



ÉCOLE SUPÉRIEURE DE TECHNOLOGIE
UNIVERSITÉ HASSAN II DE CASABLANCA

École Supérieure de Technologie de Casablanca
Département Génie Informatique

INTERNET DES OBJETS

Architecture, Technologies et Applications

Support de cours

Pr. Moad Hicham Safhi

Département Génie Informatique

Email : h.m.safhi@gmail.com

Website : <https://safhi.me>

Internet des Objets

Table des matières

1	Chapitre 1 : Introduction à l'Internet des Objets	3
1.1	Contexte et Définitions Fondamentales	3
1.1.1	Le Phénomène IoT dans Notre Quotidien	3
1.1.2	IoT vs. M2M : Clarification Conceptuelle	3
1.2	Évolution Historique et Contexte	4
1.2.1	Les Quatre Phases d'Évolution d'Internet	4
1.2.2	Jalons Historiques Clés	4
1.3	Motivation et Intérêt Économique	4
1.3.1	Les Forces Motrices de la Révolution IoT	5
1.3.2	Impact Sectoriel et Domaines d'Application	6
1.4	Architecture et Fonctionnement des Systèmes IoT	6
1.4.1	La Boucle de Contrôle IoT : Sense-Think-Act	6
1.4.2	Modèles Architecturaux	7
1.4.3	Technologies Sous-jacentes	8
1.5	Défis et Perspectives	8
1.5.1	Les Cinq Grands Défis Techniques et Sociétaux	9
1.5.2	Tendances Futures	9
2	Chapitre 2 : La Couche de Perception : Capteurs et Actionneurs	9
2.1	Introduction à la Couche de Perception	9
2.1.1	Rôle Fondamental de la Couche de Perception	9
2.2	Composants des Systèmes IoT : Rôles et Interactions	10
2.2.1	Les Trois Composants Fondamentaux	10
2.2.2	Exemples d'Applications par Secteur	10
2.3	Les Capteurs : Principes et Classification	11
2.3.1	Définition et Principes de Fonctionnement	11
2.3.2	Critères de Choix d'un Capteur	11
2.3.3	Principes Physiques des Capteurs	12
2.4	Étude des Principaux Types de Capteurs	13
2.4.1	Capteurs de Température	13
2.4.2	Capteurs d'Humidité	13
2.4.3	Capteurs de Luminosité	14
2.4.4	Autres Capteurs Spécialisé	14
2.5	Les Actionneurs : Principes et Applications	14
2.5.1	Définition et Rôle des Actionneurs	14
2.5.2	Principaux Types d'Actionneurs	15
2.5.3	Critères de Choix d'un Actionneur	15
2.6	Les Contrôleurs : Cerveaux des Systèmes IoT	16

2.6.1	Rôle et Définition des Contrôleurs	16
2.6.2	Microcontrôleurs vs Microprocesseurs	16
2.6.3	Plateformes Matérielles Courantes en IoT	17
2.6.4	Focus sur Arduino : Philosophie et Écosystème	18
2.7	Connectivité et Protocoles de Communication	19
2.7.1	Importance de la Connectivité dans l'IoT	19
2.7.2	Topologies Réseau pour l'IoT	19
2.7.3	Critères de Choix des Technologies de Communication	20
2.7.4	Bandes de Fréquences et Réglementation	20
3	Chapitre 3 : Protocoles de Communication IoT	21
3.1	Introduction aux Protocoles IoT	21
3.1.1	Besoins et Enjeux des Protocoles IoT	21
3.1.2	Architecture en Couches des Protocoles IoT	22
3.2	Protocoles d'Infrastructure et d'Identification	22
3.2.1	Protocoles d'Infrastructure Réseau	23
3.2.2	Protocoles d'Identification	23
3.3	Protocoles de Communication et Transport	23
3.3.1	Réseaux Courte/Moyenne Portée	24
3.3.2	Réseaux Longue Portée (LPWAN)	24
3.4	Protocoles de Découverte et de Données	25
3.4.1	Protocoles de Découverte de Services	25
3.4.2	Protocoles d'Échange de Données	26
3.5	Protocole CoAP (Constrained Application Protocol)	26
3.5.1	Principes Fondamentaux du CoAP	26
3.5.2	Caractéristiques Techniques du CoAP	27
3.5.3	Mécanisme Observe et Interopérabilité	27
3.6	ProtocolMQTT (Message Queuing Telemetry Transport)	28
3.6.1	Principes Fondamentaux du MQTT	28
3.6.2	Composants et Connexions MQTT	29
3.6.3	Topics et Filtrage MQTT	29
3.6.4	Qualité de Service (QoS) MQTT	31
3.6.5	Fonctionnalités Avancées MQTT	31
4	Chapitre 4 : Réseaux LPWAN et Technologie LoRa	32
4.1	Introduction aux Réseaux LPWAN	32
4.1.1	Définition et Contexte des LPWAN	32
4.1.2	Objectifs et Compromis des LPWAN	33
4.1.3	Cas d'Usage Typiques des LPWAN	33
4.2	Technologie LoRa et LoRaWAN	33
4.2.1	Comprendre la Distinction Fondamentale : LoRa vs LoRaWAN	34
4.2.2	La Modulation LoRa : Chirp Spread Spectrum (CSS)	35
4.2.3	Pourquoi LoRaWAN est-il Exceptionnel ?	36
4.2.4	Architecture LoRaWAN : Topologie "Star-of-Stars"	36
4.2.5	Classes de Devices LoRaWAN	38
4.2.6	Sécurité LoRaWAN	40
4.2.7	Performances et Limitations Réelles	41
4.2.8	Écosystème et Cas d'Usage	41
4.2.9	Conclusion sur LoRa/LoRaWAN	42
	References	43

1 Chapitre 1 : Introduction à l'Internet des Objets

1.1 Contexte et Définitions Fondamentales

1.1.1 Le Phénomène IoT dans Notre Quotidien

Dans notre environnement quotidien, de nombreux dispositifs intègrent des capteurs et des capacités de communication pour interagir avec leur environnement et échanger des données. Des systèmes de contrôle d'accès par badge aux capteurs environnementaux dans les bâtiments intelligents, en passant par les dispositifs de suivi de la consommation énergétique, ces systèmes forment un écosystème interconnecté où des objets physiques collectent, traitent et transmettent des informations. Cette réalité marque l'avènement de l'Internet des Objets.

Définition

Internet des Objets (IdO) / Internet of Things (IoT) : Un réseau d'objets physiques identifiables, équipés de capacités de communication et de traitement, qui échangent des données pour surveiller et piloter des processus du monde réel. Ces objets, capables d'envoyer des informations et de recevoir des ordres via Internet, forment un système intégré reliant le monde physique au monde numérique.

Pour bien comprendre cette définition, il convient de décomposer ses éléments constitutifs :

- **Internet** : Réseaux d'ordinateurs interconnectés basés sur des protocoles de communication standardisés (TCP/IP).
- **Objets (Things)** : Tout élément physique identifiable du monde réel (capteurs, actionneurs, dispositifs).
- **Connectivité** : Capacité à échanger des données via des réseaux (Wi-Fi, Bluetooth, LoRa, 5G, etc.).
- **Intelligence** : Traitement des données (local ou distant) pour analyse et prise de décision.

1.1.2 IoT vs. M2M : Clarification Conceptuelle

Une distinction importante doit être établie entre l'IoT et le M2M (Machine-to-Machine), souvent confondus.

M2M (Machine-to-Machine)	IoT (Internet des Objets)
<ul style="list-style-type: none"> - Communication directe entre appareils - Connexions point-à-point dédiées - Principalement industriel et fermé - Peu ou pas d'intelligence embarquée <p>Exemple : Télésurveillance industrielle</p>	<ul style="list-style-type: none"> - Écosystème connecté via Internet - Architecture décentralisée et ouverte - Applications grand public et industrielles - Intelligence distribuée et données massives <p>Exemple : Maison connectée, ville intelligente</p>

TABLE 1 – Comparaison entre M2M et IoT

Point Clé

L'IoT n'est pas simplement "des objets connectés à Internet". C'est un système intégré qui relie le monde physique au monde numérique pour observer, comprendre et agir sur l'environnement, souvent sans intervention humaine constante : Objets intelligents + Connectivité + Traitement des données + Valeur applicative.

1.2 Évolution Historique et Contexte

1.2.1 Les Quatre Phases d'Évolution d'Internet

La figure suivante illustre l'évolution conceptuelle d'Internet en quatre phases distinctes :

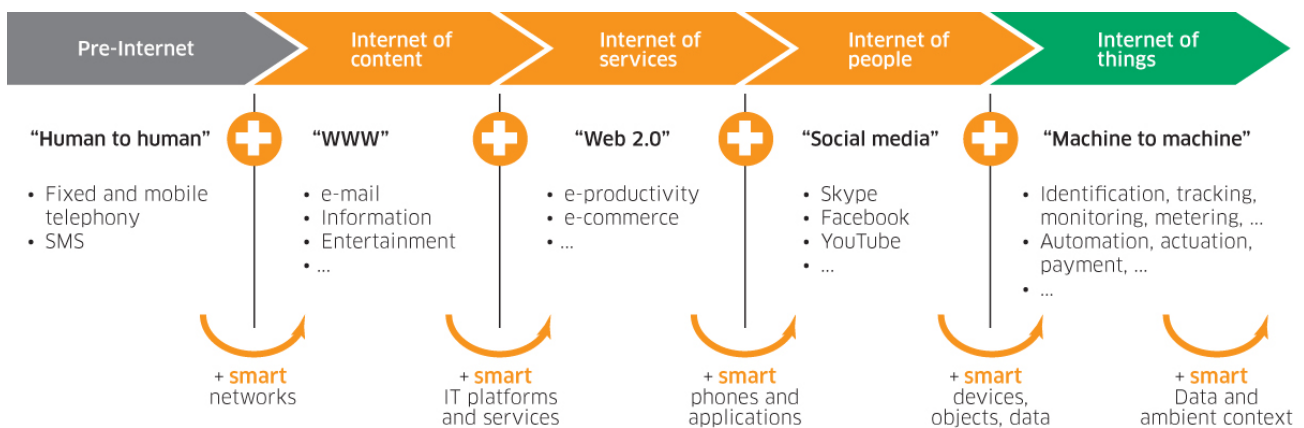


FIGURE 1 – Les phases d'évolution d'Internet (Source Nokia Insights)

Comme le montre la figure, l'IoT représente la quatrième phase de cette évolution, où ce ne sont plus seulement les humains mais les objets du monde physique qui deviennent acteurs actifs du réseau.

1.2.2 Jalons Historiques Clés

L'histoire de l'IoT est ponctuée d'innovations marquantes :

- **1982** : Première machine connectée ; une machine à soda à l'Université Carnegie Mellon qui envoyait son niveau de remplissage par email.s
- **1990** : Premier grille-pain connecté à Internet (contrôlable via TCP/IP).
- **1999** : Kevin Ashton invente le terme "Internet of Things" pour décrire les micropuces RFID.
- **2008** : Le nombre d'objets connectés dépasse le nombre d'habitants sur Terre.
- **2016** : Attaque Mirai ; botnet créé avec des caméras de sécurité piratées qui a bloqué Twitter, Netflix et Reddit.
- **2020-2025** : Explosion des "villes intelligentes" et intégration de l'IA embarquée (edge AI).

1.3 Motivation et Intérêt Économique

1.3.1 Les Forces Motrices de la Révolution IoT

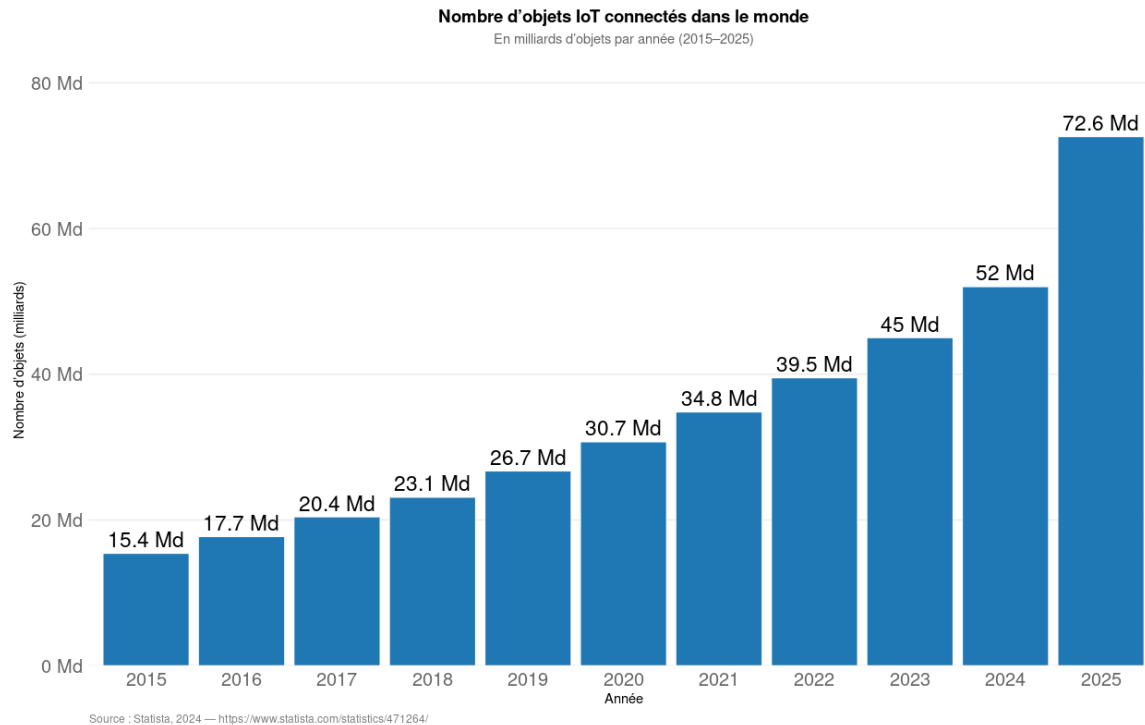


FIGURE 2 – Croissance exponentielle du marché IoT (Source : IoT Analytics)

L'explosion de l'IoT s'explique par la convergence de plusieurs facteurs :

a. **Progrès technologiques**

- Miniaturisation des composants électroniques.
- Baisse drastique des coûts matériels (capteurs, microcontrôleurs).
- Évolution des réseaux de communication (5G, LoRaWAN, NB-IoT).
- Amélioration de l'autonomie énergétique (batteries, énergie ambiante).

b. **Infrastructures émergentes**

- Cloud Computing ubiquitaire et abordable.
- Plateformes IoT spécialisées (AWS IoT, Azure IoT Hub).
- Outils de développement simplifiés (Arduino IDE, PlatformIO).

c. **Évolution des usages et attentes**

- Transformation numérique des entreprises.
- Attentes croissantes des consommateurs pour des solutions connectées.
- Développement des villes intelligentes (smart cities).
- Vieillesse démographique et santé connectée.

d. **Facteurs économiques stratégiques**

- Nouveaux modèles économiques basés sur les données.
- Marché en croissance exponentielle (estimé à 1 500 milliards USD en 2025).
- Gains d'efficacité opérationnelle significatifs.

