Université Assane Seck de Ziguinchor

UFR Sciences et Technologies

Département Informatique

MÉMOIRE DE FIN D'ÉTUDES

Pour l'obtention du diplôme de Master

Mention : Informatique

Spécialité : Génie Logiciel

Sujet :

Étude des technologies de communication dans l'Internet des objets

Présenté par :

Mme. Ndeye Fatou Gueye Dite Tabaski DIAW

Soutenance le 09/01/2023

Membres du jury :

- Pr. Youssou FAYE (Président du Jury).

-Dr El Hadji Malick NDOYE (Examinateur).

-Dr Mouhamadou GAYE (Examinateur).

-Dr Abel DIATTA (Encadrant).

Sous la direction de :

- Dr. Abel DIATTA

Année Universitaire : 2021 – 2022

Résumé

Parmi les technologies de communications sans fil existantes, les LPWANs (Low Power Wide Area Network) attirent de plus en plus l'attention, notamment grâce à leur longue portée radio et leur faible consommation d'énergie. Cependant, chercher à minimiser la consommation d'´énergie peut parfois compromettre la résilience de la transmission des données face à des perturbations de l'environnement (interférences, obstacles) et de la mobilité des objets connectés. Par ailleurs, la longue portée radio aussi impose une limitation du temps d'occupation de la bande de fréquence par chaque nœud.

Dans ce mémoire, nous nous intéressons de manière générale aux technologies de communications dans un système IoT. Grace aux nombreux paramètres configurables, l'interconnexion entre objet peut s'adapter potentiellement a des environnements et applications IoT très hétérogènes suivant le type de communication utilisé.

La contribution principale de ce mémoire est une synthèse des technologies de communication qui permettra à un architecte pour la mise en place de son système IoT de savoir quel méthode de communication utilisé en fonction des besoins de son système.

Pour y parvenir, une étude du système IoT, des objets connectées, des types de réseaux sans fils a été fait au préalable tout en présentant le types de fonctions de certains protocoles, leurs avantages et inconvénients.

Dans ce mémoire aussi après cette étude de manière générale nous avons fait un choix de type de communication qui sera utilisé avec le réseau pour un cas pratique pour.

Mots clés : IOT, LoRaWAN, LPWANs.

Abstract

Among the existing wireless communication technologies, LPWANs (Low Power Wide Area Network) are attracting more and more attention, especially due to their long radio range and low energy consumption. However, seeking to minimize energy consumption can sometimes compromise the resilience of data transmission to environmental disturbances (interference, obstacles) and the mobility of connected objects. Moreover, the long radio range also imposes a limitation on the time of occupation of the frequency band by each node.

In this paper, we are interested in the communication technologies in an IoT system in a general way. Thanks to the numerous configurable parameters, the interconnection between LoRaWAN can potentially adapt to very heterogeneous environments and IoT applications depending on the type of communication used.

The main contribution of this thesis is the synthesis of communication technologies that will allow an architect for the implementation of his IoT system to know which communication method to use according to the needs of his system.

To achieve this, a study of the IoT system, connected objects, types of wireless networks has been done beforehand while presenting the types of functions of some protocols, their advantages and disadvantages.

In this dissertation also after this study in a general way we made a choice of type of communication that will be used with the network for a practical case for.

Keywords: IoT, LoRaWAN, LPWANs.

Remerciements

En premier lieu et avant tout, nous remercions Allah le tout-puissant, le miséricordieux, de nous avoir appris ce que nous ignorons, de nous avoir donné la santé, la volonté et le courage et tout ce qui nous était nécessaire, pour l'achèvement de ce mémoire de recherche.

On tient à remercier notre encadrant Dr. Abel DIATTA, Enseignant-Chercheur à l'Université Assane SECK de Ziguinchor, de nous avoir proposé ce sujet, ses précieux conseils, sa confiance en ma personne, sa disponibilité, sa rigueur, ses orientations précises, sa patience et son aide durant toute la période de travail.

Nous remercions vivement tous nos enseignants du département Sciences et technologies pour leurs efforts au cours de nos études universitaires.

Nous n'oublions pas nos collègues de la promotion 'GL-2018'.

Enfin, nous remercions tous ceux qui ont contribué de loin ou de près à la réalisation de ce travail.

Dédicace

A la mémoire de NDEW DIOUF.

A mes très chers parents.

A Ma chère famille.

Liste des Abréviations

IOT: Internet of Things (internet des objets).

FDMA : Single-Carrier Fréquence Division Multiple Access

TDD : Time Duplex Division

IP : Internet Protocol

ROM: Read Only Memory

RAM: Random Acces Memory

TLS: Transport Layer Security

DTLS: Datagram Transport Layer Security

UDP: User Datagram Protocol.

RFID: Radio Frequency Identification.

VMSK: Very Minimum Shift Keying.

MIC : Message Integrity Control.

LPWAN : Low Power Wide Area Network.

UNB : Ultra Narrow Band

Avant-propos

Pour l'obtention du diplôme de master en génie logicielle à l'université Assane Seck de Ziguinchor, du Sénégal, les étudiants doivent présenter un mémoire professionnel ou de recherche de fin de cycle.

C'est dans ce dessein que j'ai choisi de faire un sujet de recherche qui consiste à élaborer une étude des technologies de communication dans l'Internet des objets.

Listes des tableaux

Listes des figures

Tables des matières

Introduction générale

L'Internet of Things (internet des objets) ou l'IoT marque le début d'une nouvelle ère en matière de connectivité, de communication et de mobilité. Grâce à elle, les objets courants deviennent des actifs « intelligents », s'intègrent de façon transparente à un réseau mondial et sont en mesure de produire et d'échanger des données utiles sans intervention humaine. Il s'agit d'un réseau qui permet, via des systèmes d'identification électronique normalisés et sans fil, d'identifier et de communiquer numériquement avec des objets physiques afin de pouvoir mesurer et échanger des données entre les mondes physiques et virtuels. À travers un tel paradigme, une gigantesque expansion de l'Internet d'aujourd'hui est anticipée avec de nouveaux domaines d'applications comprenant la surveillance, la sécurité, la santé, les maisons et villes intelligentes, et les systèmes de logistique et de transportation intelligents.

Cependant comme tout système informatique l'IoT présente quelques risques. Certains objets peuvent ainsi être piratés ou, tout simplement, cesser de fonctionner pour une raison logicielle. On peut ainsi, dans certains cas, perdre le contrôle non plus d'un ordinateur portable ou d'un téléphone, mais d'une voiture ou de la porte de son habitation, mais malgré ces contraintes elle peut être très utile.

Par ailleurs, dans un système IoT, la communication occupe une place centrale. Dans un monde où le nombre d'objets connectés augmente de jours en jours, il est important, avant de déployer un système IoT, de maîtriser l'ensemble des technologies utilisées pour assurer la communication de bout en bout entre les objets. En effet, la technologie de communication à utiliser dépend de plusieurs facteurs tels que la nature et le volume des données à envoyer, l'environnement géographique (des espaces avec ou sans obstacles), la nature de la zone de déploiement (des zones avec moins ou beaucoup de bruit), etc. En faisant un mauvais choix sur la technologie à utiliser par rapport à la zone de déploiement, cela peut entrainer beaucoup de désagréments sur la qualité de service, notamment des problèmes de fidélité, de fiabilité, d'intégrité, etc.

Dans ce mémoire, notre objectif essentiel est de mener une étude comparative de l'ensemble des technologies de communication utilisées dans les systèmes IoT afin d'en ressortir les forces et faibles de chacune d'elles, mais surtout de montrer les critères déterminants dans le choix d'une technologie de déploiement IoT.

Ce mémoire est divisé en quatre chapitres.

Le premier chapitre présente les concepts de base de l'internet des objets.

Le deuxième chapitre présente l'architecture de l'Internet des objets.

Le troisième chapitre présente les Technologies de communications dans l'Internet des objets.

Enfin, le dernier chapitre relate un cas pratique ou nous avons l'utilisation du capteur de température DHT11 avec le réseau LoRaWAN.

CHAPITRE 1 : Concepts de base de l'Internet des objets

Introduction

Avec l'évolution des technologies, nous allons assister à une croissance importante du nombre d'objets connectés. Par exemple, Cisco (2013) estime à 50 milliards leur nombre dans le monde en 2020. Les recherches sur ce domaine étant dans un état embryonnaire, il n'existe pas de définition standard des objets connectés qui constituent un système d'objets connectés. Néanmoins, selon Porter et Helpmann (2014), les objets connectés sont définis par trois éléments : des composants physiques (parties mécaniques, électroniques…), des composants intelligents (des capteurs permettant d'identifier/ mesurer des données et des actionneurs qui vont réaliser des actions en fonction des données captées) et des composants de connectivité (grâce à un système de transmission de ces données). Par exemple, une montre (avec ses composants physiques) devient un objet connecté si elle est dotée d'une fonctionnalité pour accéder à Internet ou à d'autres objets (des composants de connectivité) et d'un système qui lui permet en plus de stocker et d'analyser les données pour lancer des actions comme l'envoi d'alertes ou pour aider à la prise de décision (des composants d'intelligence). [1]

Nous allons dans ce chapitre faire une étude de l'internet des objets et des objets connectés de manière générale.

