Concepts fondamentaux de l'Internet des objets

1.1 Introduction

Dans ce chapitre, nous présentons l'IoT (Internet of things) définition, ses composantes, ses domaines d'application, son architecture, son fonctionnement, ainsi que ses axes de recherche, et nous consacrons par la suite le reste du chapitre à la définition de quelques notions utilisées dans le domaine de la sécurité.

1.2 Internet Of Thing (IOT)

1.2.1 Définition

L'IOT est l'acronyme de Internet Of Thing (Internet des Objets en français). Le terme IoT est apparu la première fois en 1999 dans un discours de l'ingénieur britannique **Kevin ASHTON**. Il servait à désigner un système où les objets physiques sont connectés à internet. Il s'agit également de systèmes capables de créer et transmettre des données afin de créer de la valeur pour ses utilisateurs à travers divers services (agrégation, analytique, etc).

Selon l'**UIT** (Union Internationale des Télécommunications), l'Internet des Objets est défini comme (une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physique ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution). Au fil du temps, le terme a évolué et il englobe maintenant tout l'écosystème des objets connectés. Cet écosystème englobe, des fabricants de capteurs, des éditeurs de logiciels, des opérateurs historiques ou nouveaux sur le marché, des intégrateurs, etc. Cet éclectisme en fait sa richesse.

Inspére de [4], la figure (**Figure 1.1**) montre l'architecture passée, présente et future de l'IOT. À l'avenir, les appareils ne devraient pas seulement être connectés à Internet et à

d'autres appareils locaux, mais devraient également communiquer directement avec d'autres appareils sur Internet. Outre les appareils ou les objets connectés, le concept d'IOT social (SIoT[1]) émerge également.

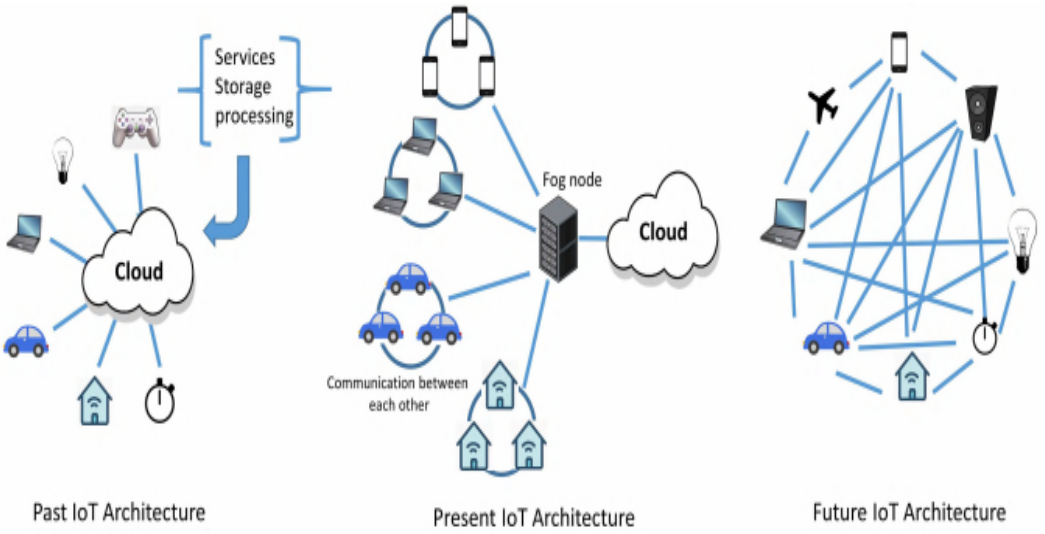

Figure 1.1: Architecture actuelle et future de l'IoT.[4]

1.2.2 Composantes de l'IOT

Les composant iot est cinq. L'objet connecté est d'abord un objet qui a une fonction mécanique et/ou électrique propre, il peut soit être conçu directement connectable, soit il est déjà existant et la connectivité est rajoutée à postériori. L'objet connecté a pour fonction de collecter des données de capteurs, de traiter ces données et de les communiquer à l'aide de d'une fonction de connectivité et de recevoir des instructions pour exécuter une action. Généralement ces fonctions de l'objet connecté nécessitent une source d'énergie, surtout quand les données sont prétraitées directement dans l'objet[5].

1.2.2.1 Les capteurs

Les capteurs sont des dispositifs permettant de transformer une grandeur physique observée (température, luminosité, mouvement etc) en une grandeur digitale utilisable par des logiciels. Il existe une très grande variété de capteurs de tous types, les objets connectés ont souvent la fonction de captation de ces grandeurs physiques sur leurs lieux d'utilisation.

Exemple de capteurs: lumière, présence, proximité, position, déplacement, accélération, rotation, température, humidité, son, vibration, électrique, magnétique, chimique, gaz, flux, force, pression, niveau[5].

[1]SIoT permettra à différents utilisateurs de réseaux sociaux d'être connectés aux appareils et les utilisateurs pourront partager les appareils sur Internet [4].

1.2.2.2 Les réseaux de capteurs

Afin de satisfaire les besoins de communication entre eux, les capteurs sont équi- pés de dispositifs sans fil pour l'émission et la réception de données. Cela ne sufit cependant pas å rendre un ensemble de capteurs accessibles ou du moins de m anière inter-opérable, transparente et simplifiée Pour cela, les capteurs doivent aussi s'organiser Ce qui c aractérise un réseau de capteurs, c'est que ses éléments sont de très petits appareils, dotés de capacités de transmission sans fil[6].

1.2.2.3 L'énerie

La plus import ante contrainte à laquelle sont soumis les rése aux capteurs concernant l'énergie. L'autonomie temporelle des noeuds s'évalue en termes d'années[12].

1.2.2.4 Les actionneurs

Les actionneurs sont des dispositifs qui transforment une donnée digitale en phénomène physique pour créer une action, ils sont en quelque sorte l'inverse du capteur. Exemple d'actionneurs: Afficheurs, Alarmes, Caméras, Haut-parleurs, Interrupteurs, Lampes, Moteurs, Pompes, Serrures, Vannes, Ventilateur, Vérins[5].

1.2.2.5 La connectivité

La connectivité de l'objet est assurée par une petite antenne Radio Fréquence qui va permettre la communication de l'objet vers un ou plusieurs réseaux (qui sont détaillés dans la section *réseaux IOT*). Les objets pourront d'une part remonter des informations telles que leur identité, leur état, une alerte ou les données de capteurs, et d'autre part recevoir des informations telles que des commandes d'action et des données. Le module de connectivité permet aussi de gérer le *cycle de vie de l'objet*, c'est-à-dire, l'authentification et l'enregistrement dans le réseau, la mise en service, la mise à jour et la suppression de l'objet du réseau[5].

1.3 Domaines d'application de l'Internet des objets

On n'en entendait à peine parler il y a quelques années, et ils sont maintenant partout. Les objets connectés ont envahi notre quotidien sans même que nous y prêtions attention.
De la télé intelligente à la voiture connectée, nos loisirs, nos déplacements sont facilités par ces nouveaux outils qui augmentent grandement notre confort.
Le potentiel des objets connectés est énorme. Une étude de 2016 du cabinet **Gartner** prévoit qu'en 2020, plus de la moitié des outils et processus métiers feront appels à l'Internet des Objets. Les applications sont variées et recouvrent de nombreux domaines: industrie, sciences, santé,...