1.3.2 Impact Sectoriel et Domaines d'Application

L'IoT transforme profondément tous les secteurs économiques :

Secteur	Applications IoT et Impact
Industrie 4.0	Surveillance continue des machines, maintenance prédictive, réduction des temps d'arrêt, traçabilité complète.
Santé Connectée	Suivi à distance des patients, télémédecine, localisation du matériel médical, gestion des stocks de médicaments.
Villes Intelligentes	Gestion optimisée des ressources (éclairage, eau, déchets), stationnement intelligent, qualité de l'air, sécurité publique.
Agriculture de Précision	Irrigation automatisée, surveillance des cultures et du bétail, optimisation des rendements, réduction des intrants.
Logistique et Transport	Traçabilité des marchandises, gestion de flotte, maintenance préventive des véhicules, optimisation des itinéraires.
Bâtiments Intelligents	Gestion énergétique optimisée, confort des occupants, sécurité des biens et personnes, maintenance prédictive.
Commerce de Détail	Gestion automatique des stocks, expérience client personnalisée, analyse du comportement en magasin.

TABLE 2 – Domaines d'application majeurs de l'IoT

Point Clé

Création de valeur : L'IoT crée de la valeur lorsqu'il résout un problème concret dans le monde physique. Son succès dépend de sa capacité à générer des bénéfices mesurables (économies, nouveaux revenus, amélioration du service) supérieurs aux coûts d'implémentation.

1.4 Architecture et Fonctionnement des Systèmes IoT

1.4.1 La Boucle de Contrôle IoT : Sense-Think-Act

Le fonctionnement d'un système IoT repose sur une boucle de contrôle fermée, souvent décrite par le paradigme **Sense-Think-Act** :

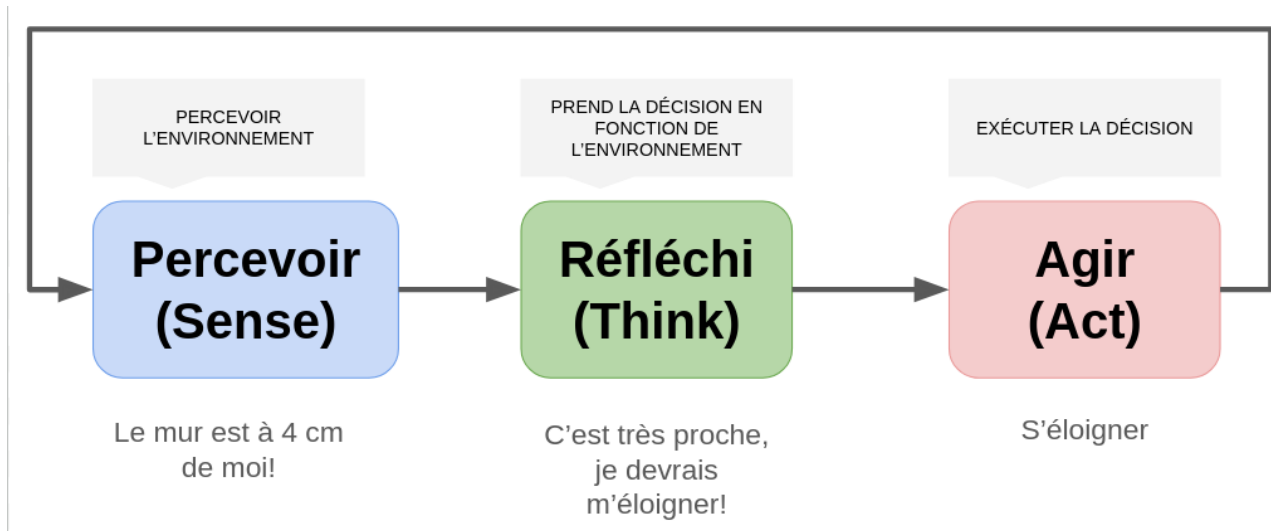


FIGURE 3 – La boucle de contrôle Sense-Think-Act dans les systèmes IoT

1. **Sense (Perception)** : Les capteurs détectent les changements dans l'environnement.
2. **Think (Traitement)** : Le système analyse les données et prend des décisions.
3. **Act (Action)** : Les actionneurs exécutent les actions physiques correspondantes.

Cette boucle permet une automatisation intelligente et en temps réel, où le système adapte continuellement son comportement en fonction des observations du monde physique.

1.4.2 Modèles Architecturaux

1.4.2.1 Architecture en 3 Couches (Modèle Universel)

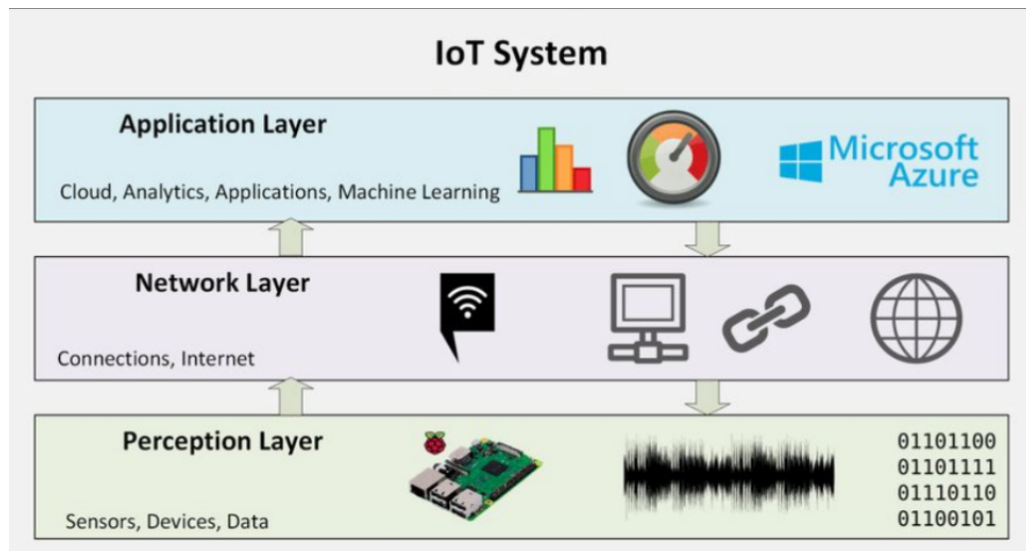


FIGURE 4 – Architecture IoT en 3 couches

1. **Couche de Perception (Perception Layer)** : Regroupe les capteurs et actionneurs en contact avec le monde physique.
2. **Couche Réseau (Network Layer)** : Assure le transport des données entre les objets et les systèmes de traitement.

3. **Couche Application (Application Layer)** : Traite les données et fournit des services aux utilisateurs finaux.

1.4.3 Technologies Sous-jacentes

L'IoT repose sur plusieurs technologies complémentaires :

1. **Réseaux de Capteurs Sans Fil (WSN)** : Réseaux d'objets autonomes dotés de capteurs, reliés par liaison radio.
2. **Cloud Computing** : Fourniture de ressources de calcul et de stockage à la demande via Internet.
3. **Big Data** : Technologies permettant de traiter des volumes massifs de données IoT.
4. **Protocoles de Communication** : Règles d'échange d'informations entre objets (MQTT, CoAP, LoRaWAN, etc.).
5. **Systèmes Embarqués** : Microcontrôleurs intégrant processeur, mémoire et interfaces d'E/S.

Exemple Concret

Exemple d'architecture complète : Un thermostat intelligent suit le parcours suivant : Capteur de température -> Microcontrôleur ESP32 -> Wi-Fi -> Broker MQTT -> Cloud AWS -> Tableau de bord web -> Application mobile -> Alertes SMS. Cette chaîne illustre parfaitement l'intégration des différentes couches et technologies IoT.

1.5 Défis et Perspectives

1.5.1 Les Cinq Grands Défis Techniques et Sociétaux

Défi	Problématique	Solutions Émergentes
Sécurité	Vulnérabilités multiples, attaques DDoS, failles de mise à jour	Chiffrement systématique, mises à jour automatiques, authentification forte
Vie Privée	Collecte massive de données personnelles, consentement flou	Conformité RGPD, anonymisation des données, politiques transparentes
Interopérabilité	Multiplicité des protocoles propriétaires, incompatibilités	Standards ouverts (Matter), passerelles universelles, API normalisées
Gestion Énergétique	Autonomie limitée, contraintes d'alimentation	Capteurs à très basse consommation, énergie ambiante, optimisation logicielle
Coût et Accessibilité	Investissement initial élevé, complexité de déploiement	Économies d'échelle, modèles SaaS, subventions publiques

TABLE 3 – Principaux défis de l'IoT et solutions associées

1.5.2 Tendances Futures

Les évolutions technologiques en cours dessinent l'avenir de l'IoT :

- **Edge Computing et Edge AI** : Déplacement du traitement des données vers la périphérie du réseau pour réduire la latence et la consommation de bande passante.
- **5G et Réseaux Dédiés** : Déploiement de réseaux à très haut débit et faible latence permettant de nouvelles applications temps réel.
- **Intégration IA/ML** : Algorithmes d'apprentissage automatique embarqués pour l'analyse prédictive et la prise de décision autonome.
- **Blockchain pour l'IoT** : Technologies distribuées pour la traçabilité, la sécurité et la confiance dans les échanges.
- **Durabilité et Éco-conception** : Focus sur l'impact environnemental des dispositifs IoT (recyclage, faible consommation, matériaux biosourcés).

2 Chapitre 2 : La Couche de Perception : Capteurs et Actionneurs

2.1 Introduction à la Couche de Perception

2.1.1 Rôle Fondamental de la Couche de Perception

La couche de perception constitue l'interface entre le monde physique et le système numérique dans l'architecture IoT. C'est à ce niveau que les grandeurs physiques (température, pression,

mouvement, etc.) sont transformées en signaux électriques puis en données numériques exploitables par les systèmes informatiques. Cette conversion est réalisée par deux familles de dispositifs complémentaires : **les capteurs** et **les actionneurs**.

Définition

Couche de Perception (Perception Layer) : Niveau d'abstraction le plus bas de l'architecture IoT, regroupant l'ensemble des dispositifs (capteurs, actionneurs, identifiants) qui interagissent directement avec l'environnement physique pour collecter des données ou exécuter des actions.