1 L'Internet des objets, qu'est-ce que c'est ?

L'internet des objets est un nouvel outil de connectivité et de mobilité, qui transforme les affaires et la vie quotidienne à des objets connectés. Les objets courants deviennent des actifs intelligents, s'intègrent de façon transparente à un réseau mondial et sont en mesure de produire et d'échanger des données utiles sans intervention humaine. Il s'agit d'un réseau de réseaux qui permet, via des systèmes d'identification électronique normalisés et sans fil, d'identifier et de communiquer numériquement avec des objets physiques afin de pouvoir mesurer et échanger des données entre les mondes physiques et virtuels. A travers un tel paradigme, aujourd'hui l'internet des objets est anticipé avec de nouveaux domaines d'applications comprenant la surveillance, la sécurité, la santé, les maisons et villes intelligentes ainsi que les systèmes de logistique et de transportation intelligents.

1.1 Définition de l'IoT

Le terme «Internet des objets» (IoT) a été utilisé pour la première fois en 1999 par le pionnier de la technologie britannique « Kevin Ashton » pour décrire un système dans lequel les objets du monde physique pouvaient être connectés à l'Internet par des capteurs. Ashton a inventé le terme pour illustrer la puissance des étiquettes d'identification par la radiofréquence (RFID) utilisées dans les chaînes d'approvisionnement d'entreprise à l'Internet pour compter et suivre les marchandises sans intervention humaine.

Le CERP-IoT4 définit l'Internet des objets comme : « une infrastructure dynamique d'un réseau global. Ce réseau global a des capacités d'auto-configuration basée sur des standards et des protocoles de communication interopérables. Dans ce réseau, les objets physiques et virtuels ont des identités, des attributs physiques, des personnalités virtuelles et des interfaces intelligentes, et ils sont intégrés au réseau d'une façon transparente ».[2]

1.2 Les composants impliqués dans l'Internet des Objets

Généralement, le concept d'Internet des Objets exige la coordination des dispositifs suivants:

- ✓ une étiquette physique identifie chaque objet / une étiquette virtuelle identifie chaque lieu;
- ✓ un dispositif mobile (téléphone cellulaire, organiseur, ordinateur portable...) doté d'un logiciel additionnel, lit les étiquettes physiques ou localise les étiquettes virtuelles ;
- ✓ un réseau sans fil relie le dispositif portable à un serveur contenant l'information relative à l'objet étiqueté ;
- ✓ les informations sur les objets sont gérées dans des pages existantes sur le web ;
- ✓ un dispositif d'affichage (écran d'un téléphone mobile, par exemple) permet de consulter les informations relatives à l'objet ou à un ensemble d'objets.[2]

1.3 Domaines d'application d'IoT

- ✓ La **Santé intelligente** (Smart Heath) : l'IoT contribuera également à élargir l'accès et à améliorer la qualité de la santé. À mesure que la demande de soins de santé doublera, les appareils intelligents connectés aideront à relever ce défi en soutenant une gamme de services de santé en ligne qui améliorent l'accès et permettent le suivi des maladies chroniques et des conditions liées à l'âge à la maison. Ce faisant, ils amélioreront la qualité des soins et la qualité de vie des patients, tout en réduisant la pression exercée sur l'ensemble du système de santé. [3]

- ✓ Les **villes intelligentes** (Smart Cities) : dans les villes, le développement de réseaux intelligents, d'analyse de données et de véhicules autonomes constituera une plate-forme intelligente pour fournir des innovations en matière de gestion de l'énergie, de gestion du trafic et de sécurité, en partageant les bénéfices de cette technologie dans toute la société. [3]
- ✓ Dans **les transports**: la dernière avancée majeure fut l'adoption du GPS. Les petits appareils IoT possédant une connectivité sont un excellent choix pour développer des produits dans le domaine du transport. Selon le département américain des transports, plus de 32 000 personnes sont mortes dans des accidents de voiture aux États-Unis. Ça a permis de mettre en place une solution innovante utilisant l'IoT. Plus de 3000 capteurs ont été placés sur les routes pour réduire le délai entre un accident et l'arrivée des secours. [3]
- ✓ Le **bien-être et le confort** : La domotique ou la maison intelligente est un classique. Imaginez un instant que votre thermostat soit capable de se mettre en marche tout seul en fonction de l'emplacement de votre voiture vous permettant de vous réchauffer une fois rentré à la maison. Aussi, imaginez que votre réfrigérateur vous informe lorsque vous aurez besoin d'acheter du lait ou qu'il soit capable de créer une liste d'achats personnalisée en fonction de vos articles les plus achetés. Ou encore vous dire quand votre nourriture est sur le point de périmer.[3]

1.4 Les défis à relever de l'internet des objets

Donc, les principaux défis que rencontre l'IoT sont :

- ✓ La détection d'un environnement complexe : des façons novatrices de saisir et de diffuser de l'information - du monde physique au nuage.
- ✓ Connectivité : Une variété de normes de connectivité câblées et sans fil sont requises pour permettre différents besoins d'application.
- ✓ La puissance est critique : de nombreuses applications IoT doivent fonctionner pendant des années sur des batteries et réduire la consommation globale d'énergie.
- ✓ La sécurité est vitale : protéger la confidentialité des utilisateurs et l'IP des fabricants; Détection et blocage d'activités malveillantes.
- ✓ IoT est complexe : le développement d'applications IoT doit être facile pour tous les développeurs, pas seulement pour les experts.
- ✓ Cloud est important : les applications IoT requièrent des solutions de bout en bout, y compris des services en nuage.[3]

Donc, plusieurs obstacles pourraient ralentir la progression de l'IoT, notamment le déploiement du protocole IPv6, l'alimentation des capteurs et la définition de normes.

2 Les objets connectés.

Les objets connectés se définissent en termes d'identité, d'interactivité, de sensibilité et d'autonomie. Ces caractéristiques permettent non seulement aux éléments physiques d'acquérir de nouvelles capacités, mais aussi de créer de nouveaux objets. L'Internet des objets ouvre donc un environnement ultra-connecté, des capacités et des services permettant une interaction avec les objets physiques et leur représentation virtuelle.

2.1 Définition d'un objet connecté

Un **objet connecté** peut aussi être définit comme objet physique équipé de capteurs ou d'une puce qui lui permettent de transcender son usage initial pour proposer de nouveaux services. Il s'agit d'un matériel électronique capable de communiquer avec un ordinateur, un smartphone ou une tablette via un réseau sans fil (**Wi-Fi**, **Bluetooth**, réseaux de téléphonie mobile, réseau radio à longue portée de type **Sigfox** ou **LoRa**, etc.), qui le relie à Internet ou à un réseau local. [4]

2.2 Caractéristiques d'un objet connecté

Les caractéristiques d'un objet connecté sont les suivantes :

- ✓ **Identification :** c'est un code qui permet à l'objet d'être identifié parmi d'autres objets connectés.
- ✓ **Sensibilité à son environnement :** un objet connecté peut avoir la capacité de communiquer avec son environnement.
- ✓ **Interactivité :** la connexion en permanence d'un objet connecté à son réseau n'est pas nécessaire, sauf si l'objet a besoin de communiquer des informations à travers le réseau.
- ✓ **Représentation virtuelle :** est un programme résidant dans le Cloud pouvant agir au nom d'un objet connecté. Cette représentation est nommée parfois cyber-objet ou agent virtuel.
- ✓ **Autonomie :** un objet connecté doit fonctionner indépendamment d'un contrôle à distance.

2.3 Les composants de base d'un objet connecté

Les composants de base d'un objet connecté sont les suivants :

- **Le microcontrôleur**

Un microcontrôleur est un circuit intégré composé des éléments de base suivants :

- ✓ **Microprocesseur** qui se charge des calculs.
- ✓ **Mémoire permanente (ROM)** qui contient le programme à exécuter.
- ✓ **Mémoire temporaire (RAM)** qui contient les données temporaires.
- ✓ **Des ports d'entrée/sortie.**

Il en existe de différents types de microcontrôleurs pour le développement des projets d'IoT, nous allons citer en guise d'exemple le microcontrôleur Arduino:

- ✓ **Le microcontrôleur Arduino**

Figure 1:la Carte Arduino UNO.

Le tableau ci-dessous (Tableau 1) contient les spécifications permettant de comparer la carte Arduino et d'autres cartes tel que le BeagleBone et la carte.