Figure 1.2: Domains d'application de l'IOT[7].

L'utilisation de l'IOT permettra le développement de plusieurs applications intelligentes qui toucheront essentiellement ceux qu'on citera dans ce qui suit, nous citrons brièvement des exemples d'applications de l'IOT:

1.3.1 La domotique

La domotique regroupe l'ensemble des technologies informatique, électrotechnique et électronique, qui permettant l'automatisation des équipements d'un habitat et transforment une maison en une mais intelligente. C'est l'ensemble des techniques visant à intégrer à l'habitant tous les automatismes en matière de sécurité (comme les alarmes), de gestion de l'énergie (optimisation de l'éclairage et du chauffage etc.), de communication (contacts et discussion avec des personnes extérieures), etc[7].

1.3.2 Automobile

Avec le nombre croissant de véhicules intelligents, presque tous les véhicules vendus aujourd'hui dans le monde contiennent des capteurs et des moyens de communication pour faire face aux embouteillages, à la sécurité et au trafic[7].

L'objectif est que le véhicule puisse communiquer de manière autonome avec d'autres véhicules ou une station de surveillance pour éviter les accidents, réduire le trafic et sauver des vies[7].

Par exemple: si la voiture a un accident, elle demande automatiquement de l'aide et explique son emplacement et sa capacité à communiquer avec les utilisateurs[7].

Aujourd'hui, Les constructeurs automobiles travaillent sur des projets de véhicules autonomes (sans conducteur) capables de se déplacer d'un point A à un point B sans aucune intervention humaine[7].

1.3.3 La sante

Le secteur de la santé a connu un très grand nombre d'applications permettant à un patient et à son docteur de recevoir des informations, parfois même en temps réels, qu'il aurait été impossible de connaître avant l'apparition d'IoT[7].

Par exemple, il existe un médicament qu'il s'appelle **Porteuse Digital Health** qui est le premier médicament connecté sur le marché grâce à un capteur directement intégré dans l'être humain qui permet après ça le suivi des patients à distance[7].

Aussi, Il existe Plusieurs autres dispositifs sont disponibles, fixé autour du poignet et permettent également de suivre l'activité physique quotidienne du patient, mesurer le taux de sucre, compter le nombre de pas et les kms parcourus, le nombre de calories brûlées, le dispositif lui envoie une alerte dans les cas anormaux[7].

1.3.4 L'agriculture

L'agriculture intelligente a pour objet de renforcer la capacité des systèmes agricoles, de contribuer à la sécurité alimentaire en intégrant le besoin d'adaptation et le potentiel d'atténuation dans les stratégies de développement de l'agriculture durable[7].

Cet objectif a été atteint enfin par l'utilisation des nouvelles technologies, telles que l'imagerie satellitaire et l'informatique, les systèmes de positionnement par satellite de comme GPS, aussi par l'utilisation des capteurs qui vont s'occuper de récolter les informations utiles sur l'état du sol, taux d'humidité, taux des sels minéraux, etc. Et envoyer ces informations au fermier pour prendre les mesures nécessaires garantissant la bonne production[7].

1.3.5 Les villes intelligentes

Les villes intelligentes ou smart city sont en croissance dans les pays qui connaissent une avancée technologique. Il existe dans ce cas, des systèmes qui permettent de contrôler le fonctionnement de ville, les activités des populations, la gestion des bâtiments, la sécurité. Pour la sécurité, l'internet des objets permet d'effectuer la gestion du trafic dans les lieux de grande affluence, le suivi des caméras de télésurveillance publiques, l'éclairage connecté. Les enjeux d'une ville connectés sont entre autres, l'optimisation des ressources économiques, la gestion de la population et l'assainissement de la ville[8].

1.3.6 L'industrie

Le déploiement de l'IoT dans l'industrie sera certainement un support pour le développement de l'économie et du secteur des services, puisque. L'IOT il permettra d'assurer un suivi total des produits, de la production à la distribution, par la gestion automatisée, la surveillance

à distance, et le renforcement de la comptabilité. Ce travaille compte de développer les techniques de production en entreprises ainsi que le renforcement des capacités de gestion[8].

Donc La technologie IOT permet aux usines d'améliorer l'efficacité de ses opérations, d'optimiser la production et en plus améliorer la sécurité des employés[8].

1.3.7 IOT dans le domaine du sport

De nombreux objets connectés comme des montres ou des bracelets connectés vous permettrons pendant la journée de calculer le nombre de pas effectuée, la distance par courue, votre temps d'activités, les calories brulées, ainsi pendant la nuit en calculant vos heurs de sommeil. Pour les passionnés de High-tech, c'est un grand marché qui s'ouvre à eux! De la montre connectée au téléviseur connecté en passant par les appareils photos, les montre, les drones, les lunettes (Google glass)[26].

1.3.8 IOT dans le domaine de la sécurité

Pour le cabinet en stratégie, ces entreprises vont rapidement se positionner comme des alliés des personnes qui résident dans leur domicile. En fournissant des données relatives à la consommation d'énergie aux foyers, ces groupes vont apparaitre comme des arguments contre le facteur EDF pour les fournisseurs d'énergie la précision sera difficile à tenir car ils seront probablement contraints d'accompagner leurs clients dans une baisse de leurs facteurs énergétique[27].

1.4 Les étapes pour la mise en place de l'IOT

Pour simplifier le cadrage d'un projet IoT, nous avons modélisé en 6 étapes incontournables la construction déun objet connecté. Avec une solution IOT simple et pratique, facilement utilisable, pour aider tous les entrepreneurs souhaitant se lancer dans le monde de l'Internet des objets[29]:

1.4.1 Elément central du projet IoT

l'objet Boitier inséré dans un véhicule pour surveiller les déplacements, capteur permettant de mesurer les éléments de température ou de pression d'un équipement industriel, ou encore pour gérer des matériels médicaux dans les hopitaux (maintenance, taux d'utilisation), l'objet connecté peut être représentatif d'éléments extrémement différents et diversifiés. La première étape est donc d'acquérir, ou de construire le cas échéant, l'objet adapté aux contraintes physiques du cas d'usage de l'entreprise.

1.4.2 Connectivité pour la communication des objets connectés

Une fois cette problématique de l'objet traitée, l'objectif est de le rendre communiquant. Si l'objet capte les données, elles n'ont aucun sens si elles ne sont pas transférées. Un ensemble de solutions de connectivité existe pour faire 'parler' l'objet. En fonction de la nature de l'objet et des données qu'il capte, il faudra choisir le bon réseau: 2G/3G/4G, réseaux bas débit et basse consommation (type Sigfox, NB-IoT).

1.4.3 Collecte de l'ensemble des données

Face à la multitude des objets, la collecte et la modélisation de l'ensemble des données produites est un point crucial. Pour les traiter, toutes les données doivent etre collectées et traitées afin d'étre exploitable et ce à travers un seul outil simple et ergonomique.

1.4.4 Hébergement et le stockage des données

Les données doivent étre stockées, gérées et administrées en toute sécurité. Face à la criticité des données (exemple données de santé ou de géolocalisation), il est important de bénéficier d'une infrastructure qui garantit la sécurité des données et qui soit en mesure de s'adapter à la montée en charge du projet.