2.2 Composants des Systèmes IoT : Rôles et Interactions

2.2.1 Les Trois Composants Fondamentaux

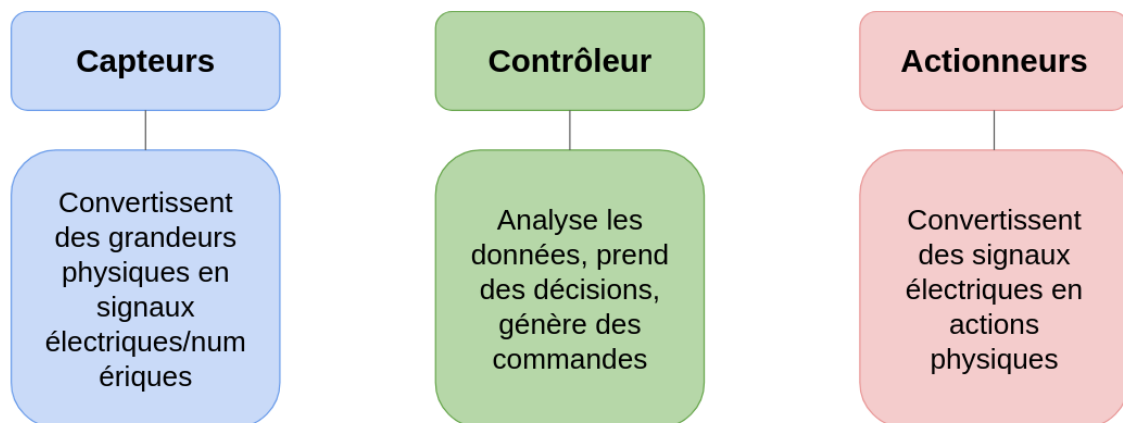


FIGURE 5 – Rôles des composants fondamentaux d'un système IoT

2.2.2 Exemples d'Applications par Secteur

L'interaction capteurs-contrôleur-actionneurs permet de résoudre des problèmes concrets dans divers domaines :

Secteur	Chaîne Sensorielle	Bénéfice Apporté
Domotique	Capteur luminosité -> Contrôleur -> Stores motorisés	Confort visuel et économie d'énergie
Agriculture	Capteur humidité sol -> Contrôleur -> Pompe d'irrigation	Optimisation de la consommation d'eau
Industrie 4.0	Capteur vibration -> Contrôleur -> Arrêt machine	Maintenance prédictive, sécurité des équipements
Santé Connectée	Capteur rythme cardiaque -> Contrôleur -> Alerte secours	Surveillance médicale continue et réactive

TABLE 4 – Applications concrètes de la boucle Sense-Think-Act par secteur

Point Clé

Le cycle complet d'automatisation : Un système IoT réalise un cycle complet d'interaction avec le monde réel : 'Monde physique -> Données -> Décision -> Action -> Monde physique'. Cette circularité permet aux systèmes IoT de s'adapter dynamiquement à leur environnement.

2.3 Les Capteurs : Principes et Classification

2.3.1 Définition et Principes de Fonctionnement

Définition

Capteur (Transducteur) : Dispositif qui convertit une grandeur physique mesurable (température, pression, lumière, mouvement, etc.) en signal électrique exploitable par un système électronique ou informatique. Ce sont les « yeux » et les « oreilles » électroniques du système IoT.

Le fonctionnement d'un capteur suit généralement trois étapes :

1. **Interaction** avec la grandeur physique à mesurer.
2. **Conversion** en signal électrique (analogique ou numérique).
3. **Conditionnement** du signal pour l'exploitation par le système.

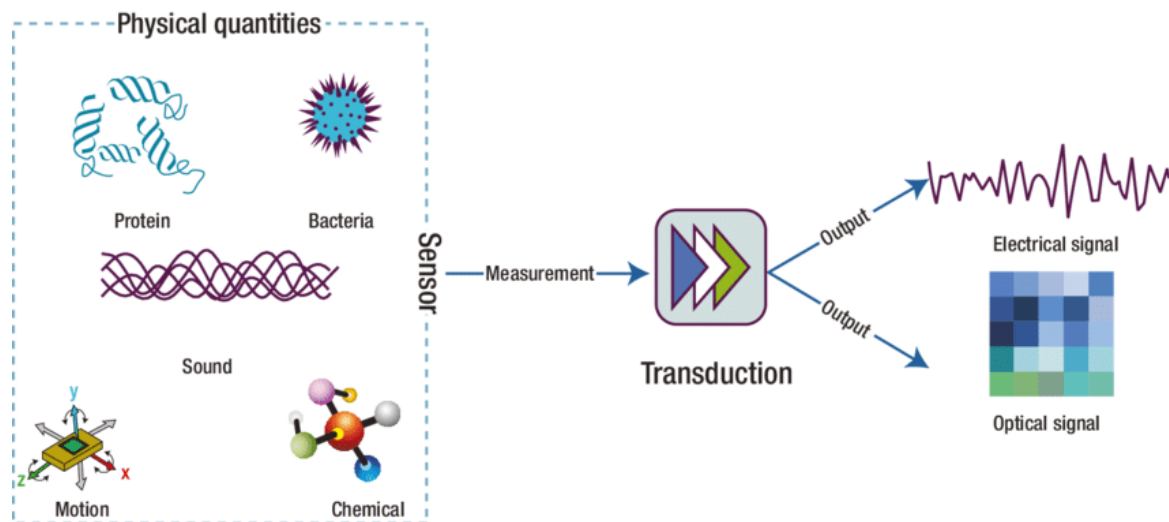


FIGURE 6 – Processus de conversion d'une grandeur physique en signal

2.3.2 Critères de Choix d'un Capteur

La sélection du capteur idéal pour les projet IoT nécessite une analyse de plusieurs facteurs. Voici les principaux éléments à considérer :

Précision : La capacité du capteur à fournir des mesures proches de la réalité. Particulièrement crucial dans les applications médicales ou industrielles où la moindre erreur peut avoir des conséquences graves.

Plage de mesure : L'étendue des valeurs que le capteur peut mesurer. Il est essentiel de choisir un capteur dont la plage couvre toutes les variations possibles dans votre environnement d'utilisation.

Résolution : La plus petite variation que le capteur peut détecter. Si votre application nécessite de détecter des changements infimes, comme dans les systèmes de surveillance de précision, ce critère devient primordial.

Temps de réponse : Le délai entre la détection d'un changement et la transmission de la mesure. Les applications en temps réel, comme les systèmes de contrôle industriel ou les dispositifs médicaux, nécessitent des temps de réponse très courts.

Résistance aux conditions environnementales : La capacité du capteur à fonctionner dans des conditions spécifiques de température, d'humidité ou de pression. Par exemple, les capteurs utilisés en extérieur ou dans des environnements industriels doivent être particulièrement robustes.

Consommation énergétique : La quantité d'énergie nécessaire au fonctionnement du capteur. Un facteur déterminant pour les appareils fonctionnant sur batterie, où l'autonomie est un enjeu majeur.

Coût : Le prix d'achat, mais aussi les coûts de maintenance et de remplacement. Dans les projets à grande échelle, même une petite économie par unité peut représenter des économies significatives.

Facilité d'intégration : La compatibilité avec les systèmes existants et la simplicité d'installation. Un capteur plus cher mais facile à intégrer peut s'avérer plus économique à long terme.

Fiabilité et durée de vie : La capacité du capteur à maintenir ses performances dans le temps. Un capteur plus cher mais plus fiable peut être plus rentable qu'une solution bon marché nécessitant des remplacements fréquents.

Support technique et documentation : La qualité de la documentation et la disponibilité d'un support technique peuvent faire la différence, surtout dans les environnements professionnels.

2.3.3 Principes Physiques des Capteurs

Les capteurs reposent sur quelques idées physiques simples : une grandeur physique modifie une propriété électrique (tension, courant, résistance, capacité, etc.).

- **Piézoélectricité** : Une contrainte mécanique (choc, vibration, pression) déforme un matériau et génère une petite tension mesurable. Exemple : capteurs de choc, capteurs de pression, accéléromètres.
- **Variation de résistance** : La résistance d'un matériau change avec la température, la lumière ou la déformation.
Exemple : thermistances (température), jauges de contrainte (effort), LDR (luminosité).

- **Effet Hall** : Un courant soumis à un champ magnétique crée une tension latérale.
Exemple : capteurs de position ou de vitesse de rotation (moteurs, roues).
- **Effets optiques (photoélectrique, photovoltaïque)** : La lumière libère ou déplace des charges électriques dans un matériau.
Exemple : photodiodes, cellules photovoltaïques, capteurs de luminosité.
- **Absorption infrarouge par les gaz** : Certains gaz absorbent une partie d'un faisceau infrarouge : la quantité absorbée dépend de la concentration.
Exemple : détecteurs de CO , analyseurs de gaz.

2.4 Étude des Principaux Types de Capteurs

2.4.1 Capteurs de Température

Les capteurs de température sont parmi les plus répandus dans les applications IoT. Retenez surtout les grandes familles plutôt que chaque référence précise :

- **Capteurs résistifs (thermistances, RTD)**
La résistance du capteur varie avec la température.
Utilisés lorsque l'on cherche une bonne précision sur une plage de température modérée (stations météo, domotique, procédés industriels).
- **Thermocouples**
Deux métaux différents forment une jonction qui génère une tension liée à la température.
Utilisés surtout pour les températures très élevées ou difficiles d'accès (fours, moteurs).
- **Capteurs sans contact / numériques (IR, capteurs intégrés)**
Mesurent le rayonnement infrarouge émis par un objet ou intègrent directement la mesure et la conversion numérique (I2C, 1-Wire, etc.).
Idéals pour les objets connectés : simples à interfacer, avec souvent une calibration interne (exemple : DHT22, DS18B20).

2.4.2 Capteurs d'Humidité

Idée centrale : l'humidité modifie une propriété d'un matériau (capacité, résistance, conduction thermique, etc.).

- **Capteurs capacitifs**
L'humidité change la constante diélectrique d'un matériau : la capacité mesurée varie.
Fréquents dans les stations météo, systèmes HVAC, serres agricoles.
- **Capteurs résistifs**
La résistance d'un polymère ou d'un film conducteur change avec l'humidité.
Utilisés dans de nombreux objets du quotidien (smartphones, montres connectées, électroménager).

D'autres technologies (conductivité thermique, optiques, SAW, etc.) existent pour des environnements plus extrêmes ou des mesures très précises, mais l'idée reste la même : *l'humidité influence un paramètre électrique mesuré.*

2.4.3 Capteurs de Luminosité

Tous ces capteurs transforment la lumière en signal électrique ; il est plus utile d'en retenir les usages typiques que de mémoriser toutes les variantes.

- **LDR / photoconducteurs**

La résistance diminue quand la lumière augmente.

Très économiques, parfaits pour l'allumage automatique de lampes ou la détection jour/nuit.

- **Photodiodes et phototransistors**

La lumière génère un courant ou amplifie un courant existant.

Utilisés quand on a besoin de rapidité et de précision (télécommandes IR, barrières optiques, communication optique).

- **Capteurs intégrés (RGB, luminosité)**

Petits circuits intégrés qui donnent directement une valeur numérique d'éclairement ou de couleur.

Idéals pour l'éclairage intelligent, la mesure de couleur, les objets connectés.

2.4.4 Autres Capteurs Spécialisé

Capteurs de force et de pression Mesurent une déformation mécanique (piézoélectricité ou jauges de contrainte) pour en déduire une force ou une pression.

Capteurs d'accélération et d'inclinaison Détectent les mouvements et l'orientation grâce à des éléments piézoélectriques ou des microsystèmes MEMS (smartphones, airbags, monitoring structural).

Capteurs à ultrasons Envoyent une onde sonore et mesurent le temps de retour pour estimer une distance (stationnement, mesure de niveau, détection d'obstacles).

2.5 Les Actionneurs : Principes et Applications

2.5.1 Définition et Rôle des Actionneurs

Définition

Actionneur : Dispositif électromécanique ou électromagnétique qui convertit un signal électrique provenant du contrôleur en une action physique sur l'environnement (mouvement, force, chaleur, lumière, etc.). Ce sont les « muscles » du système IoT.

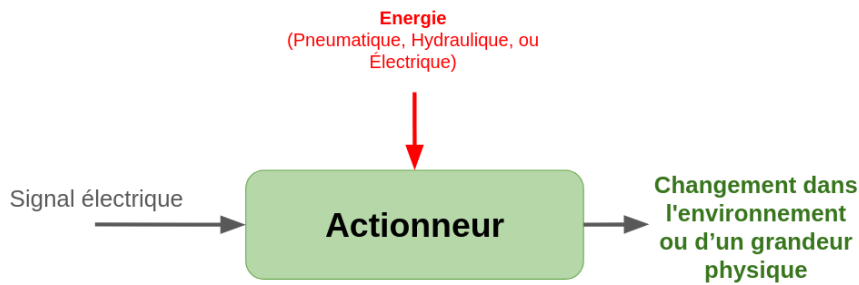


FIGURE 7 – Processus de conversion d’un signal de commande en action physique

2.5.2 Principaux Types d’Actionneurs

Les actionneurs peuvent être regroupés en quelques grandes familles :

- **Moteurs CC** : transforment un courant continu en rotation grâce à l’interaction entre un champ magnétique et un courant électrique.
Utilisés lorsqu’on a besoin d’une rotation continue avec un contrôle simple par la tension (robotique mobile, ouverture/fermeture automatique, petites pompes).
- **Moteurs pas-à-pas** : avancent par petits angles fixes (pas).
Très utiles pour positionner précisément un axe sans capteur de retour (imprimantes 3D, bras robotisés légers, systèmes de focalisation).
- **Servomoteurs** : combinent moteur, réducteur et capteur de position dans un même boîtier.
Permettent de commander directement un angle précis (souvent 0–180°). Courants en modélisme, robotique éducative et pour orienter des caméras.
- **Relais** : utilisent un électroaimant pour ouvrir ou fermer un contact électrique.
Servent à commander de fortes charges (chauffage, éclairage, moteurs) avec un petit signal de commande, tout en assurant une isolation électrique.
- **Électrovannes** : contrôlent l’écoulement d’un fluide (liquide ou gaz) en ouvrant ou fermant un passage.
Très présentes dans l’irrigation automatique, la régulation de débit et les systèmes de chauffage.
- **Affichages (LCD, OLED, 7-segments, etc.)** : convertissent un signal électrique en information visuelle.
Ils constituent l’interface homme-machine directe dans de nombreux objets connectés.
- **Éléments chauffants** : transforment l’énergie électrique en chaleur (effet Joule).
Utilisés pour chauffer ou maintenir une température (thermostats, buses d’imprimantes 3D, plaques ou systèmes de cuisson).