Tableau 1:Description des microcontrôleurs : Arduino UNO, BeagleBone et Raspberry

Nom de la carte	ARDUINO UNO	BEAGLEBONE	RASPBERY (model b)
Origine	Interaction Design Institute d'Ivrea (Italie)	Projet de Hardware Open Source pilote par Texas Instruments	Université de Cambridge
Organisations en charge des Spécifications	Arduino.cc	BeagleBoard.org	Raspberry Pi Foundation (fondation de droit en anglais)
Naissances	2005 fabrications en Italie par (Smart Projets)	2008(BeagleBoard)-2011(BeagleBone) (accord de fabrication/distribution avec Digi-Key)	2008(accord de fabrication avec RS Components et Famell/ Element 14 en 2011)
Prix	30 dollars	90 dollars (45 dollars pour le BeagleBone Black)	Moins de 40 dollars

Taille	45,43X32, 34mm	86,36X53, 34mm (bords arrondis)	85,60X53, 98mm
Processeur	ATMega328 8bits d'Atmel à 16MHz	Sitara 335 de TI basé sur un Cortex-QB à 720MHz (1GHz BeagleBone Black)	BCM2835 de Broadcom basé sur un ARM11 a 700MHz GPU intégrée (Vidéo Core 4 de Broadcom)
Mémoires	2ko ram, 1ko Eprom	256 Mo DDR2 (512 Mo DDR3 pour le BeagleBone Black)	512 Mo Sdram
Mémoire Flash	32ko	Sur MicroSD (4GO)	Sur Carte SD
Tension d'entrée	7V-10V	5V-3,3V	5V
Consommation	42mA (0.5W)	210 à 450mA (2,5W max.)	
Ethernet	Non	10/100 Ethernet	10/100 Ethernet
USB	Non	1 USB 2.0	2 USB 2.0
Sorties Vidéo	Non	Non (micro HDMI pour la BeagleBone Black)	Composite et HDMI

- **La plaque d'essai (BreadBoard)**

La plaque d'essai est une plaque en plastique isolant et pleine de trous. Elle sert à tester des montages avant de souder les composants. Elle est répartie en deux parties, partie extérieure où les trous sont reliés de façon horizontale, et la partie intérieure où les trous sont reliés de façon verticale.

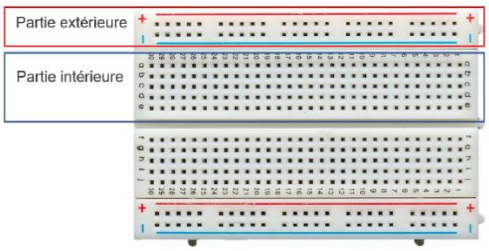


Figure 2:BreadBoard (plaque d'essai).

- **Les capteurs**

Un capteur est un composant électronique qui permet de transformer une grandeur physique en une grandeur électronique. Il existe trois types de capteurs, classifié selon leurs sorties :

- ✓ **Numérique** dont la sortie est une valeur binaire.

- ✓ **Logique (Tout ou rien)** dont la sortie n'a que deux états électriques, soit Haut (1) soit Bas (0), qui est un cas spécial du type numérique.
- ✓ **Analogique** dont la sortie est un signal continu et proportionnel à la valeur mesurée.

1. **Exemples de capteurs :**

- ✓ **Capteur de température (LM35) :**

Type : Numérique.

Voltage : de 4V jusqu'à 30V.

Intervalle : de -55°C jusqu'à +150°C.

Fonctionnement : le capteur fournit la température de son entourage en Celsius avec un large intervalle.

Figure 3: le Capteur de température (LM35).

Les actionneurs

Un actionneur est un composant électronique qui transforme un signal en entrée en une action. Nous citons ces deux exemples :

- ✓ **LED :** C'est une composante électronique émettant un signal lumineux, généralement blanc, rouge, vert ou bleu.

Figure 4:Exemple d'actionneur LED

- ✓ **Buzzer :** C'est une composante électronique émettant un signal sonore, l'intensité du son dépond de l'intensité du courant.

Figure 5:Exemple d'actionneur : Piezo Buzzer

Les câbles

Il en existe deux types de câble essentiels pour la mise en œuvre des montages, qui sont présentés ci-dessous :

- ✓ **Câble USB** qui sert à relier la carte Arduino à l'ordinateur, soit pour le chargement du programme, ou l'alimentation de la carte.

Figure 6:Câble USB type A-B

- ✓ **Les fils de liaison** qui servent à connecter les composants pour construire des montages des objets connectés.

Figure 7:fils de liaison

Conclusion

Ce chapitre a fait l'objet d'une étude détaillée de l'IoT et des objets connectés. Nous avons présenté les différents concepts et composants ainsi que les caractéristiques liés à l'IoT et aux objets connectés.

Afin de mettre le point sur la communication dans un système IoT, nous consacrons tout un chapitre pour l'étude de ce paradigme (voir chapitre 3).

Parmi les problématiques posées par l'utilisation des systèmes d'IoT, on trouve le diagnostic qui consiste à établir une architecture fiable. Donc, le prochain chapitre est consacré à l'étude de l'architecture de l'internet des objets.

CHAPITRE 2 : Architecture de l'Internet des objets

Introduction

Ce chapitre s'articule autour de deux axes essentiels qui sont les éléments de base d'une architecture IoT et les protocoles et couches dans l'internet des objets. Nous allons dans la suite faire une étude détaillée de ces derniers tout en mettant en exergue leur complexité, leur hétérogénéité...

1 Éléments de base d'une architecture IoT

1.1 Qu'est-ce que l'architecture IoT?

L'architecture IoT peut en fait varier considérablement en fonction de la mise en œuvre. Elle doit être suffisamment ouverte avec des protocoles ouverts pour pouvoir prendre en charge plusieurs applications réseau.

Dans la majeure partie des cas elle se compose de 4 blocs constitutifs :

- ✓ La scalabilité
- ✓ La fonctionnalité
- ✓ La disponibilité
- ✓ La maintenabilité

Même s'il n'existe pas d'architecture IoT unique universellement acceptée, le format le plus basique et le plus largement accepté est une **architecture IoT à quatre couches.**

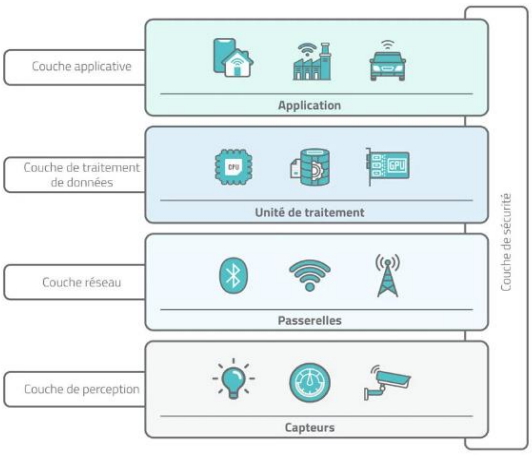


Figure 8:Architecture Basique de L'IOT

1.2 Etude détaillée de l'architecture IOT

L'architecture IOT se compose de différentes couches de technologies prenant en charge l'IOT. Il sert à illustrer les relations entre différentes technologies et à communiquer l'évolutivité, la modularité et la configuration des déploiements IOT dans différents scénarios.

1.2.1 La couche des appareils intelligents (couche de perception)

Elle est la couche la plus basse et est constituée d'objets intelligents intégrés à des capteurs. Les capteurs permettent l'interconnexion des mondes physique et numérique permettant de collecter et de traiter des informations en temps réel. Il existe différents types de capteurs à des fins différentes. Les capteurs ont la capacité d'effectuer des mesures telles que la température, la qualité de l'air, la vitesse, l'humidité, la pression, le débit, le mouvement, l'électricité, etc. Dans certains cas, ils peuvent également disposer d'une certaine mémoire leur permettant d'enregistrer un certain nombre de mesures.[5]

1.2.2 Passerelle et réseaux (couche réseau)

Un volume massif de données sera produit par ces minuscules capteurs, ce qui nécessite une infrastructure de réseau filaire ou sans fil robuste et performante comme moyen de transport. Les réseaux actuels, souvent liés à des protocoles très différents, ont été utilisés pour prendre en charge les réseaux machine à machine (M2M) et leurs applications. Avec la demande nécessaire pour desservir une gamme plus large de services et d'applications IOT tels que les services transactionnels à haut débit, les applications contextuelles, etc., plusieurs réseaux avec diverses technologies et protocoles d'accès sont nécessaires pour fonctionner les uns avec les autres dans une configuration hétérogène. Ces réseaux peuvent se présenter sous la forme de modèles privés, publics ou hybrides et sont conçus pour prendre en charge les exigences de communication en matière de latence, de bande passante ou de sécurité. [5]

1.2.3 Couche de service et de gestion (couche de traitement de donnée)

Le service de gestion rend possible le traitement des informations grâce à l'analyse, aux contrôles de sécurité, à la modélisation des processus et à la gestion des appareils. L'une des caractéristiques importantes de la couche de service de gestion est les moteurs de règles métier et de processus. L'IOT rassemble la connexion et l'interaction d'objets de systèmes en fournissant des informations sous la forme d'événements ou de données contextuelles telles que la température des marchandises, l'emplacement actuel et les données de trafic. Certains de ces événements nécessitent un filtrage ou un acheminement vers des systèmes de post-traitement tels que la capture de données sensorielles périodiques, tandis que d'autres nécessitent une réponse aux situations immédiates telles que la réaction aux urgences sur l'état de santé d'un

patient. Les moteurs de règles prennent en charge la formulation de logiques de décision et déclenchent des processus interactifs et automatisés pour permettre un système IOT plus réactif.