1.4.5 Développement de logiques applicatives

Pour donner un sens aux données collectées et en dégager toute la valeur (optimisation de l'activité de l'entreprise, fidélisation de ses clients ou encore proposition de nouveaux services innovants), il faut pouvoir les utiliser et les lier entre elles. Cela se traduit par le développement et la mise en oeuvre d'une application IoT. Au travers d'une telle application, l'entreprise peut utiliser au mieux ces données et piloter les objets ou les processus.

1.4.6 Restitution des données captées par les objets connectés

Pour proposer ces nouveaux services innovants à ses clients, l'entreprise doit mettre une interface à leur disposition pour interagir avec eux. Cette application IoT, proposée sous forme d'interface web, d'application mobile permet de partager les données avec ses clients ou ses fournisseurs, en toute simplicité et d'améliorer l'expérience client par exemple.

1.5 Architecture de l'Internet des objets

Le développement rapide l'IdO, il devenait nécessaire architecture de référence qui permettrait d'un iformiser la conception des systèmes et favoriserait l'interopérabilité? et la communication entre les différents écosystèmes de l'IdO[28].

1.5.1 Architecture et Standardisation

Les racines de l'IdO remontent aux technologies M2M (machine à machine) pour le contrôle des processus à distance. L'IdO qui est aujourd'hui un mélange de plusieurs technologies telles que la RFID, NFC, les capteurs et actionneurs sans fil, le M2M, l'ultrage bande ou 3/4G, IPv6, 6lowPAN, et RPL nécessite la définition d'une architecture et des standards afin de faciliter son développement dans le futur. L'ETSI propose une architecture découpée en trois domaines distincts, le domaine du réseau d'objets, le domaine du réseau coeur d'accès et le domaine des applications M2M et applications clientes[9].

1.5.2 Le domaine du réseau d'objets

Dans ce domaine nous trouvons les différentes technologies d'interconnexion des objets M2M, RFID, Bluetooth, IETF6L low PAN, IETFRPL et des passerelles vers les réseaux coeur de transport[10].

1.5.3 Le domain du réseau cœur

Dans ce domaine nous trouverons les différentes technologies de réseaux de transport et d'accès comme xDSL, WIMAX, WLAN, 3/4G, etc[11].

1.5.4 Le domaine des applications M2M et applications clientes

Ce domaine est composé de plateformes M2M, les Middlewares et API des applications M2M, processus métiers exploitant l'IDO, etc[11].

1.6 Notions de base de la sécurité

On peut définir la sécurité informatique comme étant le fait d'assurer le bon fonctionnement d'un système et de garantir les résultats attendus de sa conception. Autrement dit, la sécurité représente l'ensemble de politiques et pratiques adoptées pour prévenir et surveiller l'accès non autorisé, l'utilisation abusive, la modification ou le refus d'une opération informatique. A partir de cette définition, on peut extraire les bases de la sécurité qui sont décrites dans ce qui suit[27]:

1. **Authentification:** l'authentification est le mécanisme de sécurité qui permet de prouver l'identité d'une entité. En effet, il existe plusieurs méthodes d'authentification qu'on peut classer en quatre catégories[27].

   L'authentification avec ce qu'on sait, c'est à dire que l'entité prouve son identité avec une information secrète, qui n'est connue que par un nombre limité d'objets légitimes. Généralement le nombre d'objets concernés ne dépasse pas deux (ex. un client et un

serveur). Les mécanismes les plus utilisés dans cette catégorie sont les mots de passe et les numéros personnels d'identité (Personal Identity Number (PIN))[27].

- ✔ Authentification avec ce qu'on possède. Dans cette catégorie, une entité s'authentifier grâce à une donnée stockée. Cette donnée peut être secrète comme les clé pré-partagé (Pre-Shared Key (PSK)), ou publique comme les certificats numériques et les jetons[27].

- ✔ L'authentification avec ce qu'on est. Ça concerne généralement les utilisateurs humains, qui ont des caractéristiques biométriques qui leurs sont uniques telle que la voix, l'empreinte digitale, l'iris, et les veines[27].

- ✔ Authentification avec comment on se comporte. Cette dernière catégorie est basée sur les profiles comportementaux de chaque utilisateurs. Chaque entité à une façon de travaille particulière, par exemple, sa façon de taper sur un clavier, les horaires de travail habituels, l'environnement de travail habituel, etc[27].

❷ **Confidentialité:** la confidentialité est le mécanisme qui permet de cacher une donnée, et de cacher même l'information de son existence. Ainsi, empêcher toutes entité(s) non autorisée(s) d'avoir accès à cette donnée. Généralement, on assure ce service en utilisant le chiffrement de données. Ce dernier est basé sur des algorithmes mathématiques permettant de déformer un texte en clair est le remettre à sa forme initiale grâce au à une ou plusieurs clés cryptographiques[27].

❸ **Intégrité:** l'intégrité est un mécanisme assurant qu'une donnée ne soit pas: falsifiée, modifiée, altérée ou supprimée par une entité non autorisée. Dans la plupart des cas, ce service est réalisé en utilisant des fonctions de hachages avec des propriétés de signature de données[27].

❹ **Disponibilité:** la disponibilité est le mécanisme qui permet de garantir la bonne exécution d'un service, et le bon fonctionnement du système. Afin de garantir la disponibilité d'un service, on utilise des mécanismes qui le protègent contre les arrêts intentionnels telles que les attaques de dénies de service et dénies de service distribués (Denial/Distributed Denial of service(Dos/DDos)), et non intentionnels (ex. les erreurs humaines). En outre, on duplique et distribue ce service sur plusieurs serveurs. De cette façon, si l'un des serveurs ne fonctionne plus, les autres maintiennent le service[27].

❺ **Non répudiation:** la non répudiation est un mécanisme permettant de garantir qu'une opération ne peut être niée par celui qui l'avait établis. On garantie ce service grâce

aux signatures numériques combinées avec desmécanismes qui assurent le non rejeu de données[27].

❻ **Non rejeu:** le non rejeu est un mécanisme garantissant qu'un message échangé entre deux entités A et B, ne doit pas être réutilisé par une entité non autorisée C. La plus part des systèmes intègrent des compteurs et des numéros de séquence différents au niveau des messages échangés, ce qui fait qu'un message ne peut pas avoir le même numéro de séquence que ses n messages précédents (n un nombre de message qui varie selon la politique de sécurité utilisée), sinon il sera automatiquement rejeté[27].

❼ **Résilience:** on peut définir la résilience par la capacité d'un système à surmonter une altération de son environnement. Par exemple dans le cas de l'IoT, si un objet est compromis, cela ne devrait pas influencer l'ensemble du réseau.
La confidentialité persistante (forward secrecy) La confidentialité persistante est une caractéristique cryptographique qui garantit que la découverte d'une information secrète (ex. clé privée) d'un objet légitime par un utilisateur malicieux ne compromet pas la confidentialité des communications passées[27].

❽ **Èvolutivité:** l'évolutivité représente l'aptitude d'un système à maintenir des bonnes performances lorsque des ressources (notamment ressources matérielles) lui sont ajoutées[27].

❾ **Tolérance aux fautes:** la tolérance aux fautes est un mécanisme permettant à un système de continuer à fonctionner lorsque l'un de ses composants tombe en panne (ex. en dupliquant les serveurs)[27].