2.5.3 Critères de Choix d’un Actionneur

La sélection d’un actionneur dépend de contraintes techniques et applicatives. Les principaux critères à considérer sont :

- **Type de mouvement** : rotationnel, linéaire ou angulaire.
- **Précision requise** : tolérance acceptable sur la position, l'angle ou le déplacement.
- **Couple / force** : puissance mécanique nécessaire pour entraîner la charge.
- **Vitesse** : plage de fonctionnement en vitesse ou en débit.
- **Niveau de contrôle** : commande simple marche/arrêt ou pilotage plus fin (vitesse, position).
- **Environnement** : température, humidité, poussière, risques d'explosion, etc.
- **Contraintes énergétiques** : tension disponible, courant maximal, autonomie éventuelle.
- **Coût et fiabilité** : budget global et durée de vie attendue de l'installation.

2.6 Les Contrôleurs : Cerveaux des Systèmes IoT

2.6.1 Rôle et Définition des Contrôleurs

Définition

Contrôleur IoT : Unité de calcul (microcontrôleur, automate programmable, ordinateur monocarte) qui exécute les algorithmes de commande, traite les données des capteurs, prend des décisions et pilote les actionneurs, éventuellement en communication avec d'autres systèmes.

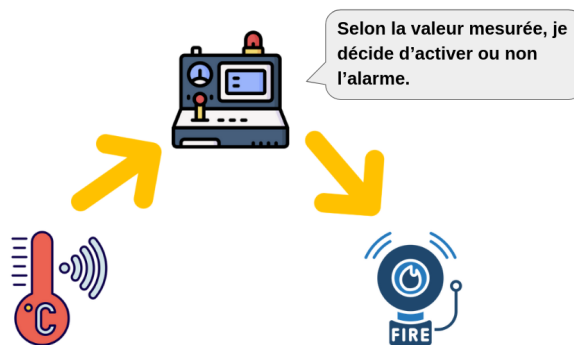


FIGURE 8 – Fonctionnement du contrôleur dans la chaîne IoT

2.6.2 Microcontrôleurs vs Microprocesseurs

Une distinction fondamentale existe entre ces deux familles de composants :

Microprocesseur (μ P)	Microcontrôleur (μ C)
Cœur de calcul généraliste nécessitant composants externes	Système sur puce (SoC) intégrant CPU, mémoire, périphériques
Pour systèmes complexes nécessitant OS complet (Linux, Windows)	Pour systèmes embarqués dédiés, fonctionnant souvent sans OS
Architecture Von Neumann ou Harvard	Architecture généralement Harvard modifiée
Puissance de calcul élevée, consommation importante	Puissance modérée mais consommation optimisée
Exemples : Intel Core i7, AMD Ryzen, ARM Cortex-A	Exemples : ARM Cortex-M, AVR (Arduino), PIC
Applications : Ordinateurs, serveurs, smartphones	Applications : Objets connectés, automobile, domotique

TABLE 5 – Comparaison microprocesseur vs microcontrôleur

Point Clé

Pourquoi les microcontrôleurs dominent l'IoT ? : Leur conception « tout-en-un » (faible coût, faible consommation, compacité) les rend idéaux pour les objets connectés qui doivent fonctionner pendant des années sur batterie tout en restant économiques à produire en masse.

2.6.3 Plateformes Matérielles Courantes en IoT

Plateforme	Type	Caractéristiques Principales	Applications Types
Arduino Uno	Microcontrôleur (AT-mega328P)	16 MHz, 32 KB Flash, 2 KB RAM, entrées/-sorties numériques/analogue	Prototypage éducatif, projets makers, automation simple
ESP32	Microcontrôleur (Xtensa dual-core)	240 MHz, Wi-Fi, Bluetooth, 520 KB RAM, périphériques avancés	IoT connecté, domotique, wearables, interfaces réseau
Raspberry Pi Pico	Microcontrôleur (RP2040)	133 MHz dual-core, 264 KB RAM, PIO programmables	Contrôle avancé, projets nécessitant parallélisme
Raspberry Pi 4	Ordinateur monocarte (ARM Cortex-A72)	1.5-1.8 GHz quad-core, 2-8 GB RAM, Ethernet, USB 3.0, HDMI	Gateway IoT, edge computing, vision par ordinateur

TABLE 6 – Principales plateformes matérielles pour le développement IoT

2.6.4 Focus sur Arduino : Philosophie et Écosystème

Arduino, créé en 2005 à Ivrea (Italie), a révolutionné le prototypage électronique grâce à sa philosophie open-source et sa simplicité d'utilisation.

Avantages clés de l'écosystème Arduino :

- **Langage simplifié** basé sur C++ avec abstraction matérielle.
- **IDE intuitif** et multiplateforme.
- **Vaste bibliothèque** de codes et de shields (extensions).
- **Communauté mondiale** avec milliers de projets partagés.
- **Coût abordable** et matériel largement disponible.

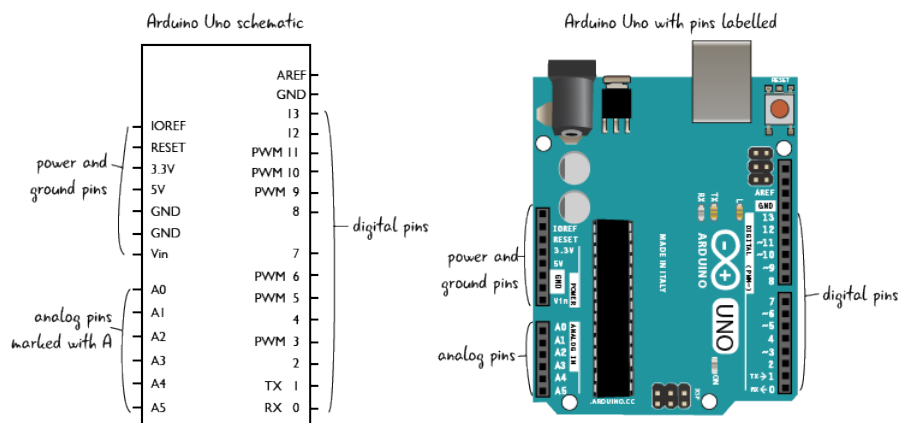


FIGURE 9 – Anatomie d'une carte Arduino

Structure de programmation typique :

```
void setup() {
  // Configuration initiale (exécutée une fois)
  pinMode(13, OUTPUT);      // Broche 13 en sortie
  Serial.begin(9600);       // Initialisation communication série
}

void loop() {
  // Boucle principale (exécutée indéfiniment)
  digitalWrite(13, HIGH);    // Allumer LED
  delay(1000);               // Attendre 1 seconde
  digitalWrite(13, LOW);     // Éteindre LED
  delay(1000);               // Attendre 1 seconde
}
```

Interfaces de communication supportées :

- **UART** : Communication série asynchrone (broches 0-RX, 1-TX).
- **I²C** : Bus à deux fils pour capteurs/actionneurs (A4-SDA, A5-SCL).
- **SPI** : Interface série synchrone haute vitesse (broches 10-13).

- **PWM** : Modulation largeur d'impulsion pour contrôle analogique (broches ~3, ~5, ~6, ~9, ~10, ~11).

2.7 Connectivité et Protocoles de Communication

2.7.1 Importance de la Connectivité dans l'IoT

Définition

Connectivité IoT : Capacité d'un objet à échanger des données avec d'autres objets ou avec des plateformes distantes via des réseaux de communication. C'est cette interconnexion qui transforme un capteur isolé en composant d'un système intelligent.

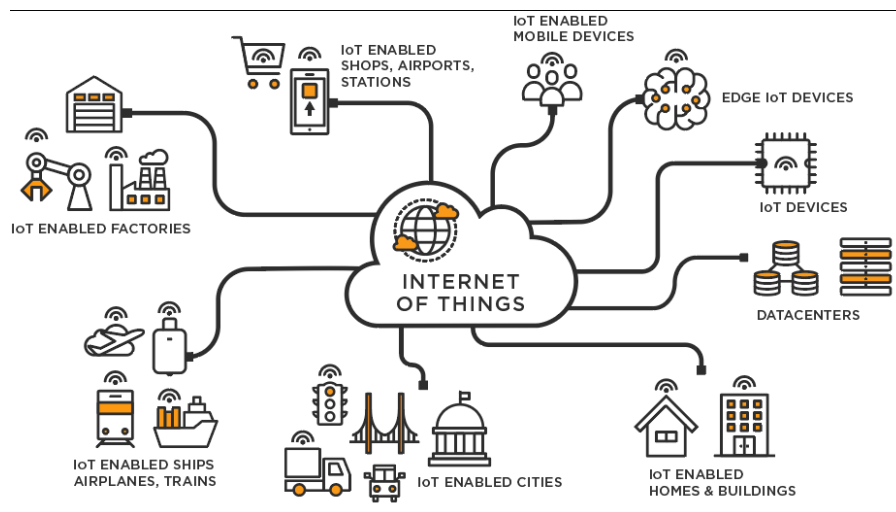


FIGURE 10 – Évolution d'un capteur isolé vers un système IoT interconnecté

2.7.2 Topologies Réseau pour l'IoT

L'organisation des connexions entre objets (topologie réseau) influence fortement les performances du système :

Topologie	Description	Avantages	Inconvénients
Étoile	Tous les nœuds connectés à un concentrateur central	Simplicité, faible consommation des nœuds	Point de défaillance unique, portée limitée
Maillée (Mesh)	Chaque nœud communique avec ses voisins, relayant les messages	Grande résilience, couverture étendue	Consommation élevée, complexité de routage
Arbre	Structure hiérarchique avec nœuds racine et intermédiaires	Évolutivité, organisation claire	Dépendance aux nœuds intermédiaires
Linéaire (Bus)	Nœuds alignés sur un support commun (câble, pipeline)	Simplicité, faible coût de déploiement	Faible résilience, performances limitées
Cellulaire	Division en cellules géographiques avec antennes relais	Couverture très étendue, infrastructure existante	Coût d'abonnement, consommation énergétique

TABLE 7 – Comparaison des principales topologies réseau pour l'IoT

2.7.3 Critères de Choix des Technologies de Communication

Le choix d'une technologie de communication repose sur un compromis entre plusieurs contraintes principales :

- **Portée** : distance maximale de communication entre les nœuds (Bluetooth ou Zigbee pour quelques dizaines de mètres ; LoRa ou NB-IoT pour plusieurs kilomètres).
- **Débit** : volume de données transmissible par unité de temps (Sigfox ou LoRa pour quelques octets épisodiques ; Wi-Fi ou 4G/5G pour des flux continus ou importants).
- **Consommation** : énergie nécessaire pour transmettre et recevoir (Bluetooth Low Energy ou LoRaWAN pour des objets sur batterie ; Wi-Fi lorsque l'alimentation est disponible).
- **Coût** : prix du matériel, de l'infrastructure et des éventuels abonnements (réseaux privés basés sur LoRa ou Zigbee pour de grands déploiements à faible coût ; NB-IoT ou LTE-M lorsqu'on s'appuie sur un opérateur).
- **Fiabilité** : capacité à maintenir la liaison malgré le bruit, les obstacles et les interférences (protocoles maillés comme Zigbee, ou utilisation de répétitions et d'accusés de réception).
- **Sécurité** : niveau de protection contre l'interception et la modification des données (chiffrement et authentification sur Wi-Fi, 4G/5G ou LoRaWAN pour les applications sensibles).

2.7.4 Bandes de Fréquences et Réglementation

Les communications IoT utilisent principalement des bandes de fréquences radio réglementées :

Bande ISM	Fréquences	Technologies IoT Principales
Basse fréquence	13,56 MHz	RFID, NFC (identification à très courte portée)
Fréquence moyenne	433 MHz (EU), 915 MHz (US)	Télécommande, capteurs sans fil propriétaires
Sub-GHz	868 MHz (EU), 915 MHz (US)	LoRa, Sigfox, Zigbee (longue portée, bas débit)
2,4 GHz	2,4-2,4835 GHz (mondial)	Wi-Fi, Bluetooth, Zigbee, Thread (débit moyen)
5 GHz	5,15-5,825 GHz (selon région)	Wi-Fi 5/6, liaisons point à point (haut débit)

TABLE 8 – Bandes ISM (Industriel, Scientifique, Médical) utilisées en IoT

Point Clé

Bandes libres vs licenciées : Les bandes ISM sont libres (pas de licence, utilisation gratuite) mais partagées (risque d'interférences). Les bandes licenciées (ex : fréquences cellulaires) offrent une qualité de service garantie mais nécessitent un paiement à un opérateur.

3 Chapitre 3 : Protocoles de Communication IoT

3.1 Introduction aux Protocoles IoT

3.1.1 Besoins et Enjeux des Protocoles IoT

L'Internet des Objets connecte des milliards d'objets hétérogènes (capteurs, actionneurs, passerelles, plateformes cloud), nécessitant des protocoles de communication spécialisés pour garantir leur interopérabilité et leur bon fonctionnement. Ces protocoles doivent répondre à plusieurs besoins fondamentaux :

1. **Identification** : Attribution d'un identifiant unique à chaque objet.
2. **Transport des données** : Transmission fiable ou opportuniste selon les contraintes.
3. **Découverte de services** : Détection automatique des objets et de leurs capacités.
4. **Gestion des périphériques** : Configuration, mise à jour et supervision à distance.
5. **Interopérabilité** : Communication entre objets de différents fabricants.
6. **Sécurité** : Confidentialité, intégrité et authentification des échanges.