Dans le domaine de l'analyse, divers outils d'analyse sont utilisés pour extraire des informations pertinentes à partir d'une quantité massive de données brutes et pour être traitées à un rythme beaucoup plus rapide. L'analyse en mémoire permet de mettre en cache de grands volumes de données dans la mémoire vive (RAM) plutôt que de les stocker sur des disques physiques. L'analyse en mémoire réduit le temps d'interrogation des données et augmente la vitesse de prise de décision. L'analyse en continu est une autre forme d'analyse où les données, considérées comme des données en mouvement, doit être effectuée en temps réel afin que les décisions puissent être prises en quelques secondes.[5]

La gestion des données est la capacité à gérer le flux d'informations sur les données. Avec la gestion des données dans la couche de service de gestion, les informations peuvent être consultées, intégrées et contrôlées. Les applications de couche supérieure peuvent être protégées du besoin de traiter des données inutiles et réduire le risque de divulgation de la confidentialité de la source de données. Les techniques de filtrage des données telles que les données.[5]

L'anonymisation, l'intégration des données et la synchronisation des données, sont utilisées pour masquer les détails de l'information tout en ne fournissant que les informations essentielles utilisables pour les applications concernées. Avec l'utilisation de l'abstraction de données, les informations peuvent être extraites pour fournir une vue commerciale commune des données afin d'obtenir une plus grande agilité et une réutilisation dans tous les domaines. La sécurité doit être appliquée dans toute la dimension de l'architecture IOT, depuis la couche d'objet intelligent jusqu'à la couche d'application. La sécurité du système empêche le piratage du système et les compromis par du personnel non autorisé, réduisant ainsi la possibilité de risques.[6]

1.2.4 Couche d'application

L'application IoT couvre les environnements/espaces "intelligents" dans des domaines tels que : les transports, le bâtiment, la ville, le style de vie, la vente au détail, l'agriculture, l'usine, la chaîne d'approvisionnement, les urgences, les soins de santé, l'interaction avec l'utilisateur, la culture et le tourisme, l'environnement et l'énergie.[5]

1.3 La Sécurité dans IoT

La figure 9 expose un schéma d'attaque qu'un attaquant pourrait suivre pour gagner le contrôle total d'un système IoT. Elle est divisée en 3 parties : les paquets, les protocoles et finalement le système. La première étape se concentre sur les objets et plus précisément sur les messages envoyés et reçus. La seconde étape concerne le protocole et les potentielles façons d'altérer la topologie pour contrôler une partie ou la totalité d'un réseau. La dernière étape décrit les attaques contre le système après que ce dernier soit compromis.[7]

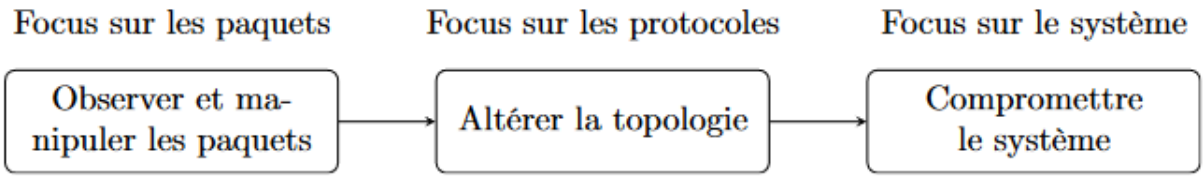


Figure 9:Schéma de la sécurité dans IOT.

1.3.1 Focus sur les paquets

La sécurité des paquets est le premier élément à prendre en compte comme il est montré sur la figure 9. Cette étape consiste à extraire des informations ou gagner potentiellement le contrôle d'un objet. Comme décrit plutôt, seules les vulnérabilités contre les communications et protocoles sont considérés, excluant ainsi toutes l'exploitation logicielle. Donc, cette étape décrit les attaques contre les communications d'un objet vers un autre ; en d'autres mots, les attaques dites cryptographiques. De plus, nous distinguons les attaques cryptographiques dites actives (l'absence de chiffrement, le chiffrement étrange, le mauvais chiffrement et le bon chiffrement) et celles considérées comme passives.

Les attaques cryptographiques passives consistent à extraire des secrets ou des données confidentielles, de messages interceptés, sans en émettre. Parce qu'aucune action n'est menée contre le réseau, le risque d'altérer l'intégrité ou la disponibilité de ce dernier est nul. Elles visent seulement à compromettre la confidentialité des données en accédant aux informations par l'écoute passive et furtive, autrement appelée eavesdropping.

Avec les attaques cryptographiques actives, un attaquant cherche à modifier le message transmis sur le réseau. Il peut alors injecter son propre trafic en forgeant ou en rejouant des paquets interceptés afin de perturber le réseau. Ainsi, une attaque cryptographique active vise à compromettre les trois principes de sécurité : la confidentialité, l'intégrité et la disponibilité.

1.3.2 Focus sur les protocoles

Après la première étape montré en figure 9, un attaquant est alors en mesure de récupérer certaines informations ou potentiellement prendre le contrôle d'un objet. L'étape suivante est de propager son contrôle ou simplement d'augmenter ses privilèges. Dans un système IoT, ceci consiste à altérer la topologie pour contrôler une ou plusieurs sous parties du réseaux en utilisant les faiblesses du protocole.il peut utiliser les attaques tel que l'attaque MiTM , l'attaque de flooding, l'attaque spoofing, l'attaque sybil , l'attaque wormhole

L'**attaque MiTM** (Man in The Middle) est une attaque qui consiste à secrètement intercepter, modifier et relayer les informations entre deux entités (objets ou personnes) qui croient qu'elles communiquent ensemble.

L'**attaque de flooding** consiste à envoyer une succession de requêtes à un objet en particulier, afin que ce dernier épuise la plupart de ses ressources dans le traitement de ces requêtes. Dans un contexte comme l'IoT, où les objets disposent de peu de ressources (batterie, puissance de calcul, etc…),

L'**attaque de Spoofing** décrit un attaquant ayant réussi à se faire passer pour un autre objet du réseau en altérant ou modifiant les données de la cible. Il utilise un objet que l'attaquant afin d'usurper ou imiter un objet légitime dans le réseau pour effectuer différentes actions, comme par exemple une déconnexion ou l'envoie de fausses informations.

L'**attaque sybil** vise à créer et utiliser un grand nombre d'identités depuis un unique nœud du réseau, considéré comme malveillant. Cette attaque est principalement utilisée pour cibler la réputation des systèmes distribués, mais elle est également une menace pour les protocoles de routage distribués.

L'**attaque wormhole** ici un tunnel est utilisé entre deux nœuds malveillants pour relayer plus rapidement des messages d'une zone A vers une zone B ou en faisant moins de sauts qu'il ne faudrait avec l'utilisation de l'algorithme de routage classique. L'attaquant peut utiliser un lien filaire, ou une technologie sans fil plus rapide, entre les deux points relais. Cette manipulation permet aux nœuds contrôlés par un attaquant d'être considérés comme le meilleur chemin entre les deux zones. Ainsi, la plupart des paquets entre ces deux zones sont transmis en suivant cette route. L'attaquant peut ensuite gagner des privilèges en écoutant ou en manipulant les paquets routés. [7]

1.3.3 Focus sur le système

Après la seconde étape, présentée dans la figure 9, un attaquant est en mesure de modifier une partie ou l'ensemble de la topologie d'un réseau. L'attaquant peut alors essayer de modifier ou d'altérer le bon fonctionnement du système dans son ensemble en utilisant l'attaque sinkhole ou l'attaque selective-forwarding.

L'**attaque sinkhole** se décrit par la création d'un point centralisé depuis un nœud contrôlé par l'attaquant pour attirer tout le trafic en provenance d'une zone spécifique. De plus, tous les objets de cette zone doivent communiquer en passant par cet objet malveillant. Cette attaque est également une condition d'exécution de nombreuses autres attaques, comme par exemple l'attaque selective-forwarding.