L'objectif de la sécurité est de protéger les systèmes informatiques contre les différentes menaces et attaques qui les ciblent. Ces attaquent consistent en l'exploitation d'une faille au niveau d'un système afin d'atteindre un objectif précis. Ces objectifs peuvent être l'obtention illégale d'un accès au système, le vol des données confidentielles d'une entreprise, l'obtention des informations personnelles sur un utilisateur, récupérer des codes de carte bancaires, etc. Ces attaques peuvent également avoir comme objectif l'interruption ou la perturbation d'un service, la falsification des données, ou l'exploitation des ressources du système[27].

❿ **Catégories d'attaques:**

- Attaques d'usurpation d'identité (spoofing attack): c'est lorsqu'une entité malveillante réussit à se faire passer pour une autre, obtenant ainsi les droits d'accès et les avantages de la victime[30].
- Attaques de rejeu: c'est quand un utilisateur malicieux copie et renvoie un ou plusieurs message(s) déjà transmis afin d'exploiter les vulnérabilités du système[30].
- Attaques par force brute: en effet le principe de ces attaques consiste à tester un grand nombre de mots de passe dans l'espoir de deviner le bon. Il peut également s'agir d'une opération de déchiffrement de données où l'attaquant essaie toutes les clés possibles jusqu'à ce que la clé correcte soit trouvée (recherche de clé exhaustive)[30].
- Attaques par cryptanalyse: cette catégorie concerne l'étude du flux de chiffrement (cipher), du texte chiffré, ou des crypto-systèmes, afin de trouver des vulnérabilités qui permettent de récupérer le texte en clair à partir du texte chiffré[30].
- Attaques de l'homme au milieu (Man In The Middle (MITM)): c'est lorsqu'une entité non autorisée se met entre deux ou plusieurs entités communicantes afin d'écouter une communication confidentielle, ou modifier/supprimer des données échangées, voire interrompre le trafic (dénie de service)[30].
- Attaques par dénie de service / dénie de service distribué (Dos/DDos) elle vise à rendre une ressource ou une information indisponible. Elle peut être réalisée (1) en inondant la machine source ou le réseau par un grand nombre de messages (ex. attaque d'inondation), ou (2) en exploitant une vulnérabilité dans le protocole. Comparé aux objets utilisés dans l'Internet classique qui représentent majoritairement Des ordinateurs- les objets dans l'IoT représentent tout équipement électronique Ayant une capacité de calcul et de mémorisation, qu'il s'agisse d'un capteur très limité en Performances et en consommation d'énergie, ou d'un grand data-center alimenté, avec des capacités ultra-puissantes. À cause de cette diversité d'objets, il est difficile de concevoir un protocole de sécurité robuste et au même temps adapté à ces objets variés. En plus, le faite que la tendance dans l'IoT est d'utiliser les technologies de communication sans fil rend le système IoT encore plus vulnérable et plus exposé à toute sorte de cyberattaque[30].

Afin de sécuriser les systèmes IoT, et d'assurer les propriétés vu ci-dessus. Il faut concevoir un protocole basé sur des algorithmes robustes, mais aux même temps légers et flexibles. Ce protocole doit être adapté aux différents types d'objet, du plus puissant au plus faible, sans qu'il y aie une dégradation en terme de performance sécuritaire.

1.7 Travaux connexes sur la sécurité IoT

Année	Auteurs	contributions
2016	Arslan Mosenia. al	Une brève discussion de la vulnérabilité rencontrée par la couche côté bord de l'IOT.
2017	YU Wei .al	Survey sur l'utilisation de l'informatique de périphérie pour sécuriser l'IOT.
2017	Jei Lin .al	Discussion sur la relation entre l'IOT et le calcul du brouillard (fog computing).
2017	Y Yang .al	Une brève discussion sur les limitations les plus pertinentes des dispositifs IOT.
2017	L chen, S, Thombre .al	Problèmes de sécurité spécifiques aux services basés sur la localisation dans l'IOT.
2017	A H Ngu, V.Metsis .al	Problèmes de sécurité liés au middleware IOT.
2018	I Farris, T Taleb .al	Mécanisme de sécurité pour la sécurité IOT comme SDN et NFB.
2019	Ikram Ud din, M. Guizani .al	Technique de gestion de la confiance pour l'Internet des objets.

Table 1.1: Travaux connexes sur la sécurité IoT[4]

1.8 Conclusion

Dans ce chapitre nous avons exposé l'Internet des objets (IOT) d'une manière générale, ces différents composantes, on s'est focalisé sur ses concepts de base, ses applications, et ses caractéristiques.
Bien que le IOT a permis le développement de nouveaux usages qui sont de plus en plus appréciés par les utilisateurs, mais malheureusement beaucoup de problèmes restent à résoudre. La sécurité et la protection des données privées des objets connectés soulèvent cependant plusieurs problèmes qui peuvent constituer des obstacles sérieux au déploiement ou à l'acceptation de l'IoT.

Après avoir présenté l'architecture IOT et les travaux connexes sur la sécurité IoT , une étude sur la confidentialité dans cet environnement IOT sera faite dans le prochain chapitre.

Chapitre 2

Technologies de communication de l'IOT et leurs mécanismes de sécurité

2.1 Introduction

L'IoT (Internet of Things) est un système décentralisé et faiblement couplé d'objets (appareils physiques, véhicules, appareils électroménagers, ...) capables de détecter ou d'exploiter, stocker et interpréter les informations créées en eux-mêmes et autour du monde extérieur voisin où ils se trouvent.

Enfait que la tendance dans l'IoT est d'utiliser les technologies de communicationsans fil,l'objectif de ce chapitre est de fournir un état de l'art sur différentes technologies decommunication et domaines utilisés par l'IoT et expliquer leurs architectures et modede fonctionnement. On va étudier principalement les aspects de sécurités, notamment l'aspect confidentialité.

2.2 Sécurité IOT

On peut définir la sécurité informatique comme étant le fait d'assurer le bon fonctionnement d'un système et de garantir les résultats attendus de sa conception. Autrementdit, la sécurité représente l'ensemble de politiques et pratiques adoptées pour prévenir etsurveiller l'accès non autorisé, l'utilisation abusive, la modification ou le refus d'une opération informatique. A partir de cette définition, on peut extraire les bases de la sécuritéqui sont (Authentification, Confidentialité, Intégrité, ..).

Dans ce travail comme il est déjà mentionné on s'intéresse seulement à la gestion confidentialité dans un environnement IoT. [13].

2.2.1 Confidantialite IOT

La confidentialité est le mécanisme qui permet de cacher une donnée, et de cacher même l'information de son existence. Ainsi, empêcher toutes entité(s) nonautorisée(s) d'avoiraccès

à cette donnée. Généralement, on assure ce service en utilisant le chiffrement dedonnées. Ce dernier est basé sur des algorithmes mathématiques (AES, DES, RSA) permettant de déformer un texte en clair est le remettre à sa forme initiale grâce au à une ou plusieurs cléscryptographiques. Dans ce qui suit, nous étudions la confidentialité dans quelques technologies de communication IoT. [14].

2.3 Technologies IOT

Les technologies IoT ne sont pas tous d'un seul et même type de réseau, ils sontclassés par catégorie, par rapport à un ensemble de caractéristiques communes, tel que le débit, la portée et la bande de fréquences dans laquelle ils opèrent[15].