Définition

Protocole IoT : Ensemble de règles et de formats standardisés qui régissent l'échange d'informations entre les différents composants d'un système IoT, de la couche physique jusqu'à l'application.

3.1.2 Architecture en Couches des Protocoles IoT

Les protocoles IoT sont organisés selon une architecture en couches fonctionnelles, adaptée aux contraintes spécifiques des objets connectés (faible consommation, bande passante limitée, capacité de calcul réduite) :

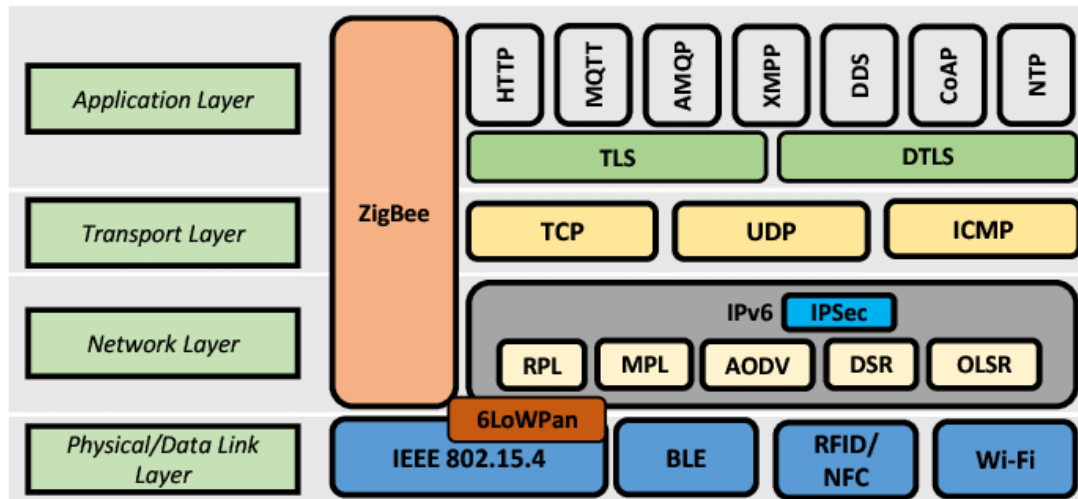


FIGURE 11 – Architecture en couches des protocoles IoT

On peut distinguer plusieurs couches fonctionnelles principales :

- **Infrastructure** : adressage et routage dans des environnements contraints (IPv6, 6LoWPAN, RPL).
- **Identification** : attribution d'identifiants uniques aux objets et aux ressources (adresses MAC, adresses IPv6, URI, EPC/uCode).
- **Communication** : transmission des données sur le support physique ou radio (Wi-Fi, Bluetooth, LoRa, NB-IoT).
- **Découverte** : détection automatique des services et des objets disponibles sur le réseau (mDNS, DNS-SD, Physical Web).
- **Données** : formats et protocoles d'échange au niveau applicatif (MQTT, CoAP, WebSocket).
- **Gestion** : supervision, configuration et mise à jour des dispositifs (TR-069, OMA-DM, LwM2M).
- **Sémantique** : description et interprétation des données pour assurer l'interopérabilité (JSON-LD, Web Thing Model).

3.2 Protocoles d'Infrastructure et d'Identification

3.2.1 Protocoles d'Infrastructure Réseau

Protocole	Objectif et Principe	Caractéristiques Techniques
IPv6	Adressage nouvelle génération pour tous les objets	128 bits (3.4×10^3 adresses), élimine le NAT, IPsec intégré
6LoWPAN	Adaptation d'IPv6 aux réseaux à faible consommation	Compression d'en-têtes pour IEEE 802.15.4, support des réseaux maillés
RPL	Routage pour réseaux à ressources limitées	Création de topologies efficaces, auto-réparation, faible consommation

TABLE 9 – Protocoles d'infrastructure réseau pour l'IoT

3.2.2 Protocoles d'Identification

Protocole	Niveau d'Utilisation	Caractéristiques et Applications
Adresse MAC	Identification matérielle	Unique gravée dans l'interface, suffisante pour prototypes et petits réseaux
IPv6	Adressage réseau	Hiérarchique mondial, auto-configuration (SLAAC), support multicast
URI (Web of Things)	Identification web	Format standardisé RFC 3986, exposition des objets comme ressources web
EPC/uCode	Identification industrielle	EPC (logistique GS1), uCode (Japon), pour infrastructures industrielles à grande échelle

TABLE 10 – Méthodes d'identification des objets IoT

Point Clé

En pratique : Les petits systèmes IoT utilisent principalement l'adresse MAC ou un identifiant logiciel interne. Les systèmes EPC/uCode sont réservés aux grandes infrastructures industrielles et logistiques nécessitant une traçabilité fine.

3.3 Protocoles de Communication et Transport

3.3.1 Réseaux Courte/Moyenne Portée

Technologie	Portée Typique	Débit	Applications Principales
Wi-Fi (IEEE 802.11)	20-50 m (intérieur)	10 Mbps - 1 Gbps	Vidéosurveillance, domotique haut débit, objets connectés alimentés
Bluetooth/BLE	Jusqu'à 100 m	1-2 Mbps (BLE : 125 kbps-2 Mbps)	Wearables, périphériques personnels, santé connectée
ZigBee (IEEE 802.15.4)	10-100 m	20-250 kbps	Domotique, automatisation bâtiment, réseaux maillés
NFC/RFID	Contact à quelques cm	106-848 kbps (NFC)	Identification, paiement, badges d'accès, inventaire

TABLE 11 – Technologies de communication courte/moyenne portée

3.3.2 Réseaux Longue Portée (LPWAN)

Les principales technologies LPWAN sont :

LoRa/LoRaWAN - Portée : 2-15 km (jusqu'à 30 km en vue directe) - Débit : 0.3-50 kbps - Caractéristiques : Basse consommation, bande ISM (868 MHz EU), topologie étoile

Sigfox - Portée : 10-40 km (rural) - Débit : 100 bps - Caractéristiques : Ultra basse consommation, réseau opérateur, messages 12 octets

NB-IoT - Portée : 1-10 km - Débit : ~250 kbps - Caractéristiques : Réseau cellulaire (bandes licenciées), bonne pénétration intérieur

LTE-M - Portée : 1-10 km - Débit : ~1 Mbps - Caractéristiques : Évolution LTE pour IoT, support mobilité, voix possible

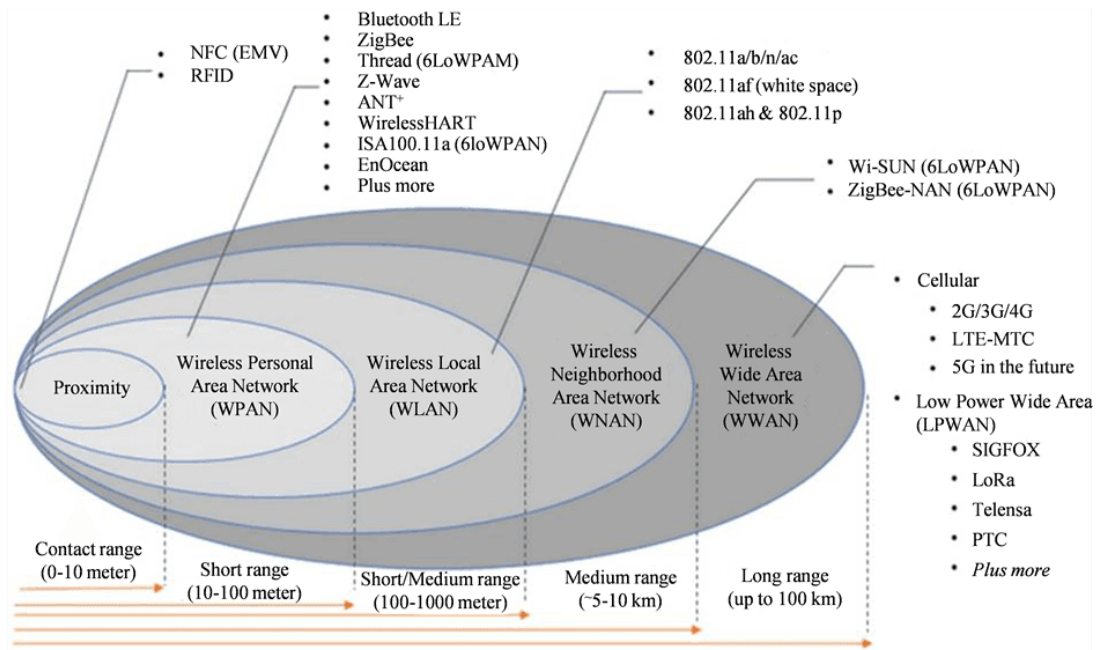


FIGURE 12 – Comparaison des technologies IoT par portée et débit

3.4 Protocoles de Découverte et de Données

3.4.1 Protocoles de Découverte de Services

Protocole	Principe de Fonctionnement	Applications Typiques
Physical Web	Accès aux objets via URL sans infrastructure centrale	Interactions utilisateur simples, affichages publics, beacons
mDNS	Résolution de noms en réseau local par multicast	Découverte automatique dans les réseaux domestiques/small office
DNS-SD	Annonce et découverte de services via DNS	Intégration avec l'infrastructure DNS existante, réseaux d'entreprise

TABLE 12 – Protocoles de découverte de services pour l'IoT

3.4.2 Protocoles d'Échange de Données

Protocole	Modèle	Caractéristiques	Cas d'Usage
MQTT	Publish/Subscribe	Léger, faible overhead, QoS multiples, idéal pour connexions intermittentes	Télémétrie, domotique, capteurs à batterie
CoAP	Requête/Réponse RESTful	Inspiré de HTTP mais optimisé pour contraintes, support UDP	Capteurs contraints, réseaux à faible débit, applications REST
WebSocket	Bidirectionnel temps réel	Communication full-duplex sur HTTP, maintien de connexion	Tableaux de bord temps réel, contrôle à distance, notifications push

TABLE 13 – Principaux protocoles d'échange de données IoT

3.5 Protocole CoAP (Constrained Application Protocol)

3.5.1 Principes Fondamentaux du CoAP

Définition

CoAP (Constrained Application Protocol) : Protocole de messagerie web conçu spécifiquement pour les nœuds et réseaux contraints (faible puissance, capacité mémoire limitée, réseaux instables). Il implémente un modèle RESTful sur UDP avec des mécanismes de fiabilité optionnels.

Architecture en Deux Sous-couches :

1. **Couche Messages** : Gestion des échanges bas niveau sur UDP avec 4 types de messages :
 - **CON** (Confirmable) : Nécessite accusé de réception.
 - **NON** (Non-confirmable) : Sans accusé.
 - **ACK** : Accusé de réception.
 - **RST** : Signal d'erreur ou d'incompréhension.
2. **Couche Requêtes/Réponses** : Implémente le modèle REST (GET, POST, PUT, DELETE).

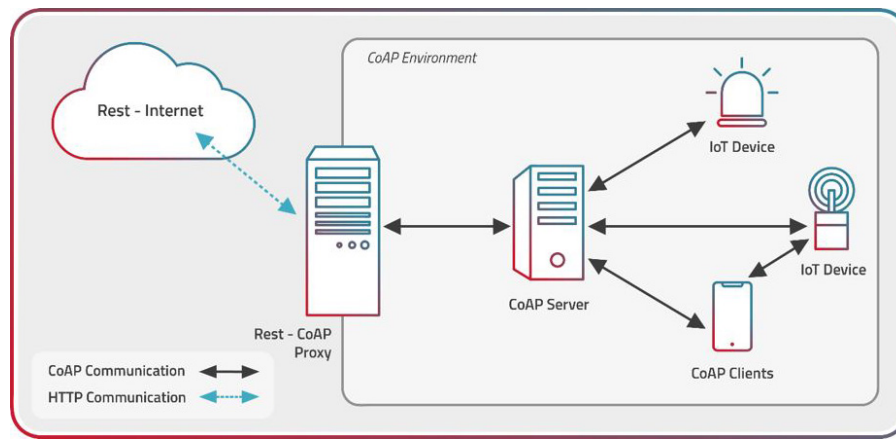


FIGURE 13 – Architecture à deux couches du protocole CoAP

3.5.2 Caractéristiques Techniques du CoAP

Caractéristique	Description et Avantages
Basé sur UDP	Réduction de l'overhead vs TCP, adapté aux réseaux à pertes
En-tête court	4 octets de base (vs 20+ pour TCP), économie bande passante
Support REST	Modèle familier aux développeurs web, intégration facile
Adressage URI	Ressources accessibles via URI (ex : 'coap://serveur/capteur/-temp')
Multicast natif	Support des communications un-à-plusieurs sur UDP
Observation (Observe)	Mécanisme de subscription pour notifications automatiques
Bloc Transfer	Transfert de données volumineuses par blocs

TABLE 14 – Caractéristiques techniques du protocole CoAP

3.5.3 Mécanisme Observe et Interopérabilité

Mécanisme Observe : Permet à un client de s'abonner aux mises à jour d'une ressource :

1. Client envoie **GET** avec option **Observe**.
2. Serveur ajoute client à la liste d'observateurs.
3. Serveur notifie automatiquement tous les observateurs lors des modifications.