Afin que le nœud contrôlé par l'attaquant soit considéré comme le point central par tous les autres nœuds, il doit être défini comme un bon choix par l'algorithme de routage. En fonction de l'algorithme utilisé, les critères pour devenir un nœud attractif diffèrent. Cependant, une route de grande qualité et des transmissions à faible latence sont deux points qui permettent de devenir un nœud central dans toutes les communications. L'usurpation ou le rejet d'un paquet de contrôle du réseau avec comme contenu les spécifications d'un chemin de qualité sont de parfaits exemples pour réaliser cette attaque.[7]

L'**attaque selective-forwarding** ne peut être réalisée dans un réseau que si les nœuds actifs du réseau ne modifient pas leur configuration de routage lorsqu'ils transfèrent des paquets. Cette attaque consiste à laisser passer uniquement le trafic désiré par les nœuds malveillants. Les paquets restants ne répondant pas aux critères de l'attaquant sont supprimés pour s'assurer qu'ils ne sont pas propagés. Il y a deux méthodes pour implémenter cette attaque. La première est d'utiliser des nœuds malveillants, les faire devenir des trous noirs et les forcer à refuser de transférer tous les paquets. Cependant, ce comportement peut mener les nœuds légitimes à chercher une autre route pour envoyer leurs paquets. Par conséquent, la seconde méthode, plus efficace, consiste à supprimer uniquement les paquets considérés comme non essentiels pour le bon fonctionnement du réseau.[7]

2 Protocoles et couches dans l'Internet des objets

2.1 Quelques protocoles et leurs fonctionnement

Il en existe plusieurs protocoles de communication, assurant l'échange de données entre les différentes parties d'un système d'IoT, nous citons à titre d'exemples :

HTTP (Hypertext Transfer Protocol) : est un protocole de transfert hypertexte qui définit la communication entre un client (exemple : navigateur) et un serveur sur le World Wide Web (WWW). [4]

MQTT (Message Queuing Telemetry Transport) : est un protocole qui utilise le principe de « Publisher / Subscriber » pour connecter les systèmes entre eux, il se base sur le TCP/IP destiné à la transmission de paquets de courte taille.[8]

AMQP (Advanced Message Queuing Protocol) : est un protocole pour les systèmes de messagerie orientés messages (MOM). [4]

STOMP : (Simple Text Oriented Messaging Protocol) : est un protocole textuel au-dessus de TCP conçu pour permettre l'interaction avec un middleware orienté messages.[4]

6LoWPAN (IPv6 Low power Wireless Personal Area Networks) est un protocole destiné à transmettre des paquets IPv6 sur le protocole IEEE 802.15.4 qui concerne les LRWPAN (Low Rate Wireless Personal Area Network). Le but de ce protocole est de fragmenter les paquets IPv6 et de compresser leurs entêtes pour qu'ils puissent être envoyés sur le protocole IEEE 802.15.4.[8]

Thread est un protocole en réseau maillée utilisant 6LoWPAN, ce qui lui permet de se comporter comme un nœud normal dans un réseau local grâce au protocole IP. Tout protocole basé sur IP peut donc être utilisé par Thread.[8]

ZigBee est un protocole en réseau maillé basé sur IEEE 802.15.4 similaire à Thread, à ceci près qu'il n'utilise pas 6LoWPAN et, par conséquent, ne peut pas utiliser IP.IL implémente ses propres mécanismes de routage. [8]

COAP (Constrained Application Protocol) est un protocole basé sur l'architecture REST et le modèle client-serveur et dédié aux appareils contraints. Il a certaines similarités avec HTTP du fait de son architecture REST.[8]

BLE (Bluetooth Low Energy) est une version basse consommation de Bluetooth intégrée à la version 4.0 de ce dernier bien qu'il soit incompatible avec le mode standard de Bluetooth. Il est destiné aux paquets de petite taille. Tout comme Bluetooth et permet uniquement la transmission de paquets locaux et n'est pas destiné à la transmission de paquets sur Internet.[8]

2.2 Les défis relevés par les protocoles

L'un des **premiers défis** de l'IoT concerne la consommation d'énergie. L'augmentation du nombre d'objets connectés a pour effet inévitable d'augmenter la consommation énergétique. Des lors, le but de certains protocoles est de minimiser cet impact énergétique. Ce défis est donc relevé par 6LoWPAN et les protocoles bases sur lui comme Thread ou compatibles avec IEEE 802.15.4 comme ZigBee. Il est également relevé, dès la couche physique, par BLE, la version

basse consommation de Bluetooth, LoRaWAN/LoRa, SigFox, EnOcean et Z-Wave. Bien que certains protocoles plus applicatifs soient indiqués comme ayant une basse consommation, cela est dû aux protocoles sous-jacents qui le sont. Les protocoles bas consommation partent du principe que les petits appareils faibles en ressources et peu consommateurs d'énergie doivent être en mesure de participer à l'IoT. Pour ce faire, ces protocoles emploient des mécanismes de compression, réduisent leur portée et leur bande passante, supportent des objets dont les composants consomment peu, voire récoltent de l'énergie (mouvements, lumière, etc.), ou encore implémentent un mode dormant. Toutes ses solutions permettent de réduire tant que possible la consommation énergétique de l'appareil. A titre d'exemple, Pour un objet consommant 1 W en Bluetooth, son homologue basse consommation Bluetooth Low Energy (BLE) consomme entre 0,5 et 0,01 W, soit une division par 2 dans le pire des cas, et par 100 dans le meilleur. [8]

Deuxième défis : la sécurité. Cette sécurité implique beaucoup de fonctionnalités à remplir comme le chiffrement, l'authentification, des preuves d'authenticité, etc… Cependant, le chiffrement est une nécessité absolue pour qu'une communication soit sécurisée et est un bon élément de comparaison dans notre cas. On voit que la plupart des protocoles de la couche application reposent sur l'utilisation d'un protocole sous-jacent qui, lui, est chiffrée ou non. Par exemple COAP et MQTT peuvent utiliser TLS (DTLS étant la version UDP de TLS). Les protocoles de couche physique comme Bluetooth, 3G/4G, LoRaWAN/Lora, Wi-Fi et Z-Wave utilisent leur propre chiffrement, ce qui permet théoriquement de protéger tous les protocoles encapsules sur le segment, mais pas de bout en bout. Enfin ZigBee et Thread implémentent leur propre couche de chiffrement indépendamment de la couche physique, ce qui permet de se détacher, théoriquement de la couche physique.[8]

Troisième défi : l'accessibilité, une topologie en étoile est appréciée dans la plupart des réseaux domestiques, le principale protocole utilise dans un tel contexte étant le Wifi, cependant dans le monde de l'IoT, elle n'est pas idéale. Partant du principe que la consommation énergétique doit rester la plus basse possible pour la plupart des protocoles de l'IoT, comme vu précédemment, un compromis doit être fait en matière de débit et/ou de portée. Au contraire, les réseaux type Wi-Fi sont, du fait de leur topologie en étoile, contraints d'avoir un routeur central qui se chargera de relayer toutes les communications du réseau, ce qui oblige à avoir une portée suffisante pour atteindre tous les objets de la maison, et par conséquent, demande une consommation électrique relativement élevée. Pour pallier ce problème, et partant du principe que les objets connectés sont omniprésents dans une maison, les topologies maillées sont adaptées, puisqu'elles permettent d'avoir des objets prenant le rôle de relais, idéalement

place sa courte distance d'autres objets. Ainsi, deux objets positionner aux extrêmes opposes d'une maison peuvent communiquer entre eux en utilisant des objets intermédiaires comme relais. Ce mécanisme nécessite une courte distance entre chaque objet intermédiaire, et permet donc de conserver un débit correct sans impacter la consommation d'énergie. De telles topologies sont employées par les protocoles ZigBee, Thread et Z-Wave. Dans une certaine mesure, Bluetooth peut aussi être inclus dans cette catégorie grâce à sa topologie scatternet qui est très proche d'un réseau maille à ceci près qu'elle nécessite des nœuds maıtres et esclaves, ce qui n'est pas le cas des réseaux mailles purs.[8]

Quatrième défis : la standardisation. Il existe plusieurs normes standards, dont principalement ceux citées ici :

IEEE 802.3 concerne les réseaux câblés dont Ethernet ;

IEEE 802.11 concerne les WLAN (Wireless Local Area Network) ou réseaux sans- locaux dont principalement le Wi-Fi ;

IEEE 802.15.1 concerne les WPAN (Wireless Personal Area Network) ou réseaux sans-fil personnels et est dédié à Bluetooth ;

IEEE 802.15.4 concerne les LR WPAN (Low Rate WPAN) ou réseaux sans-fil personnels a bas débit comme ZigBee, Thread et 6LoWPAN;

IEEE 802.15.7 concerne les réseaux optiques comme Li-Fi ;

ISO/IEC 14443 concerne les carte a circuits intégrés sans contact comme NFC et RFID ;

ISO/IEC 14543-3-10 concerne les composants optimisés pour la récolte d'énergie.

Standards IETF (RFC) Une grande quantité de protocoles utilisés par l'Internet des objets sont standardisées par l'IETF. On peut citer IP (v4 et v6), 6LoWPAN, TCP, UDP, TLS, HTTP ou encore COAP.