2.3.1 Réseaux etandus sans fil (WWAN)

Ces réseaux sont considérés comme étant les réseaux les plus étendus. Ils représentent généralement les réseauxà liaisons sans fil à faible consommation énergétique (LoRaWAN et Sigfox), et les réseaux cellulaires tels que GSM, UMTS, et LTE. Les WWANs incluent aussi les réseaux satellitaires telsque le (GPS)[16]:

2.3.1.1 LORAWAN

LoRAWAN est l'une des technologies de réseau étendu à faible puissance (LPWAN) qui a reçu une attention considérable de la communauté des chercheurs au cours des dernières années. Il offre une communication à faible puissance et faible débit sur une large gamme de zones couvertes[17].

Elle possèdeune architecture totalement adaptée à l'IoT, lui permettant de localiser facilement les objets mobiles. Elle est déployée pour des réseaux nationaux par des grands opérateurs detélécommunications (ex. Orange). Les réseaux LoRaWAN sont généralement présentés par une topologie en étoile dans laquelle des passerelles relient des terminaux (ex.capteurs, ordinateurs, etc) à un serveur réseau central, qui est relié à son tour à un serveur d'applications.

❒ **Architecture**

L'architecture LoRaWAN est composée de nœuds d'extrémité, de passerelles, d'un serveur de réseau et d'un serveur d'applications comme présenté dans la **figure2.1** ci-dessous[18]:

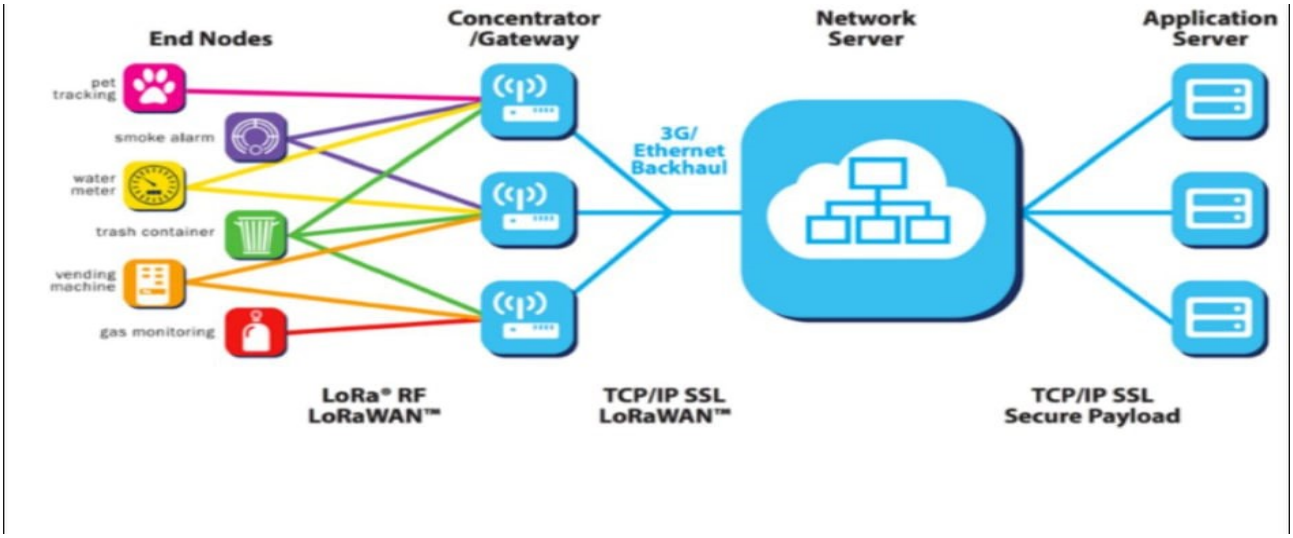

Figure 2.1: Architecure de LORAWAN[18].

Premeirment, le nœud d'éxtrimité envoie les données recueillies à une plusieurs passerelles à l'aide de la couche physique LoRa. Ensuit chaque passerelle enverra les données reçus des nœuds d'éxtrimité aux serveur de réseau en utilisant une liaison (Wi-Fi, cellulaire ethernet ou satellite). Le serveur réseau est l'entité intellegente qui va gérer le réseau, effectuer les controles de sécurité, effectuer des débits de données adaptatifs, filtrer les paquets reçus redondants, etc[18].

❒ **Sécurité**

La politique de sécurité de LoRaWAN assure les mécanismes de base qui sont l'authentification des objets, la confidentialité et l'intégrité des données. Cette politique définie également des techniques de partage de clés[27].

❒ **Confidantialite**

Une fois que l'objet soit associé au réseau de LoRaWAN, tous les messages échangés doivent étre chiffrés pour assurer la confidentialité en utilisant les clés de session connus uniquement par le serveur réseau et l'objet concerné. Le chiffrement de message est établis via le standard AES128[20] avec le mode d'opération à compteur (CounTeR (CTR))[31].

2.3.1.2 Technologies Cellulaire

Ce sont des réseaux longue portée (de quelques kilométrés en ville à 30 km en zone rurale) et consommateurs d'énergie. A l'image des réseaux GSM, 2G, 3G ou 4G, ils permettent le transport de grands volumes de données (vidéos, images, etc.) et ont une bonne couverture

au niveau national et international[22].

A. technologies 2G

La 2G est basée sur le GSM (Global System for Mobile technologie de la communication). Systéme 2G utilisé combinaison de TDMA (Time Division Multiple) Access) et FDMA (Frequency Division Multiple Accés). Grace à cela, un plus grand nombre d'utilisateurs ont pu se connecter à un moment donné dans une bande de fréquence donnée[22].

B. Les technologies 3G

Le systéme 3G utilise le CDMA (Code Division Multiple Access) et WCDMA (Wide Band Code Division Accès multiple). Le CDMA est une technique dans laquelle un un code unique est attribué a chaque utilisateur utilisant lea ce momentlà. Après avoir attribué un code unique, la largeur de bande entiérement disponible est utilisée efficacement en elle. De ce fait, un trés grand nombre d'utilisateurs peuvent utiliser la chaine en meme temps par rapport à la TDMA et FDMA[22].

C. Les technologies 4G

La technologie LTE (Long Term Evolution) ou la 4G s'appuie sur un réseau de transport commutation de paquet IP. Elle nia pas prévu de mode d'acheminement pour la voix, autre que la VoIP, contrairement à la 3G qui transporte la voix en mode circuit. Le LTE utilise des bandes de fréquences hertziennes d'une largeur pouvant varier de 1,4 MHz, 20 MHz,permettant ainsi d'obtenir (pour une bande 20 MHz) un débit binaire théorique pouvant atteindre 300 Mbit/s en downlink a, alors que la *vraie 4G* offre un débit descendant atteignant 1 Gbit/s[22].

- **Architecture LTE**

L'architecture générale du système LTE comme le montre la figure2.2 [24].

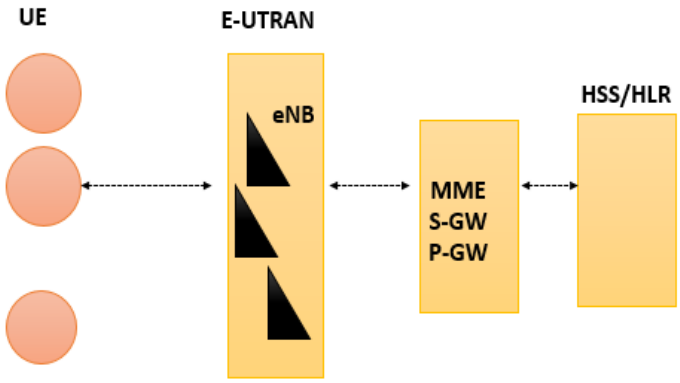

Figure 2.2: Architecture du système LTE[25].