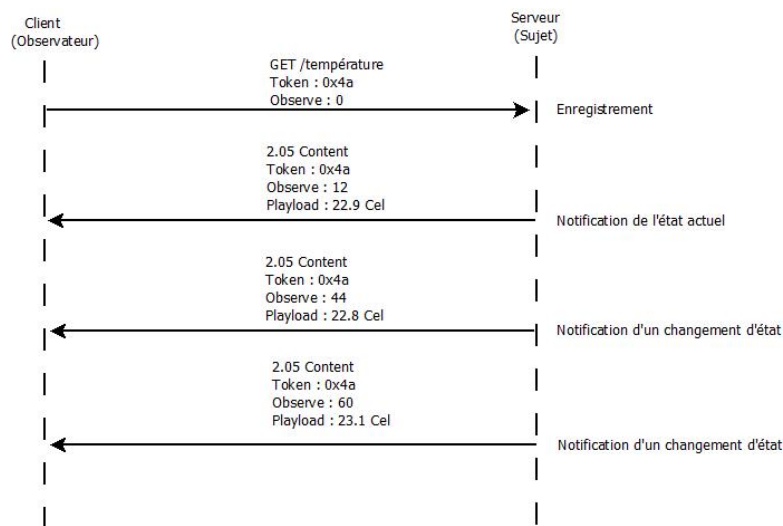


FIGURE 14 – Fonctionnement du mécanisme Observe dans CoAP

Interopérabilité CoAP-HTTP : Des proxys permettent la traduction transparente entre CoAP et HTTP, facilitant l'intégration d'objets CoAP dans des infrastructures web existantes.

Exemple Concret

Cas d'usage CoAP : Un réseau de capteurs de température dans un bâtiment intelligent. Chaque capteur expose ses données via CoAP sur une URI spécifique. Une application de supervision peut récupérer ponctuellement les valeurs (GET) ou s'abonner aux mises à jour (Observe). Un proxy CoAP-HTTP permet d'intégrer ces données dans un tableau de bord web standard.

3.6 ProtocolMQTT (Message Queuing Telemetry Transport)

3.6.1 Principes Fondamentaux du MQTT

Définition

MQTT (Message Queuing Telemetry Transport) : Protocole de messagerie léger basé sur le modèle publish/subscribe, conçu initialement par IBM en 1999 pour la télémétrie M2M dans des environnements à ressources limitées (satellite, pipelines). Standard OASIS depuis 2014.

Architecture Publish/Subscribe :

- **Publishers :** Produisent des données et les publient sur des topics.
- **Subscribers :** S'abonnent à des topics d'intérêt.
- **Broker :** Centralise et distribue les messages aux abonnés concernés.

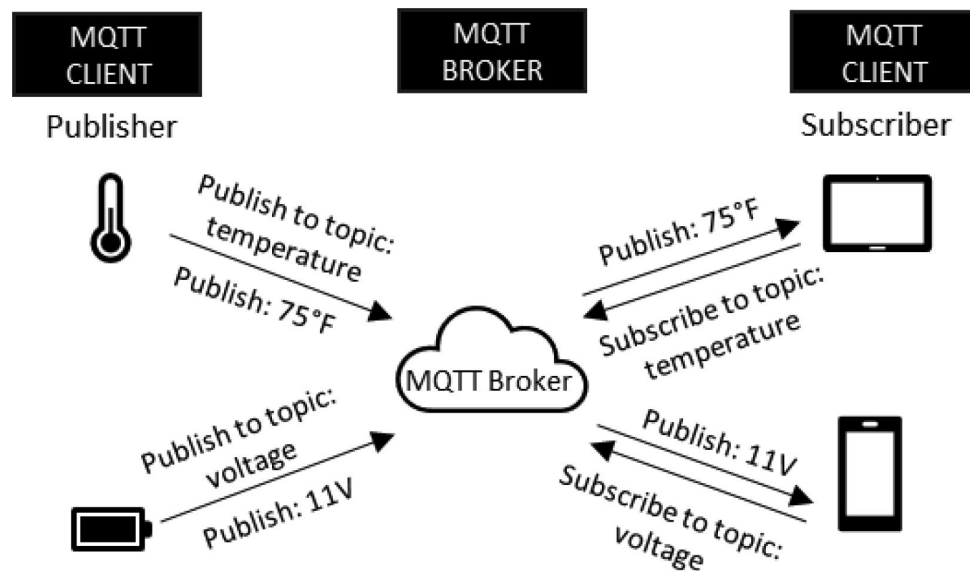


FIGURE 15 – Architecture publish/subscribe de MQTT

Découplage Spatial et Temporel :

- **Spatial** : Éditeurs et abonnés n'ont pas besoin de se connaître.
- **Temporel** : Éditeurs et abonnés n'ont pas besoin d'être connectés simultanément.

3.6.2 Composants et Connexions MQTT

Composant	Rôle et Fonctionnement
Client MQTT	Appareil utilisant une bibliothèque MQTT, peut être publier, subscriber ou les deux. Se connecte au broker via TCP/IP.
Broker MQTT	Serveur central qui reçoit, filtre et distribue tous les messages. Gère les sessions, l'authentification, la rétention des messages.
Topic	Chaîne hiérarchique (ex : 'maison/salon/temperature') identifiant le sujet du message.
Message CONNECT	Établit la connexion avec paramètres : 'clientId', 'cleanSession', 'keepAlive', 'username/password', 'lastWill'
Message CONNACK	Réponse du broker confirmant la connexion, avec 'sessionPresent' et 'returnCode'

TABLE 15 – Composants et messages de connexion MQTT

3.6.3 Topics et Filtrage MQTT

3.6.3.1 Structure des Topics

Exemples concrete, topics MQTT d'une maison connectée :

```
maison/salon/temperature
maison/salon/humidite
maison/salon/lumiere/etat
```

maison/salon/lumiere/intensite
maison/cuisine/temperature
maison/cuisine/humidite
maison/garage/portee/etat
maison/jardin/arrosage/statut

3.6.3.2 Règles Simples pour les Topics

- Pas de slash au début : `salle/temp` pas `/salle/temp`.
- Utiliser minuscules et tirets : `etage-1` pas `Étage 1`.
- Être spécifique : `batimentA/salle304/temp` pas juste `temp`.

3.6.3.3 Filtrage : Les 2 Jokers Essentiels

- **Joker Simple** : `+` (un seul niveau)

Exemple 1 : `maison/+/temperature`

Topics correspondants :

- `maison/salon/temperature`
- `maison/cuisine/temperature`

Exemple 2 : `maison/salon/+`

Topics correspondants :

- `maison/salon/temperature`
- `maison/salon/humidite`

- **Joker Multiple** : `#` (zéro ou plusieurs niveaux)

Exemple : `maison/salon/#`

Topics correspondants :

- `maison/salon/temperature`
- `maison/salon/humidite`
- `maison/salon/lumiere/etat`
- `maison/salon/lumiere/intensite`

Exemple : `maison/#`

Topics correspondants (TOUS) :

- `maison/salon/temperature`
- `maison/salon/humidite`
- `maison/salon/lumiere/etat`
- `maison/salon/lumiere/intensite`
- `maison/cuisine/temperature`
- `maison/cuisine/humidite`

- maison/garage/porte/etat
- maison/jardin/arrosage/statut

3.6.3.4 Conseils pour Bien Débuter

Commencez simple : lieu/appareil/mesure.

Testez vos filtres avec des outils comme Mosquitto.

Documentez : Listez vos principaux topics.

Pensez évolutif : Ajoutez des identifiants si besoin (capteur-id123/temp).

3.6.4 Qualité de Service (QoS) MQTT

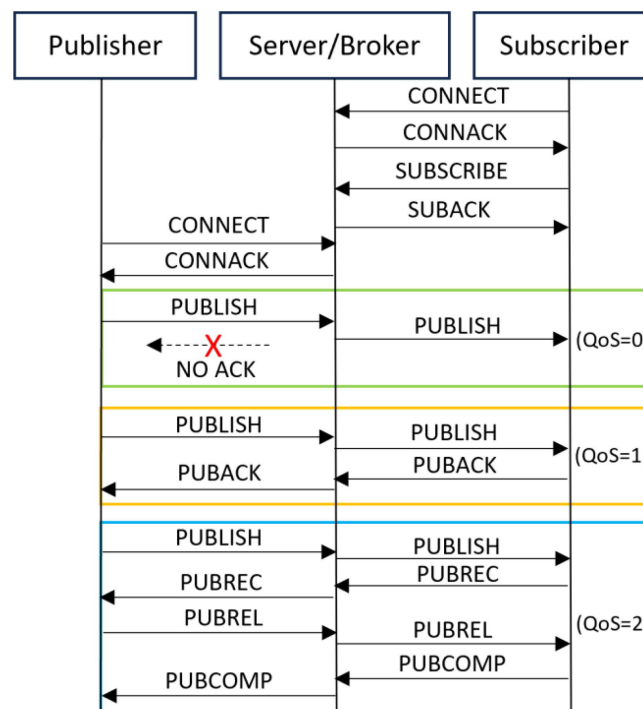


FIGURE 16 – QoS MQTT

Niveau QoS	Garantie	Échange de Messages	Utilisation Typique
QoS 0	Au plus une fois	Publisher -> Broker (pas d'ACK)	Données non critiques, publications fréquentes
QoS 1	Au moins une fois	Publisher -> Broker -> PUBACK	Données importantes, tolérance aux doublons
QoS 2	Exactement une fois	Publisher -> Broker -> PUBREC -> PUBREL -> PUBCOMP	Données critiques, tran- sactions sensibles

TABLE 16 – Niveaux de Qualité de Service (QoS) dans MQTT

3.6.5 Fonctionnalités Avancées MQTT

Session Persistante : Lorsque `cleanSession=false`, le broker conserve :

- Les abonnements du client
- Les messages QoS 1/2 non acquittés
- Permet la reprise transparente après déconnexion

Last Will and Testament (LWT) : Message programmé que le broker publie si le client se déconnecte anormalement. Utile pour :

- Détecter les pannes.
- Notifier les autres clients.
- Nettoyer les états.

Retained Messages : Dernier message conservé par le broker pour un topic. Permet aux nouveaux abonnés de recevoir immédiatement la dernière valeur connue.

Point Clé

Choisir entre CoAP et MQTT : CoAP est idéal pour les communications directes appareil-à-appareil sur UDP, avec des requêtes RESTful. MQTT excelle pour la collecte centralisée de données via un broker, particulièrement avec des connexions intermittentes. Le choix dépend de l'architecture réseau, des contraintes matérielles et du modèle d'interaction souhaité.

4 Chapitre 4 : Réseaux LPWAN et Technologie LoRa

4.1 Introduction aux Réseaux LPWAN

4.1.1 Définition et Contexte des LPWAN

Dans le monde de l'IoT, on a souvent besoin de connecter des objets qui sont très éloignés, dispersés sur un large territoire, tout en préservant leur batterie le plus longtemps possible. C'est là qu'interviennent les réseaux LPWAN (Low Power Wide Area Network).

Prenons l'exemple d'un agriculteur qui veut surveiller l'humidité du sol dans différents champs sur plusieurs hectares, ou d'une ville qui déploie des capteurs de stationnement dans tous ses quartiers. Le Wi-Fi ne suffit pas (trop courte portée), la 4G/5G consomme trop d'énergie ; Les LPWAN offrent justement cette combinaison unique : longue portée et faible consommation.

Définition

LPWAN (Low Power Wide Area Network) : Famille de technologies de communication sans fil conçues spécifiquement pour connecter des objets à très faible consommation d'énergie sur de grandes distances (plusieurs kilomètres), avec des débits modestes et des coûts réduits.

Contexte d'Émergence : Les technologies existantes (Wi-Fi, Bluetooth, cellulaires) présentaient des limitations pour certains cas d'usage IoT :

- **Trop grande consommation** pour des batteries de longue durée.

- **Portée insuffisante** pour les applications rurales ou étendues.
- **Coût trop élevé** pour les déploiements massifs.
- **Complexité excessive** pour des capteurs simples.

4.1.2 Objectifs et Compromis des LPWAN

Objectif	Solutions Techniques	Compromis Acceptés
Grande Portée	Bandes Sub-1 GHz, modulations robustes, récepteurs sensibles	Débit réduit, latence accrue
Faible Consommation	Topologie étoile, duty cycling, protocoles MAC légers (ALOHA)	Communications sporadiques, pas de streaming
Faible Coût	Matériel simple, bandes ISM libres, infrastructure minimale	Capacités limitées, partage du spectre
Évolutivité	Multi-canaux, ADR (Adaptive Data Rate), coordination serveur	Complexité déportée vers l'infrastructure

TABLE 17 – Objectifs et compromis des technologies LPWAN

4.1.3 Cas d'Usage Typiques des LPWAN

Domaine	Applications	Avantages LPWAN
Agriculture Intelligente	Humidité sol, niveau silos, surveillance bétail	Couverture zones rurales, autonomie années
Ville Intelligente	Gestion déchets, stationnement, éclairage public	Déploiement massif économique, faible maintenance
Industrie 4.0	Monitoring machines, détection fuites, température	Pénétration bâtiments, fiabilité
Logistique	Suivi conteneurs, capteurs choc/température	Couverture globale, coût unitaire faible
Environnement	Qualité air/eau, surveillance rivières, forêts	Autonomie longue durée, zones reculées

TABLE 18 – Cas d'usage typiques des technologies LPWAN

4.2 Technologie LoRa et LoRaWAN

4.2.1 Comprendre la Distinction Fondamentale : LoRa vs LoRaWAN

Définition

LoRa (Long Range) : Une technique de modulation radio propriétaire développée par Semtech, basée sur la technologie **Chirp Spread Spectrum (CSS)**. LoRa encode l'information sur des ondes radio en utilisant des impulsions "chirp"; <!-- une méthode similaire à celle utilisée par les dauphins et les chauves-souris pour communiquer!--> La transmission modulée LoRa est robuste aux perturbations et peut être reçue sur de grandes distances.