Cependant, certains protocoles comme KNX, Z-Wave, LoRaWAN/LoRa ou SigFox choisissent de ne pas utiliser ces standards. Ceci a pour effet de rendre les protocoles de l'IoT relativement hétérogènes. Fort de ces caractéristiques, un fabricant doit alors choisir ses critères de sélection. Différentes stratégies s'ornent a lui mais, dans le cadre des maisons intelligentes, il ne pourra pas échapper à une poignée de protocoles : Wi-Fi/Ethernet du fait de la présence d'un box Internet et 3G/4G s'il veut que l'utilisateur de son produit puisse accéder à ses objets de l'extérieur, lorsque son smartphone n'a pas d'accès Wi-Fi. Par-dessus cela, il peut en revanche utiliser d'autres protocoles, sélectionnés en fonction de leur consommation, sécurité, accessibilité et standardisation. Du fait de la popularité de certains d'entre eux, un fabricant peut choisir de sacrifier certains critères au profit d'un protocole qui lui permettra d'avoir accès à plus d'objets connectés .[8]

2.3 Quelques Protocoles et leurs comportement dans les couches du modèle 0SI

Pour comprendre la confusion que peut amener la myriade de protocoles dont fait usage l'Internet des Objets (IoT), nous allons dresser des tableaux qui nous montrent l'étendue des principaux protocoles sur les différentes couches du modèle OSI. Avec les couches du modèle OSI on constate plusieurs choses. D'abord, certains protocoles sont des alternatives l'un de l'autre, comme COAP et MQTT. D'autres sont des alternatives mais dont l'étendue est différentes comme ZigBee et Thread qui utilisent tous les deux la même base IEEE 802.15.4, mais ou ZigBee s'étend jusqu'à la couche application. Thread implémente également les protocoles DTLS, UDP et 6LoWPAN Thread implémente également les protocoles DTLS, UDP et 6LoWPAN. On constate aussi que certains protocoles gèrent toutes les couches, comme Bluetooth, Z-Wave, etc., tandis que d'autres n'implémentent que la couche physique comme SigFox, ou encore, en étendant à la couche de liaison, comme Li-Fi, Wi-Fi et 3G/4G/5G, ou jusqu'à la couche présentation comme LoRaWAN/LoRa. KNX est aussi à part puisqu'il est capable de supporter plusieurs couches physiques, dont Ethernet. [8]

Tableau 2: Tableau des protocoles capables de communiquer destiné à une utilisation locale.

<table>
<tr><th>Couches du modèle OSI</th><th colspan="7">Protocoles</th></tr>
<tr><td>Application</td><td rowspan="6">BT/BLE (1999/ 2009)</td><td rowspan="6">Z-Wave (2016*)</td><td rowspan="5">KNX (2002)</td><td colspan="3"></td><td rowspan="4"></td><td rowspan="3"></td></tr>
<tr><td>Présentation</td><td rowspan="4">NFC (2003)</td><td rowspan="4">RFID (1983)</td><td rowspan="3">LoRaWAN (2015)</td></tr>
<tr><td>Session</td></tr>
<tr><td>Transport</td></tr>
<tr><td>Réseau</td><td rowspan="2">EnOcean (2012)</td></tr>
<tr><td>Liaison</td><td rowspan="2"></td><td rowspan="2">LoRa (2015)</td><td rowspan="2">Sigfox (2019*)</td></tr>
<tr><td>Physique</td></tr>
</table>

Nb : ce tableau montre l'étendue de divers protocoles sur les couches du modèle OSI. Cette fois, les protocoles listés sont destinés à une utilisation locale. Ils devront donc procéder à un changement de protocole pour pouvoir communiquer sur Internet. KNX est particulier car il supporte plusieurs couches physiques, dont Ethernet. Les protocoles sont ici calqués sur le modèle OSI, bien que ce modèle ne soit pas réellement adapté à ces protocoles.

2.4 Etendues de protocoles et couche du modèle 0SI

Nous allons dans un tableau montrer l'étendue de divers protocoles sur les couches du modèle OSI. Les protocoles listés sont capables de communiquer directement sur Internet, sans procéder à un changement de protocole. Les dates mises entre parenthèses sont les dates des premières spécifications des protocoles. Un symbole environ est ajouté quand aucune date fiable n'a été trouvée. Li-Fi est en cage gris claire pour indiquer que son placement est une suggestion, son usage futur n'étant pas encore établi concrètement. Les flèches indiquent que le protocole Thread implémente 6LoWPAN, UDP et DTLS. ZigBee a également développe un équivalent d'IP (ZigBee IP), mais ce dernier est très peu adopté et n'est donc pas montré ici.

Par suite On constate aussi que certains protocoles gèrent toutes les couches, comme Bluetooth, Z-Wave, etc., tandis que d'autres n'implémentent que la couche physique comme SigFox, ou encore, en étendant à la couche de liaison, comme Li-Fi, Wi-Fi et 3G/4G/5G, ou jusqu'à la couche présentation comme LoRaWAN/LoRa. KNX est aussi à part puisqu'il est capable de supporter plusieurs couches physiques, dont Ethernet (voir tableau 3).[8]

Tableau 3:Tableau des protocoles capables de communiquer directement sur internet sans changement de protocoles.

<table>
<tr><th>Couches du modèle OSI</th><th colspan="6">Protocoles</th></tr>
<tr><td>Application</td><td>HTTP/S
(1996/2000)</td><td>MQTT
(1999)</td><td>CoAP
(2014)</td><td></td><td rowspan="3">Thread
(2014)</td><td rowspan="3">ZigBee
(2003)</td></tr>
<tr><td>Présentation
Session</td><td colspan="2" rowspan="2"></td><td>TLS
(1999)</td><td></td><td>DTLS
(2006)</td></tr>
<tr><td>Transport</td><td colspan="4">TCP et UDP
(1974) (1980)</td></tr>
<tr><td>Réseau</td><td colspan="3">IPv4 et IPv6
(1981) (1995)</td><td>6LoWPAN
(2007)</td><td colspan="2"></td></tr>
<tr><td>Liaison</td><td colspan="2">MAC
(?)</td><td rowspan="2">3G/4G/5G
(1998/2008/2020)</td><td rowspan="2">Li-Fi
(2020)</td><td colspan="2" rowspan="2">LR-WPAN
(IEEE 802.15.4)
(2003)</td></tr>
<tr><td>Physique</td><td>Wi-Fi
(1999)</td><td>Ethernet
(1983)</td></tr>
</table>

Conclusion

Dans ce chapitre qui parle de l'Architecture des objets connectés, nous avons présenté de manière générale l'architecture de l'écosystème IOT tout en décrivant ses particularités. Nous avons eu aussi à relater quelques problèmes liés à la sécurité et quelques protocoles et leurs comportements avec les couches du modèles OSI.

Dans le prochain chapitre nous allons nous concentrer sur l'étude des technologies de communication dans l'Internet des objets.

CHAPITRE 3 : Technologies de communication dans l'Internet des objets.

Introduction

Dans le domaine des réseaux sans fil et filaires, un protocole de communication définit les règles et les procédures des couches physique.IL permet ainsi de connecter un objet a un réseau filaire ou sans fil.

Cependant un réseau sans fil est comme son nom l'indique un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire.

Nous allons dans la suite de ce chapitre étudier le type de réseaux sans fil selon la portée et le débit.

1 Les réseaux sans fil courte portée, faible débit

Les réseaux sans fil à courte portée (distance maximale à laquelle un récepteur est capable de décoder le signal), et faible débit sont les réseaux dans lesquels la portée des technologies est faible voir des centaines de mètres et un débit pouvant plus ou moins atteindre 100kb/s [13]. Nous pouvons citer quelque protocoles et technologies que nous allons étudier dans la suite tel que Z-Wave, ZigBee, NFC, RFID.

1.1 Le RFID

La RFID, pour "Radio Frequency Idendification", est une technologie permettant de mémoriser, stocker, enregistrer des données sur un support et de les récupérer à distance. Elle existe depuis les années 1940 et servait, à l'époque, à identifier les avions de guerre entrant dans l'espace aérien du Royaume-Uni afin de les distinguer. D'abord utilisée par l'armée, la RFID s'est répandue dans différents secteurs industriels à partir des années 1980, de l'agroalimentaire à la santé, en passant par les transports.

Les étiquettes RFID, qui peuvent aussi prendre la forme de balises ou de tags, sont composées d'une puce RFID et d'une antenne et sont collées sur un produit. Elles enregistrent les données et un lecteur électromagnétique lit ensuite les ondes radio présentes sur la puce RFID grâce à l'antenne.

La RFID est un système de traçabilité. Grâce à une seule puce RFID, il est possible de tracer les produits pendant tout le processus de production, de transport et de distribution, voire même jusqu'à leur fin de vie [14].

1.2 Le protocole Z-Wave

Z-WAVE est un protocole en réseau maillée, qui a une portée courte de 30m et un débit maximale de 100 kb/s.il est adapté aux objets alimenter par batterie et communiquant à bas debit.il est un peu complexe du fait qu'il a des besoins et des appareils qui lui sont spécifiques.