- **UE**: terminal mobile.
- **E-UTRAN**: réseau d'accès radio terrestre universel évolué.
- **eNB**: station de base de la E-UTRAN.
- **MME**: entité de gestion de la mobilité.
- **S-GW**: passerelle de service.
- **P-GW**: passerelle réseau de données par paquets.
- **HLR**: enregistreur de localisation géographique des abonnés.
- **HSS**: sur-ensemble du HLR intégrant des nouveaux protocoles de cœur de réseau (Diameter et SIP) propres aux réseaux 4G.
- communiquentavec les MMEs -en passant par des passerelles si nécessaire- qui sont connectées aux HSS/ HLR[32].

- **Sécurité**

  On s'intéresse uniquement au LTE, car à partir de l'année 2012, ce dernier est devenu la technologie la plus déployée. Le LTE assure les services principaux de la sécurité, qui sont l'authentification des objets, la confidentialité et l'intégrité de données[27].

- **Confidantialite**

  Le LTE utilise un standardde confidentialité appelé Evolved Packet System Encryption-Algorithm (128-EEA3). L'algorithme de confidentialité 128-EEA3 fournit un chiffrement par flux utilisé pourchiffrer/déchiffrer des blocs de données via une clé symétrique (ex. CK). Le bloc de données peut avoir une longueur comprise entre 1 et 32 bits[42].

2.3.1.3 Technologie Satilitaire

Un systéme de communication par satellite hybride fournit des communications, en particulier un accès Internet, aux utilisateurs d'ordinateurs. Le système de communication hybride par satellite comprend un système par satellite et un système de communication terrestre. Le système satellite comprend deux émetteurs récepteurs[43].

Le premier émetteur récepteur reçoit et transmet un premier ensemble de signaux reçus du système de communication terrestre à une pluralité d'unités d'utilisateur. A l'inverse, le deuxième émetteur récepteur du système a satellites reçoit un deuxieme ensemble de signaux dans une deuxième bande de fréquences de l'utilisateur[44].

❒ **Architecture**

L'intégration des réseaux par satellite dans les réseaux terrestres peut étre faite de plusieurs manières. De nombreuses solutions techniques peuvent étre envisagées à ce propos mais le critère principal d'intégration sera principalement dicté par les modèles de role et de business qui en découlent[33].

Il est toutefois possible de définir trois types d'intégrations génériques:

1. Une intégration a fort couplage, dans laquelle le systeme mobile (3G, LTE, WIMAX) est étendu pour prendre en charge le media satellite comme un canal d'accès alternatif, demanière complétement transparente[33].
2. Une intégration relai, dans laquelle le satellite est intégré à l'infrastructure du réseau mobile, non pas directement au niveau de l'interface air mais à travers un relai spécifique (gateway) permettant l'accès au cœur de l'infrastructure mobile[33].
3. Une intégration a faible couplage, ou une interface spécifique au système satellite est ajoutée au terminal mobile satellite afin de permettre aussi l'accès à un réseau IP terrestre par cette interface. Des terminaux multimodaux et multi technologies capables de gérer plusieurs interfaces et leurs protocoles spécifiques (par exemple DVB-RCS+M) sont donc nécessaires[33].

❒ **Sécurité**

Il existe plusieurs travaux qui visent à sécuriser les réseaux de communication satellitaire. D'après[45], il étudie le service de la confidentialité dans un réseau satellitaire bidirectionnel composé de deux utilisateurs mobiles qui souhaitent échanger des messages via un satellite multi-faisceaux. D'autres travaux[46] proposent l'utilisation du protocole Satellite Secure Sockets Layer (SSL)[47] qui représente l'utilisation du protocole SSL dans les

réseaux satellitaires afin d'assurer l'authentification des utilisateurs, la confidentialité et l'intégrité de données.

❒ **Confidantialite**

La confidentialité dans la technologie satellitaire est assurée par le Data Encryption Standard (DES)[44].

2.3.2 Réseaux métropolitains sans fil (WMAN)

Le réseau métropolitain sans fil (WMAN pour Wireless Metropolitan Area Network) est connu sous le nom de Boucle Locale Radio (BLR). Les WMAN sont basés sur la norme IEEE 802.16. La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication[16].

2.3.2.1 WIMAX

Le WiMAX ou WorldwideInteroperability for Microwave Access est une famille de normes, définissant des connexions à haut-débit par voie hertzienne, développée par le Consortium WiMAX Forum et ratifié en 2001 par l'IEEE sous le nom IEEE-802.16. Le WiMAX est aussi le nom commercial délivré par le WiMAX Forum aux équipements conformes à la norme IEEE 802.16, afin de garantir un haut niveau d'interopérabilité entre ces différents équipements[46].

❒ **Architecture**

L'architecture du réseau WIMAX se compose de stations de base et des stations mobiles ou clientes (SS, Subscriber Station). La station de base joue le rôle d'une antenne centrale chargée de communiquer et de desservir les stations mobiles qui, à leur tour, servent les clients utilisant le WIFI ou l'ADSL. La station de base est constitué de deux modules[46]:

1. Module ≪ indoor ≫ qui contient le processeur, le modem, l'interface Ethernet et un module radio.
2. Module ≪ outdoor ≫ qui contient un module radio et une antenne d'émission-réception.

En plus de la station cliente qui contient les deux modules avec les mêmes rôles que pour la BS, il faudra avoir un terminal similaire au modem ADSL pour assurer la connexion.

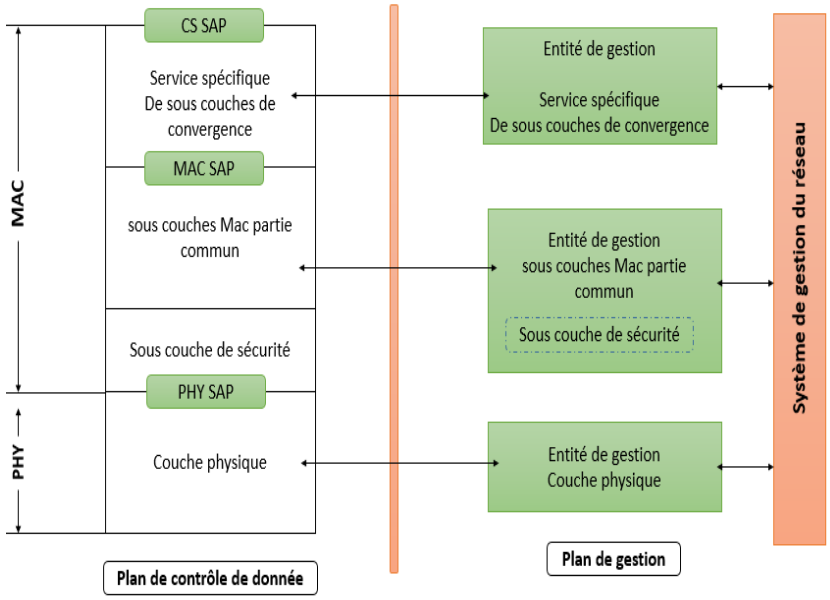

Figure 2.3: Architecture en couche de la norme 802.16[35].