Définition

LoRaWAN (Long Range Wide Area Network) : Un protocole de couche MAC (Media Access Control) ouvert, géré par la LoRa Alliance®, qui définit l'architecture réseau, les mécanismes de communication et la sécurité. LoRaWAN est la **couche logicielle** qui spécifie comment les dispositifs utilisent la modulation LoRa.

4.2.1.1 Analogie pour Comprendre

Pensez à **LoRa** comme à la **langue** (Français, Anglais, etc.) : c'est la manière fondamentale d'encoder l'information. **LoRaWAN** est alors l'**étiquette et les règles de conversation** : qui parle à qui, quand parler, comment s'identifier, etc.

LoRa (Couche Physique - PHY)	LoRaWAN (Architecture Réseau - MAC)
Modulation propriétaire Chirp Spread Spectrum (Semtech)	Protocole MAC ouvert géré par la LoRa Alliance®
Définit comment les bits deviennent des ondes	Définit qui, quand et comment communiquer
Paramètres techniques : BW, SF, CR, fréquence	Composants réseau : End-devices, Gateways, Network/Application Servers
Peut théoriquement être utilisé avec d'autres protocoles MAC	Utilise exclusivement LoRa comme couche physique
Le "matériel" de communication	Le "logiciel" qui orchestre le réseau

TABLE 19 – Distinction fondamentale entre LoRa (PHY) et LoRaWAN (MAC/réseau)

4.2.1.2 Pourquoi LoRa est-il Innovant ?

LoRa est idéal pour les applications qui transmettent de petits paquets de données à faible débit binaire. Les données peuvent être transmises sur une portée bien plus grande comparée aux technologies comme le Wi-Fi, le Bluetooth ou le ZigBee. Ces caractéristiques rendent LoRa parfaitement adapté aux capteurs et actionneurs fonctionnant en mode basse consommation.

4.2.1.3 Bandes de Fréquence LoRa

LoRa fonctionne sur les bandes ISM (Industriel, Scientifique, Médical) libres de licence :

- Sub-GHz : 868 MHz (Europe), 915 MHz (Amérique du Nord), 433 MHz (Asie)
- 2.4 GHz : Pour des débits plus élevés, au détriment de la portée

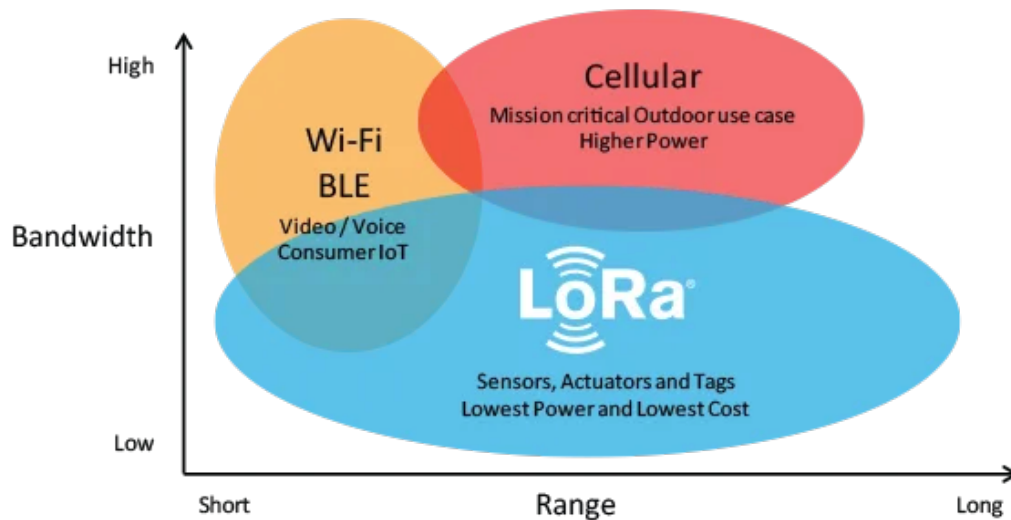


FIGURE 17 – Comparaison des technologies sans fil : portée vs bande passante. LoRaWAN excelle dans les applications longue portée à faible débit.

4.2.2 La Modulation LoRa : Chirp Spread Spectrum (CSS)

4.2.2.1 Le Principe du “Chirp”

Un **chirp** est un signal dont la fréquence varie linéairement dans le temps :

- **Up-chirp** : Fréquence qui augmente (comme le chant d’un oiseau qui monte).
- **Down-chirp** : Fréquence qui diminue.

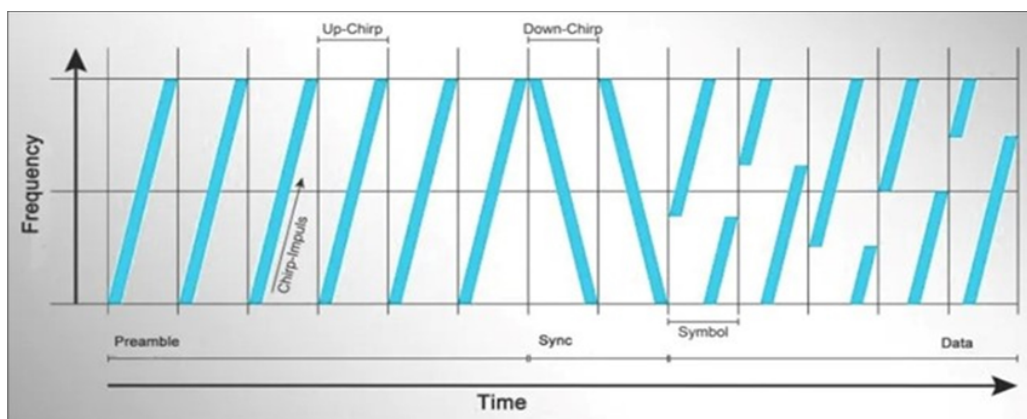


FIGURE 18 – Visualisation des chirps LoRa : montants (up) et descendants (down)

4.2.2.2 Pourquoi le CSS est-il si Efficace ?

Imaginez identifier une personne spécifique dans une foule bruyante. Avec une voix normale (modulation classique), c’est difficile. Mais si cette personne siffle une mélodie qui monte progressivement (un chirp), même dans le bruit, votre oreille peut la distinguer. C’est le principe du CSS !

Avantages Clés du CSS :

- **Détection sous le bruit** : Peut décoder des signaux sous le bruit ambiant.
- **Insensibilité à l'effet Doppler** : Idéal pour les objets mobiles (véhicules, drones).
- **Robustesse aux interférences** : Les interférences à bande étroite n'affectent qu'une petite partie du signal.
- **Précision temporelle** : Permet la localisation par triangulation (Time Difference of Arrival).

4.2.3 Pourquoi LoRaWAN est-il Exceptionnel ?

LoRaWAN combine les avantages de LoRa avec une architecture réseau intelligente :

- **Ultra basse consommation** : Les devices peuvent fonctionner 10+ ans sur une pile bouton.
- **Longue portée** : Jusqu'à 15 km en zone rurale, 3-5 km en zone urbaine.
- **Pénétration indoor** : Couvre les sous-sols et bâtiments multi-étages.
- **Spectre libre** : Pas de licence coûteuse nécessaire.
- **Géolocalisation sans GPS** : Triangulation possible si 3 gateways reçoivent le signal.
- **Sécurité de bout en bout** : Chiffrement AES-128 entre le device et l'application.
- **Mises à jour OTA** : Mise à jour du firmware à distance.
- **Roaming** : Handover transparent entre réseaux.
- **Coût réduit** : Infrastructure minimale, hardware peu cher.
- **Écosystème mature** : Large communauté et certification des devices.

4.2.4 Architecture LoRaWAN : Topologie "Star-of-Stars"

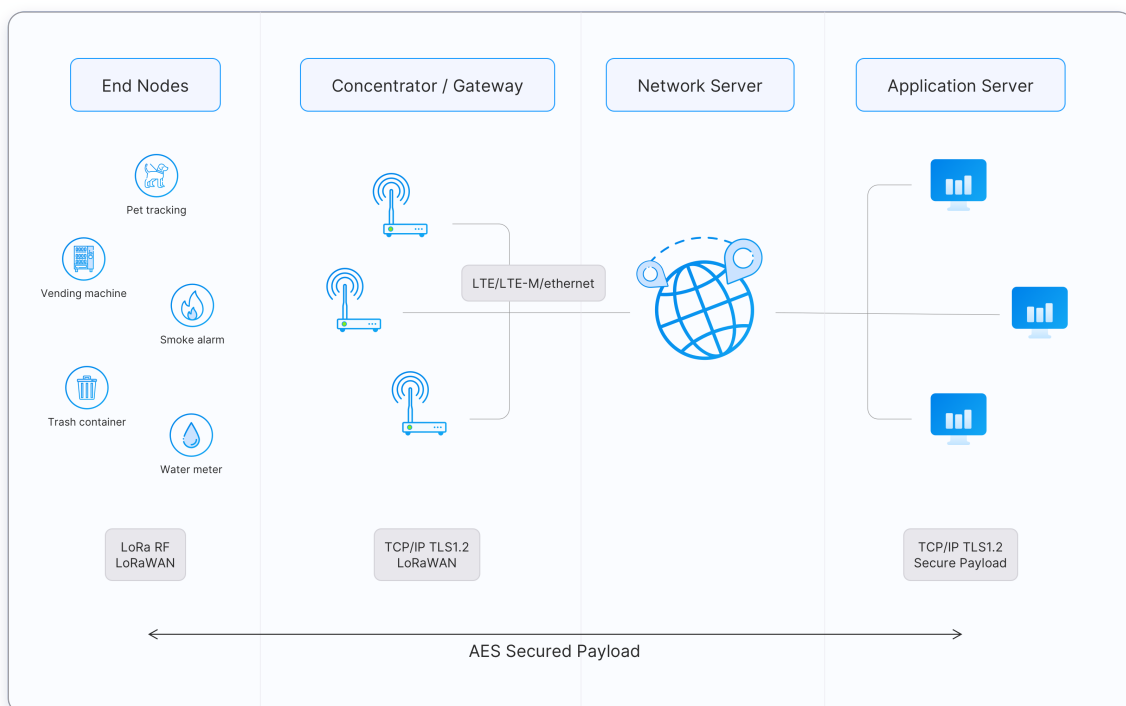


FIGURE 19 – Architecture complète d'un réseau LoRaWAN

4.2.4.1 End Devices (Dispositifs Terminaux)

Capteurs ou actionneurs équipés d'un module LoRa. Ils communiquent de manière **asynchrone** (protocole ALOHA) : ils émettent quand ils ont besoin, sans synchronisation préalable.



FIGURE 20 – Exemple de device LoRaWAN : The Things Industries Generic Node Sensor Edition

4.2.4.2 Gateways (Passerelles)

Ce sont les “oreilles” du réseau. Une gateway :

- Écoute plusieurs canaux simultanément.
- Décode différents SF en parallèle.
- Est transparente : ne traite pas les données, les forwarder simplement.



(a) Gateway indoor (The Things Indoor)



(b) Gateway outdoor (Tektelic Enterprise)

FIGURE 21 – Types de gateways LoRaWAN

Fonctionnement clé : Un même message peut être reçu par plusieurs gateways. Cette redondance améliore la fiabilité.

4.2.4.3 Network Server (Serveur Réseau)

Le **cerveau** du réseau qui :

- Déduplique les messages (garder une seule copie si plusieurs gateways ont reçu).
- Gère l'ADR (Adaptive Data Rate) : ajuste SF/BW selon les conditions radio.
- Authentifie les devices (NwkSKey).
- Route les messages vers le bon Application Server.

4.2.4.4 Application Server (Serveur d'Application)

Traite les données métier :

- Déchiffre le payload avec **AppSKey**
- Implémente la logique applicative (alertes, analyses, etc.).
- Communique souvent via **MQTT** avec les systèmes existants.

4.2.4.5 Join Server (Serveur de Jointure)

Introduit dans LoRaWAN 1.1, gère : - L'activation sécurisée des devices (OTAA) - Le stockage des clés racines - La génération des clés de session

4.2.5 Classes de Devices LoRaWAN

La spécification LoRaWAN définit trois classes de devices avec des compromis consommation/-latence différents.