1.3 Le protocole Thread

Thread est un protocole en réseau maillée utilisant 6LoWPAN, ce qui lui permet de se comporter comme un nœud normal dans un réseau local grâce au protocole IP. Tout protocole basé sur IP peut donc être utilisé par Thread. Il a été conçu pour qu'un utilisateur puisse utiliser, entre autres, son smartphone afin de connecter simplement un objet au réseau. Dans ce genre de réseau, certains nœuds vont prendre le rôle de routeur a fin de relayer les paquets jusqu'à internet grâce à une interface Wi-Fi ou Ethernet[8].

1.4 ZigBee

ZigBee est un protocole en réseau maillé basé sur IEEE 802.15.4 similaire à Thread, à ceci près qu'il n'utilise pas 6LoWPAN et, par conséquent, ne peut pas utiliser IP, bien que certains travaux aient été faits dans ce sens. D'autres travaux sont également en cours dans le but de pouvoir interconnecter ZigBee et Thread. L'absence d'IP fait que ZigBee implémente ses propres mécanismes de routage. ZigBee définit une couche application supplémentaire par rapport à Thread qui peut être avantageuse lors de l'utilisation de systèmes d'éclairage mais d'désavantageuse dans d'autres cas.[8]

2 Les réseaux sans fil courte portée, haut débit

Les réseaux sans fil à courte portée et haut débit sont les réseaux dans lesquels les protocoles lui appartenant peuvent avoir une portée allant de 0 à des centaines de mètres et un débit allant de 100 à des mégabits/s [13]. On peut citer quelque technologies que nous allons étudier dans la suite tel que le Bluetooth, le Li-Fi, le wifi…

2.1 Le Bluetooth

Le Bluetooth définit un standard de communication développé en 1994 par le fabricant suédois Ericsson. Cette technologie, basée sur l'utilisation d'ondes radio UHF, permet une connexion entre plusieurs périphériques et l'échange bidirectionnel de données et de fichiers sur une très courte distance. Il fonctionne sur les fréquences comprises entre 2.4 GHz et 2.483 GHz. Le principal avantage du Bluetooth réside dans le fait de pouvoir réaliser une connexion entre deux appareils sans aucune liaison filaire. C'est une version basse consommation, elle est destinée aux paquets de petite taille. Il permet uniquement la transmission de paquets locaux et n'est pas destiné à la transmission de paquets sur Internet. Le Bluetooth se sert des ondes radio sur la

bande de fréquences 2,4 GHz. Pour qu'un appareil fonctionne en Bluetooth, il doit disposer d'un logiciel de gestion de transfert de données adéquat ainsi que d'une puce Bluetooth disposant d'une unité émettrice et réceptrice. Chaque appareil possède une adresse et émet ses signaux. C'est à l'utilisateur de les rendre visibles en activant le Bluetooth sur ces appareils afin d'autoriser une communication entre eux. Dès que les signaux se croisent, ils vérifient leurs adresses respectives lors de l'appairage et se connectent pour le transfert de données [14].

2.2 La technologie Li-Fi

La technologie Li-Fi est une technologie de communication sans fil basée sur l'utilisation de la lumière visible, de longueur d'onde comprise entre 480 nm (670 THz, bleu-vert) et 650 nm (460 THz, orange-rouge). Le principe du Li-Fi repose sur le codage et l'envoi de données via la modulation d'amplitude des sources de lumière (scintillation imperceptible à l'œil), selon un protocole bien défini et standardisé. Le Li-Fi présente de nombreux avantages qui proviennent d'une part de l'utilisation de la lumière et d'autre part de l'utilisation de LED : Le spectre de la lumière couvre une bande fréquentielle d'environ 300 THz. L'utilisation de cette bande est gratuite et n'est pas régulée [14].

Un système Li-Fi est composé de deux blocs principaux : un bloc d'émission et un bloc de réception entre lesquels s'intercale le canal optique. Le cheminement des données à transmettre est alors le suivant :

Les données numériques à transmettre sont d'abord encodées pour rendre la transmission plus robuste aux dégradations causées par le canal optique. Ces données codées, alors sous forme de signal électrique sont converties en signal lumineux grâce à un circuit électronique pilotant une ou plusieurs LED. Plus précisément, ce circuit électronique permet de faire varier l'intensité lumineuse des LED en fonction des données à transmettre. La modulation utilisée est donc une modulation d'intensité, dont l'exemple le plus simple est la modulation On-Off Keying (OOK) où des 0 et des 1 logiques sont transmis, par exemple selon le codage Manchester.

La lumière émise se propage ensuite dans l'environnement et subit des déformations dues par exemple aux obstacles, aux conditions météorologiques... Cet environnement et les déformations associées sont regroupés sous le terme de canal optique. Le signal lumineux déformé est enfin reçu par un photorécepteur (photodiode, caméra…) qui le convertit en courant électrique. Le signal électrique résultant est traité puis démodulé et décodé pour récupérer les données transmises. Dans la pratique, les modules d'émission et de réception peuvent être équipés de dispositifs optiques (lentilles, miroirs, filtres...) permettant d'améliorer la qualité de la transmission de données [15].

2.3 Le Wifi

Le Wi-Fi est un ensemble de fréquences radio qui élimine les câbles, partage une connexion Internet et permet l'échange de données entre plusieurs postes. Il est une technologie intéressante et est régis par les normes IEEE 802.11 qui spécifient l'interopérabilité entre des équipements conformes à ces normes. Le Wi-Fi permet ainsi de créer des réseaux locaux haut débit ou WLAN (Wireless Local Area Network) pour faire communiquer des dispositifs entre eux (routeurs, modems, smartphones).pour de nombreuses sociétés liées au monde des télécoms et d'Internet. Les collectivités locales et surtout les particuliers profitent de la facilité d'accès à Internet haut débit liée à cette norme. Dans sa déclinaison la plus connue, 802.11 b, le Wi-Fi utilise la bande de fréquence de 2,4 GHz et atteint un débit théorique de 11 Mbits/s (contre 128, 512 Kbits/s ou 1 Mbits/s pour l'ADSL), le 802.11a culmine à 22 Mbits/s et le 802.11 g, enfin, flirte avec les 54 Mbits/s.

La technologie Wi-Fi, qui est donc normée, a vu ses caractéristiques et débits évoluer au fil du temps et des usages. Chaque norme Wi-Fi ayant l'identifiant 802.11 est suivi d'une lettre exprimant sa génération. Aujourd'hui, on considère que les normes 802.11 a/b/g sont quelques peu dépassées. Depuis ses origines en 1997, les normes Wi-Fi se sont succédé pour laisser place tout récemment, fin 2019 à la norme Wi-Fi 6E (802.11ax) [16].

3 Les réseaux sans fil longue portée et faible débit

Ce type de réseau on observe que le signal d'émission de donnée (distance maximale à laquelle un récepteur est capable de décoder le signal) varie de 100metres à des dizaines de km, et le débit de 0 à des dizaines de kb/s. C'est le cas des protocoles Sigfox LoRaWAN et Nb-IoT que nous allons voir dans la suite.

3.1 Le protocole SigFox

SigFox est un opérateur réseau proposant leur réseau du même nom. Par le biais de partenariat avec d'autres entreprises de télécommunication, Sigfox déploie son réseau à travers les pays qui ont adopté la technologie. Sa création a donné lieu au premier opérateur dédié à l'internet des objets. Pour cela, l'entreprise a développé et mis en œuvre la technologie UNB (Ultra Narrow Band). Par définition, les systèmes UNB occupent une très petite partie du spectre pour la transmission d'un signal. Cette largeur de bande (typiquement quelques centaines de Hz) est très petite devant la bande passante du canal. Le premier système de ce type, basé sur la modulation VMSK (Very Minimum Shift Keying), a été proposé en 2004. L'objectif était de compresser la transmission de la donnée dans une bande la plus petite possible. Cependant, en

pratique, cette technique n'a pas permis d'atteindre la très faible occupation annoncée et SigFox a proposé une autre approche, propriétaire.[9]

Architecture du Réseau Sigfox

L'architecture du réseau Sigfox comprend des appareils, des stations de base et un cœur de réseau (Figure 10).Les appareils (par exemple, les capteurs ou les actionneurs) sont fournis avec une connectivité sans fil via la base voisine gares. Un appareil n'est pas lié à une station de base particulière. Par conséquent, la signalisation d'association n'est pas nécessaire. Les stations de base sont connectées via l'Internet public avec un seul cœur basé sur le Cloud réseau. Cette approche évite les procédures de transfert pour prendre en charge la mobilité des appareils. Le cœur de réseau est composé du Centre de services et de l'Autorité d'enregistrement. Le centre de service contrôle et gère les stations de base et les appareils. L'Autorité d'Enregistrement est chargée d'autoriser l'accès au réseau des appareils. Les applications peuvent interagir avec les données collectées par les appareils, et avec appareils eux-mêmes, via une interface Web et un certain nombre d'interfaces de programme d'application (API).