La figure2.3 représente un exemple d'architecture générale d'un réseau d'accès à large bande Il s'agissait au départ dans la version 802.16a et 802.16d de liaisons point à multi-points qui offrent la possibilité de se déplacer dans un secteur donné[35].

❒ **Sécurité**

L'aspect sécurité fut reconnu comme une des principales faiblesses des premières versions. Le dernier 802.16e a amélioré ces aspects en introduisant intégrité, authentification et confidentialité sur les réseaux sans fil haut débit[48].

De plus, la sous-couche sécurité apporte aux utilisateurs une protection forte contre le détournement du service. La station émettrice (BS Base Station) se protège des accès illicites en sécurisant les flux de service associés dans le réseau. La sous-couche sécurité introduit également des mécanismes d'authentification dans le protocole client/serveur de gestion des clés, par lequel la BS contrôle la distribution des éléments de chiffrement aux stations mobiles (MS Mobile Station). En plus, les mécanismes de sécurité de base sont renforcés en ajoutant une authentification des équipements basée sur un certificat numérique[48].

❒ **Confidantialité**

Le Wimax permet de garantir une fiabilité, de segmenter les communications pour garantir la confidentialité. Il utilise un type plus solide, l'AES avec le Protocol CCMP[49].

2.3.3 Réseaux locaux sans fil (WLAN)

Le réseau local sans fil (noté WLAN pour Wireless Local Area Network) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre-eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes exemple: wifi; hepperlan[16].

2.3.3.1 Wi-Fi

Le Wi-Fi (contraction de Wireless-Fidelity) est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN). Le principe de cette technologie est d'établir des liaisons radio entre, par exemple, des terminaux et des points d'accès pour se connecter sur un réseau local ou sur Internet. Dans la pratique, le Wi-Fi permet de relier des ordinateurs portables, des machines de bureau, des assistants personnels (PDA) ainsi que des périphériques mobiles a une liaison haut débit oua des appareils électroniques communiquant sur un rayon de plusieurs dizaines de mètres en intérieur, a plusieurs centaines de metres en environnement ouvert[16].

❒ **Architecture**

La norme IEEE 802.11 s'attache a définir les couches basses du modele OSI pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire[50]:

- La couche physique: proposant trois types de codages de l'information.
- La couche liaison de données: constitué de deux sous-couches: le controle de la liaison logique (Logical Link Control, ou LLC) et le controle d'accés au support (Media Access Control, ou MAC).

Le WiFi définit les deux premières couches (basses) du modèle OSI, à savoir la couche physique et la couche liaison de données. Elle introduit des modifications sur la couche basse du niveau lien (donc niveau MAC) et sur le niveau physique avec le support de plusieurs méthodes d'accès radio et les règles de communication entre les différentes stations. Il est à noter que la nouvelle couche MAC est commune à toutes les couches physiques. La figure2.4 suivante illustre l'architecture en couches de la norme IEEE802.11[37].

Figure 2.4: L'architecture en couches de la norme IEEE802.11[37].

❒ **Sécurité / Confidantialite**

La sécurisation de wi-fi est basée sur le standard 802.11i qui supporte trois protocoles de sécurité[38][51]:

- ✈ *WEP*, importé de la norme 802.11 originale.
- ✈ *TKIP* (Temporal Key Integrity Protocol), ce protocole est le successeur de WEP. Il met en œuvre l'algorithme dechiffrement RC4, et ajoute à chaque SDU11 MAC une signature de 64 bits baptisée MIC (Message Integrity Code). La clé RC4 (128 bits) est déduite d'un compteur de 48 bits (Transmit Sequence) transmis en clair et d'une clé TK (Temporal Key).
- ✈ *CCMP* (Counter-Mode/CBC-MAC), ce protocole utilise l'algorithme de chiffrement AES en mode CCM et une signature MIC. Les paramètres de chiffrement (bloc initial?) sont déduits d'un compteur de 48 bits (PacketNumber) transmis en clair et d?une clé TK[38].

2.3.4 Réseaux personnels sans fil (WPAN)

Concernent les réseaux sans fil à faible portée, de l'ordre de quelques dizaines de mètres. Tout commela portée qui varie d'une technologie WPAN à une autre, le débit varie aussi. Ce dernierpeut être à 250 Kbits/S (ZigBee) jusqu'à 1 Mbits/S (cas du Bluetooth). Ces technologiessuivent la famille IEEE 802.15, les plus connues celles de la sous norme IEEE 802.15.1(Bluetooth), et celles qui sont utilisées dans le domaine des réseaux de capteurs sans fil(WSN pour WirlessSensor Networks) qui suivent principalement la sous norme IEEE802.15.4 tel que ZigBee, OCARI, 6LoWPAN, etc[27].

2.3.4.1 6LoWPAN

6LoWPAN est une spécification d'un réseau personnel sans fil à faiblepuissance. Il peut être déployé avec une topologie en mode étoile ou maillage. Il est basésur le protocole IPv6, ce qui

lui permet d'avoir plusieurs avantages, tel que la possibilité d'utiliser des infrastructures et technologies IP existantes qui sont testées et approuvées. On outre, les objets basée IP, peuvent être connectés facilement à d'autres réseauxIP, sans avoir besoin d'entités intermédiaires comme les passerelles[39].

❒ Architecture

La figure2.5 montre un exemple d'un réseau IPv6, y compris un maillage 6LoWPAN[52].

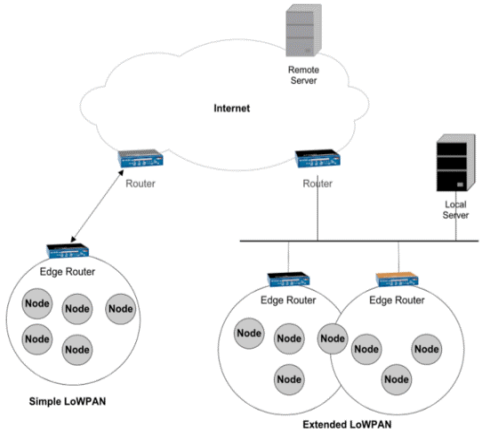

Figure 2.5: Une architecture d'un réseau 6LoWPAN[52].

Dans les réseaux 6LoWPAN, les données vont dans le réseau est destiné à l'un des appareils à l'intérieur le 6LoWPAN. Un réseau 6LoWPAN peut être connecté à d'autres réseaux IP via un ou plus de routeurs de périphérie qui transfèrent les datagrammes IP entre différents médias. [53].

❒ Sécurité

Comme dans le cas de la plupart des technologies IEEE 802.15.4, 6LoWPAN assure la confidentialité. En revanche, elle ne définit pas une méthode spécifique pour l'authentification, ni pour la gestion desclés[39]. Un travail intéressant était proposé par[39]définit une méthode d'authentification qui utilise le protocole Extensible Authentication Protocol GeneralizedPre-SharedKey (EAP-GPSK), qui est basé sur la cryptographie symétrique.

❒ Confidantialite

Afin de protéger les données échangées, [39] recommande l'utilisation du standard AESCCM, qui est un algorithme qui assure à la fois les services d'intégrité et confidentialité.

