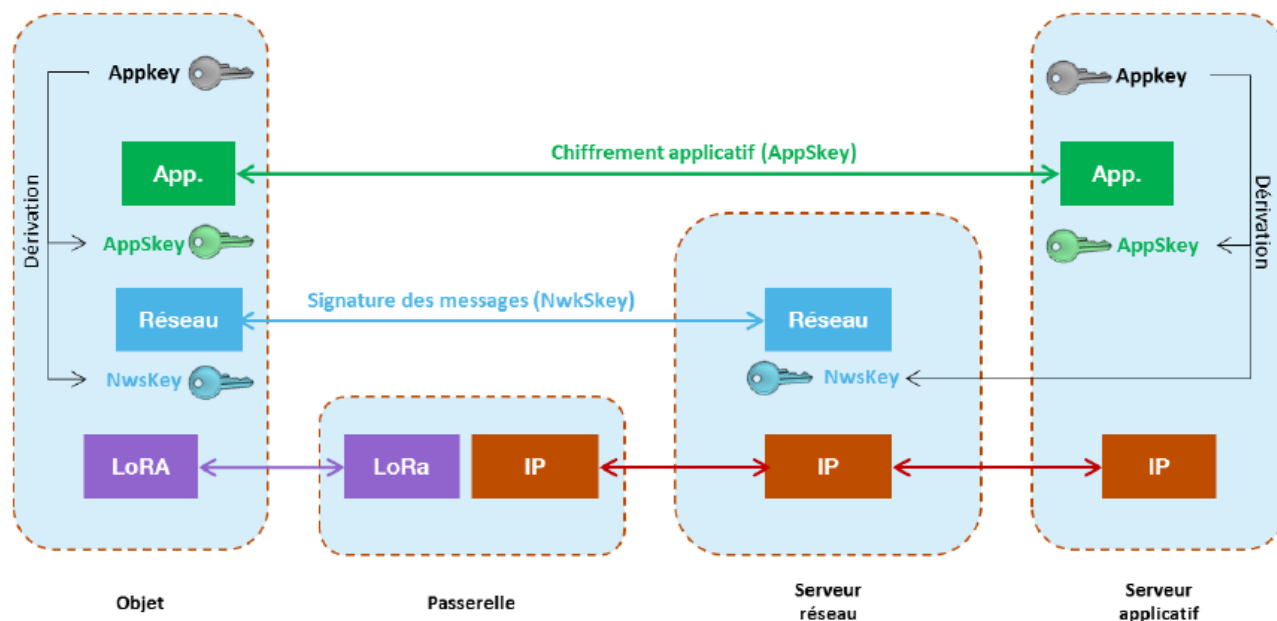
Menaces par conception du protocole

Au niveau physique :

- l'absence de mécanisme de sécurité rend vulnérable tant au brouillage qu'à l'interception sur des portées importantes ;
- la facilité d'attaque sur l'objet est fonction du durcissement initial (absence de port de maintenance ou USB exposé ...) et de l'accessibilité physique.

Au niveau logique :

- Les mécanismes d'échanges de clés peuvent être sensibles à des écoutes ou attaques par rejeu en vue de se substituer à un objet légitime en demandant à l'infrastructure dédiée de se ré-authentifier.



Des mécanismes de sécurité au niveau logique font l'objet des spécifications LORAWAN. Elles sont adaptées aux contraintes (faible consommation, faible capacité) des équipements de type « Internet des objets » correspondants.

Ces mécanismes reposent sur un jeu de clés symétriques (2 clés de sessions et 1 clé applicative) échangées avec l'infrastructure dédiée (serveur applicatif/serveur réseau) avec mécanisme de dérivation à la génération. La clé applicative est de type AES-128 et sert d'identifiant unique de l'objet (renouvelable par mécanisme de type « over the air »).

Mesures de sécurité pour les systèmes sans fil utilisant la technologie LORAWAN

SSFIL- LRWN 01 : Il est **DÉCONSEILLÉ** d'utiliser la technologie LORAWAN car son protocole est propriétaire. À défaut les mesures suivantes sont à appliquer.

SSFIL- LRWN 02 : Il est **RECOMMANDÉ** d'utiliser la version 1.1 de LORAWAN plutôt que la version 1.0

SSFIL- LRWN 03 : Il est **OBLIGATOIRE** d'utiliser un aléa robuste pour **générer les clés mises en œuvre dans le réseau LORA-WAN**. *NB : le déploiement dans le domaine civil fait souvent l'objet d'une dérivation de clés basées sur l'identifiant de l'objet. Cette pratique ne constitue pas un aléa robuste. À ce titre, ANSSI ou NIST définissent des règles associées à ces aléas.*

SSFIL- LRWN 04 : Il est **RECOMMANDÉ** d'utiliser un *secure element* au niveau des mécanismes cryptographiques des équipements terminaux (passerelle et objet) du réseau LORA WAN.