Classe	Mode de Fonctionnement	Consommation	Cas d'Usage Typiques
Classe A	Uplink + 2 fenêtres RX courtes après	Très faible (batteries 10+ ans)	Capteurs environnementaux, tracking
Classe B	Classe A + fenêtres RX planifiées (ping slots)	Faible à modérée	Compteurs intelligents, éclairage public
Classe C	RX toujours ouvert (sauf pendant TX)	Élevée (alimentation secteur)	Actionneurs, alarmes, bornes fixes

TABLE 20 – Caractéristiques des trois classes de devices LoRaWAN

4.2.5.1 Classe A : “Batterie d’une Décennie”

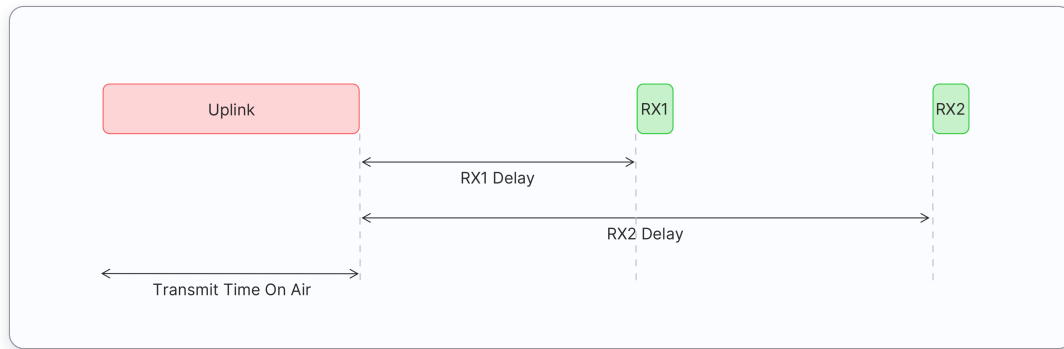


FIGURE 22 – Fenêtres de réception de la Classe A : RX1 et RX2 après chaque uplink

Principe : Après chaque émission (uplink), le device ouvre **deux fenêtres courtes de réception** (RX1, RX2). Le Network Server peut répondre dans l’une de ces fenêtres.

Avantage : Consommation minimale -> parfait pour les capteurs qui émettent rarement (ex : température toutes les 15 min).

Applications : Surveillance environnementale, agriculture intelligente, suivi d’actifs.

4.2.5.2 Classe B : “Le Juste Milieu”

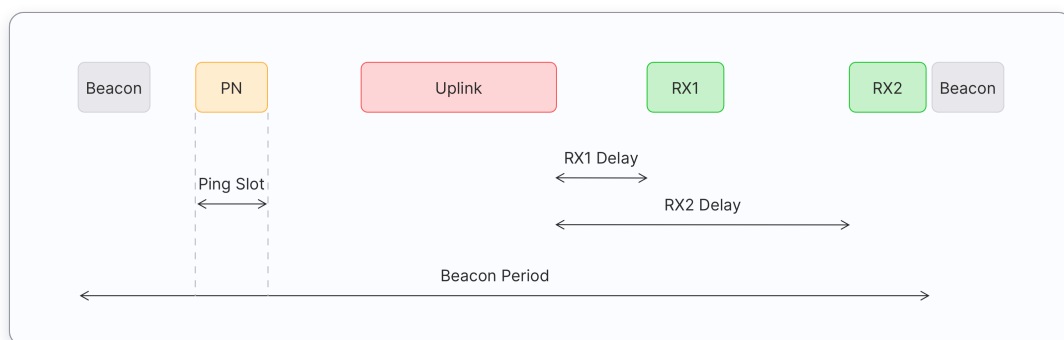


FIGURE 23 – Classe B : fenêtres RX périodiques (ping slots) synchronisées par beacon

Principe : En plus des fenêtres de Classe A, le device ouvre périodiquement des “ping slots” synchronisés par des beacons du réseau.

Avantage : Latence downlink réduite (secondes/minutes) tout en conservant une bonne autonomie.

Applications : Compteurs d’eau/électricité, contrôle d’éclairage, applications nécessitant des commandes occasionnelles.

4.2.5.3 Classe C : “Toujours à l’Écoute”

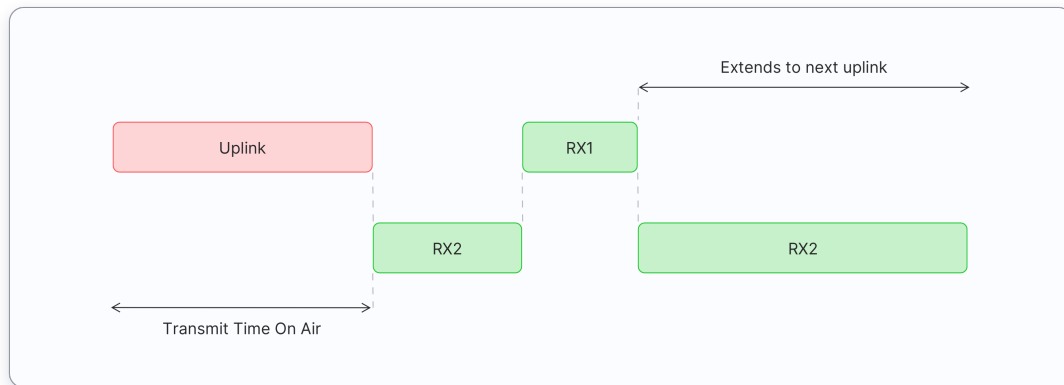


FIGURE 24 – Classe C : fenêtre RX2 toujours ouverte (sauf pendant les émissions)

Principe : Le device garde sa fenêtre de réception **toujours ouverte**, sauf quand il émet.

Avantage : Latence downlink minimale (millisecondes).

Inconvénient : Consommation élevée -> nécessite une alimentation secteur.

Applications : Actionneurs, bornes de recharge, alarmes, contrôle en temps quasi-réel.

4.2.6 Sécurité LoRaWAN

LoRaWAN implémente une sécurité double couche inspirée des meilleures pratiques IoT :

4.2.6.1 Sécurité Réseau (NwkSKey)

- **Authentification** : Vérifie que le device est autorisé sur le réseau
- **Intégrité** : Garantit que le message n’a pas été altéré
- **Confidentialité** : Optionnelle au niveau réseau

4.2.6.2 Sécurité Applicative (AppSKey)

- **Confidentialité forte** : Chiffre le payload (données utiles)
- **Isolation** : Chaque application a ses propres clés
- **Séparation** : Le Network Server ne peut pas lire les données applicatives

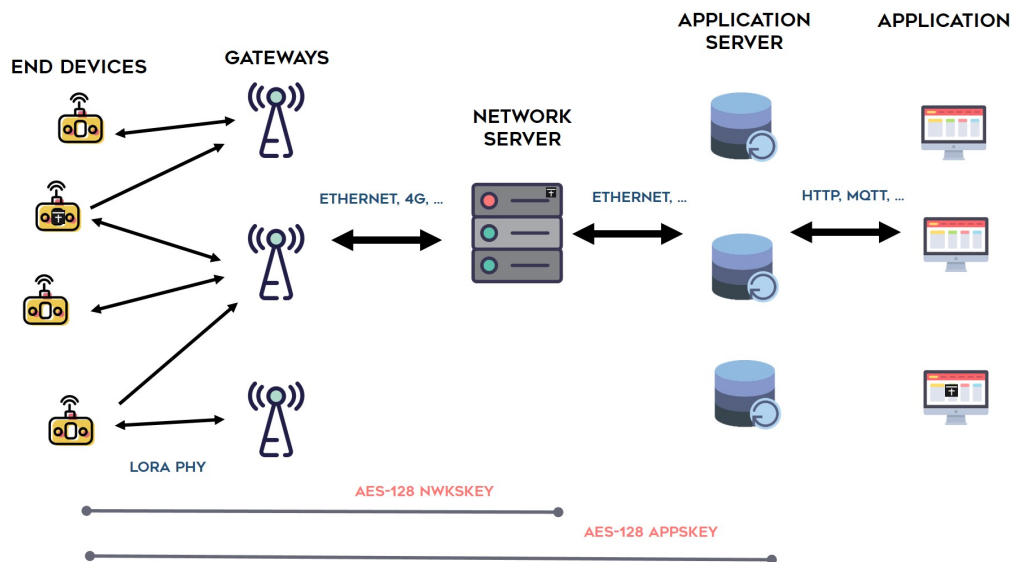


FIGURE 25 – Architecture de sécurité à deux couches de LoRaWAN

4.2.6.3 Méthodes d'Activation

OTAA (Over-The-Air Activation)	ABP (Activation By Personalization)
Recommandé pour production	Simple pour développement/test
Échange sécurisé de clés lors du "join"	Clés pré-programmées en usine
Permet rotation des clés, roaming	Pas de rotation possible
Plus sécurisé (freshness des clés)	Moins sécurisé (clés statiques)

TABLE 21 – Comparaison des méthodes d'activation LoRaWAN

4.2.7 Performances et Limitations Réelles

4.2.7.1 Portée Pratique

- **Urbain dense** : 2-5 km (bâtiments, interférences).
- **Suburbain** : 5-10 km.
- **Rural (vue directe)** : 10-15 km.
- **Records** : 30+ km (hauteur, conditions idéales).

4.2.7.2 Limitations à Maîtriser

- **Débit limité** : 300 bps (SF12) à 50 kbps (SF7, 500 kHz).
- **Taille de message** : 51-222 octets max (selon Data Rate).
- **Latence** : Secondes (Classe C) à heures (Classe A sporadique).
- **Duty cycle** : 1% max à 868 MHz EU -> 36 secondes/heure.
- **Pas de streaming** : Impossible pour audio/vidéo.

4.2.8 Écosystème et Cas d'Usage

4.2.8.1 Déploiement Flexible

- **Réseaux publics** : Opérateurs (Orange, Objenious, The Things Network)

- **Réseaux privés** : Entreprises (logistique, industrie, campus)
- **Réseaux communautaires** : The Things Network (mondial, gratuit)

4.2.8.2 Cas d'Usage Innovants

- **Santé** : Surveillance patients, chaîne du froid vaccins.
- **Environnement** : Qualité air/eau, feux de forêt.
- **Agriculture** : Irrigation intelligente, santé bétail.
- **Ville intelligente** : Stationnement, éclairage, déchets.
- **Industrie 4.0** : Monitoring machines, détection fuites.
- **Logistique** : Suivi conteneurs, chaîne logistique.
- **Espace** : Satellites LoRa pour couverture globale.

Exemple Concret

Exemple concret : Vignoble intelligent

Un vignoble de 50 hectares déploie 100 capteurs LoRaWAN (température, humidité sol, maturité raisin). Chaque capteur (Classe A, OTAA) envoie une mesure toutes les 15 minutes. Une seule gateway sur le château couvre l'ensemble du domaine (3 km). Les données remontent vers The Things Stack, qui les redirige vers une application d'aide à la décision via MQTT. Les batteries (2xAA) durent 3+ années. Résultat : optimisation de l'irrigation (économie eau 30%), récolte optimale, réduction des traitements phytosanitaires.

4.2.8.3 Matériel et Outils

- **Modules** : Semtech SX1276/8, HopeRF, Microchip.
- **Cartes dev** : Arduino MKR WAN, TTGO LoRa32, Adafruit Feather.
- **Gateways** : Multi-tech, Kerlink, RAK, DIY Raspberry Pi.
- **Serveurs** : The Things Stack, ChirpStack, AWS IoT Core.
- **Outils** : LoRaSim (simulation), SDR (analyse), TTN Mapper (couverture).

4.2.9 Conclusion sur LoRa/LoRaWAN

LoRaWAN représente un compromis optimal pour l'IoT longue portée : il sacrifie débit et latence pour maximiser portée et autonomie. Sa force réside dans sa simplicité d'utilisation (ALOHA, pas de pairing) couplée à une intelligence centralisée (Network Server).

Quand choisir LoRaWAN ?

- Données petites et peu fréquentes.
- Autonomie batterie critique (années).
- Couverture étendue nécessaire.
- Coût de déploiement limité.
- Pas de besoin temps réel strict.

Quand éviter LoRaWAN ?

- Streaming audio/vidéo.
- Contrôle temps réel (robotique).
- Transferts de fichiers.
- Applications haut débit.

Point Clé

Le futur de LoRaWAN : L'évolution vers LoRaWAN 2.4 GHz (débit augmenté), l'intégration avec la 5G (hybridation réseaux), et le déploiement de constellations satellites (couverture globale) continuent d'élargir le champ des possibles pour cette technologie clé de l'IoT.

References

- [1] O. Ayadi, « Analyse et étude de la sécurité des données médicales dans l'Internet des objets à partir d'une approche technologique Blockchain », thèse de doctorat, PhD thesis, Université de Constantine 2, 2019.
- [2] M. J. McGrath et C. N. Scanail, « Sensing and sensor fundamentals », in *Sensor technologies : Healthcare, wellness, and environmental applications*, Springer, 2014, p. 15-50.
- [3] « Arduino Tutorial ». https://jmarsico.github.io/rsma2019/tutorials/td_arduino/.
- [4] Y. Bello et E. Figetakis, « Iot-based wearables : A comprehensive survey », *arXiv preprint arXiv:2304.09861*, 2023.
- [5] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, et A. S. Uluagac, « A survey on sensor-based threats to internet-of-things (iot) devices and applications », *arXiv preprint arXiv:1802.02041*, 2018.
- [6] N. Saha, P. Paul, K. Ji, et R. Harik, « Performance evaluation framework of MQTT client libraries for IoT applications in manufacturing », *Manufacturing Letters*, vol. 41, p. 1237-1245, 2024.
- [7] J. Shuda, A. Rix, et M. Booysen, « Module-Level Monitoring Of Solar PV Plants Using Wireless Sensor Networks », in *Proceedings of the 26th Southern African Universities Power and Engineering Conference (SAUPEC 2018)*, Johannesburg, South Africa, 2018, p. 24-26.
- [8] S. Cirani, G. Ferrari, M. Picone, et L. Veltri, *Internet of things : architectures, protocols and standards*. John Wiley & Sons, 2018.