2.3.4.2 ZIGBee

Le Zigbee est une technologie WPAN à faible débit et à faible consommation de ressources (énergie, calcul, et mémorisation) qui peut être déployé avec une topologie enmode étoile ou maillée[54].

La bande de fréquences 2,4 GHz, les débits de données peuvent atteindre 250 Kb/s, tandis que dans la bande de fréquences 868 MHz, il n'a que20 Kb/s[55].

❒ **Architecture**

La structure du système Zigbee comprend trois types différents de périphériques, tels que le coordinateur Zigbee, le routeur et le périphérique final. Chaque réseau Zigbee doit comporter au moins un coordinateur qui agit en tant que racine et pont du réseau. Le coordinateur est responsable du traitement et du stockage des informations lors des opérations de réception et de transmission des données. Les routeurs Zigbee agissent comme des périphériques intermédiaires qui permettent aux données de les transmettre à d'autres périphériques[56].

Les périphériques finaux ont une fonctionnalité limité pour communiquer avec les nœuds parents, de sorte que la batterie est économisée ,comme indiqué sur la **figure2.6** suivante[56]:

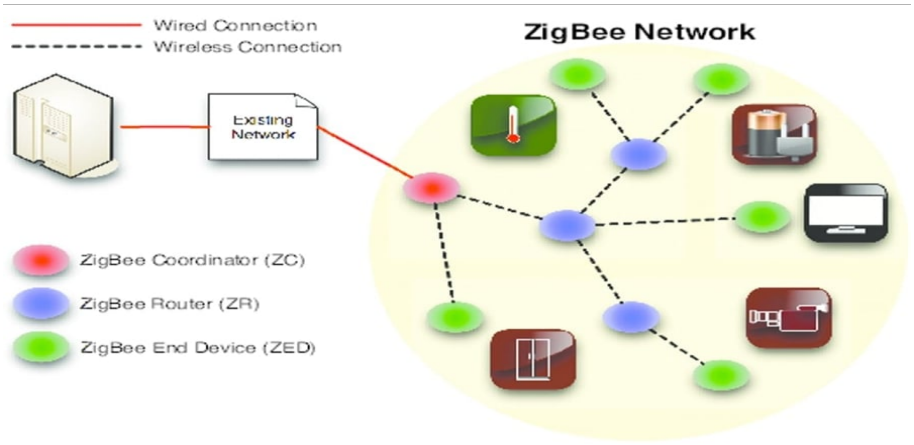

Figure 2.6: L'architecture du ZigBee[56].

❒ **Sécurité**

La sécurité est déployée au niveau de la couche application et la couche réseau. Chaque couche est responsable de sécuriser l'échange de ses données[57].

❒ Confidantialite

Les services de confidentialité et d'intégrité sont assurés grâce au chiffrement authentifié déployé au niveau de la couche application et la couche réseau. En effet, les messagessont doublement protégés au niveau des deux couches séparément, en utilisant le standard AES-CCM[58].

2.3.4.3 OCARI

OCARI (Optimisation de la communication pour un réseau industriel fiable ad hoc) est un protocole éco énergétique qui cible les réseaux de capteurs sans fil industriels. Il est adapté à applications de collecte de données où un puits, appelé CPAN, collecte les données générées par le capteur nœuds. Pour atteindre le puits, les données sont acheminées selon un arbre de collecte de données enraciné auévier[40].

❒ Architecture

figure2.7 présente un exemple d'un réseau OCARI avec trois ilots interconnectés par le biais de passerelles reliées à une unité de contrôle. Le rôle de cette unité de contrôle est de surveiller l'activité industrielle et mettre à jour les paramètres du réseau. Nous remarquons aussi un rondier qui se déplace entre les ilots et qui se connecte de manière ponctuelle à l'un de ces ilots afin d'effectuer des interventions localisées ou de collecter des informations[41].

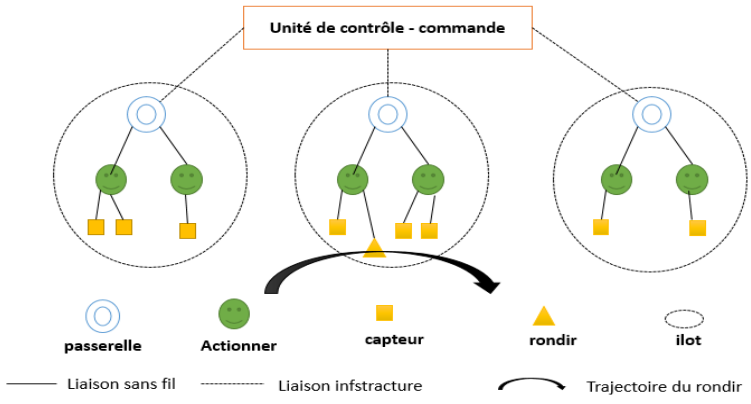

Figure 2.7: Topologie du réseau industriel OCARI[41].

❒ Sécurité

La sécurité dans OCARI En raison de la nouveauté d'OCARI, la version actuelle du protocole ne définit pas des services de sécurité. Dans[27], un protocole de sécurité robuste,

léger, rapide et économique en énergie a été proposé. Il est désigné spécialement pour être déployé sur des objets ayant des capacités limités. Il implémente ce protocole de sécurité sur la plateforme d'OCARI, et il a déployé sur des vrais capteurs.

❒ **Confidentialité**

En raison de la nouveauté d'OCARI ,la version actuelle du protocole ne définie pas des services qui assure la confidentialité[27].

2.4 Discussion

Dans ce chapitre nous avons présenté les différentes technologies de communications sans fil utilisées dans le cadre de l'IOT. Nous sommes focalisés principalement sur leurs approches de sécurités, et plus précisément sur leurs mécanismes de gestion de confidentialité.

Dans cette section, nous allons faire une comparaison entre ces différents protocoles de sécurité afin de pouvoir définir un modèle de confidentialité général.

Tableau de comparative

Type de réseau	**La technologie de communication**	**La confidentialité**
Réseaux étendus sans fil (WWAN)	LoraWAN Technologies cellulaires Technologies satellitaires	AES 128 128-EEA3 DES
Réseaux métropolitains sans fil (WMAN)	WiMax	AES CCMP (128)
Réseaux locaux sans fil (WLAN)	Wi-Fi	AES CCM (128)
Réseaux personnels sans fil (WPAN)	6LoWPANs ZigBee OCARI	AES-CCM (128) AES-CCM (128) N'est pas assurée

Table 2.1: Tableau de comparative les protocoles de sécurité.

D'après le tableau comparatif, nous concluons que la gestion de la confidentialité dans la plupart de ces technologies de communication IOT est basée sur le standard de chiffrement AES avec une clé de chiffrement de 128bits, et cela bien sûre pour plusieurs raisons, parmi lesquelles:

☛ Grande sécurité résistance à toutes les attaques connues.

☛ Large portabilité: carte à puces.

☛ processeurs dédiés.

- Rapidité.
- Lecture facile de l'algorithme Blocs de 128 bits et clés de 128/192/256 bits.
- Durée de vie de 20 à 30 ans.

2.5 Conclusion

Le long de ce chapitre, nous avons présenté quelques technologies de communications. Nous avons focalisé sur leur approche de sécurité et plus précisément sur leur confidentialité.

Donc, le but du prochain chapitre est de présenter le standard de chiffrement AES qui assure la confidentialité dans la plus part de ces technologies de communications dans le cadre de l'IOT.