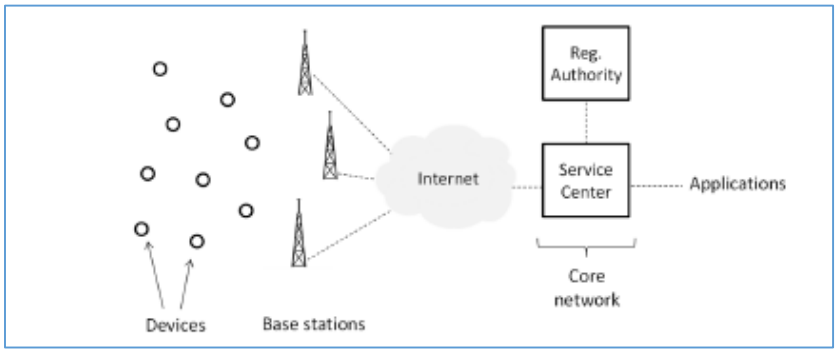


Figure 10:Architecture du réseau de Sigfox

L'interface radio de Sigfox

Sigfox prend en charge la communication unidirectionnelle et bidirectionnelle sur un spectre sans licence. Dans l'Europe, les bandes 868,00 MHz-868,60 MHz et 869,40 MHz à 869,65 MHz sont utilisées pour la liaison montante et transmission descendante, respectivement. . Afin d'obtenir une longue portée de liaison, tout en limitant la puissance d'émission, Sigfox utilise la radio à bande ultra étroite (UNB) transmission pour la liaison montante et la liaison descendante. La bande passante d'un canal de liaison montante dépend de la région (par exemple, c'est 100 Hz en Europe et 600 Hz aux États-Unis), tandis que le canal de liaison descendante de la bande passante est de 1,5 kHz. La puissance d'émission maximale de la liaison montante est de 25 mW en Europe (158 mW dans les États-Unis), alors que la puissance

d'émission maximale en liaison descendante est de 500 mW en Europe (4Win aux États-Unis).Les modulations utilisées pour la liaison montante et la liaison descendante sont la modulation par décalage de phase binaire différentielle (DBPSK) et la modulation par déplacement de fréquence gaussien (GFSK), respectivement. DBPSK est plus efficace en bande passante que GFSK, qui favorise une portée de liaison montante accrue (compensant la puissance d'émission plus faible autorisée dans la bande montante). De plus, DBPSK offre une bonne protection contre les interférences (par exemple, le brouillage), la puissance reçue se concentre alors dans une bande passante très étroite et atteint une puissance reçue élevée niveau. Le débit binaire de la couche physique de liaison montante est de 100 bit/s (en Europe) ou 600 bit/s (aux États-Unis) alors que le débit binaire de la couche physique de liaison descendante est de 600 bit/s dans le monde. Afin de se conformer à la réglementation sur l'utilisation du spectre, le système permet généralement jusqu'à 140 messages de liaison montante et quatre messages de liaison descendante par jour. Ces contraintes de débit de messages peuvent être assouplies en fonction du domaine d'exploitation réglementaire spécifique et sur les conditions du système.

Sigfox définit les formats de trame physique pour la transmission de messages en liaison montante et descendante (voir Figure 11). Les tailles minimales de trame de liaison montante et descendante sont de 14 octets.[10]

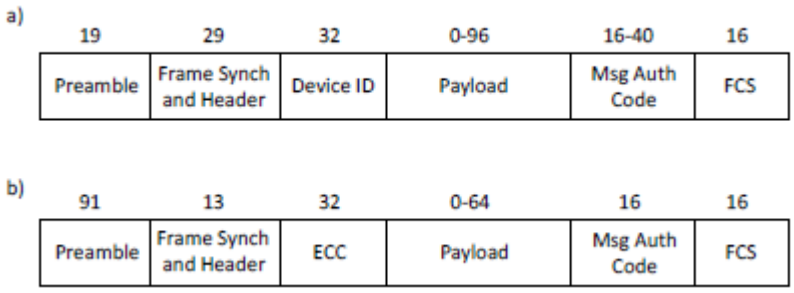


Figure 11:Format de trame SigFox

NB : dans la figure ci-dessus le (a) représente la liaison montante et le (b) liaison descendante. Toutes les tailles de champ de trame sont exprimées en morceaux. Le troisième champ d'en-tête de trame en partant de la gauche est le Device Identifier (Device ID) ou le Code de correction d'erreur (ECC), pour les formats de trame de liaison montante et de liaison descendante, respectivement. Les deux champs de trame les plus à droite sont un code d'authentification de message (code d'authentification message) et un contrôle de trame.

L'échange de donnée.

Dans l'échange de donnée de Sigfox la communication est asynchrone et initiée par l'appareil, ce qui lui permet de rester en état de veille par défaut et minimiser sa consommation d'énergie. Une transmission de message en liaison montante peut être reçu par plusieurs stations de base (en moyenne, par trois stations de base), permettant la coopération réception et diversité spatiale. Cette approche prend naturellement en charge la mobilité des appareils. Sigfox définit deux types d'échanges de messages : les transactions unidirectionnelles et bidirectionnelles (Figure 12). Dans le premier, l'appareil transmet une trame de liaison montante via une fréquence choisie au hasard canal, puis transmet deux répliques exactes de cette trame, en utilisant d'autres canaux de fréquence aléatoire à des intervalles de temps différents. Cette fonction offre une diversité de fréquence et de temps, ce qui contribue à la robustesse de la communication en présence de problèmes tels que l'évanouissement par trajets multiples, les interférences, etc..., dans les transactions unidirectionnelles, il n'y a pas de réponse à la transmission de trame de liaison montante. Par conséquent, les transactions unidirectionnelles ne sont pas confirmées. Dans les transactions bidirectionnelles, un message de liaison montante est d'abord transmis par le dispositif en utilisant la même procédure que dans les transactions unidirectionnelles (c'est-à-dire, une première trame montante est suivie de deux répliques dans des canaux de fréquence différents). Au bout d'un certain temps, noté TDL_WIN_START, depuis la fin de la première transmission de trame montante, l'appareil initie une réception fenêtre, de durée maximale notée TDL_WIN_MAX, destinée à permettre la réception d'une liaison descendante trame envoyée par une station de base. La trame de liaison descendante peut transporter des données d'application réelles pour le dispositif et, en même temps, il peut également servir d'accusé de réception pour la trame montante. Après réception du message de liaison descendante, une confirmation de liaison montante est envoyée par l'appareil après le temps T_{ack}. A noter qu'en revanche avec d'autres technologies, les retransmissions dues à l'absence de retour de l'autre point d'extrémité d'un lien n'existent pas dans Sigfox.[10]

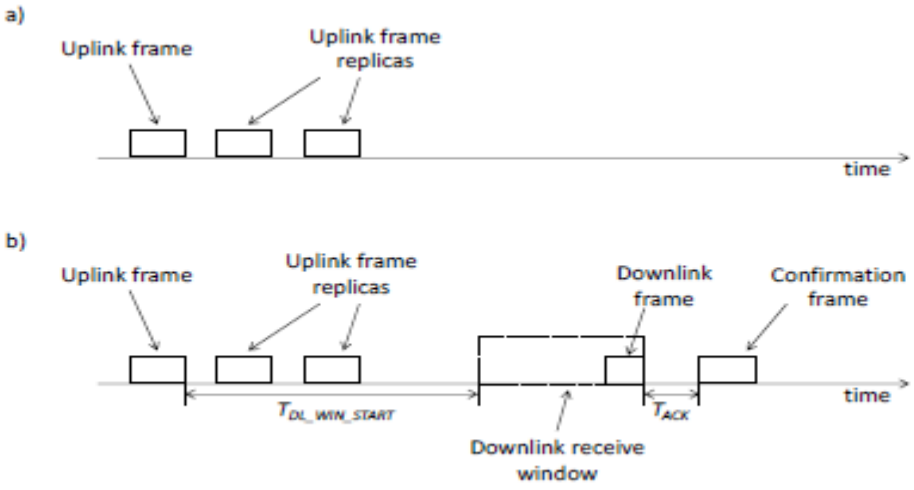


Figure 12:la transaction Unidirectionnelle(a) et la transaction bidirectionnelle(b).

3.2 Le protocole LoRaWAN

Comme son nom l'indique LoRaWAN (Low range wide area network), il s'agit d'un réseau sans fil à basse consommation. Le LPWAN est un réseau à longue portée et à bas débit, comparé aux réseaux cellulaires où le débit est élevé. Là où le LPWAN se démarque, c'est qu'il permet d'augmenter l'autonomie d'un appareil déployé, qui n'est pas possible avec un réseau cellulaire qui consomme plus d'énergie. Elle convient donc aux appareils ne nécessitant pas d'envoyer de grande quantité de données et à longue portée. Ces appareils peuvent ainsi rester actifs bien plus longtemps. Le LPWAN permet ainsi de réduire les coûts avec des appareils plus optimisés. Comme on peut le voir sur la figure 13 ci-dessous, les technologies comme le Bluetooth ou le NFC ne permettent pas d'avoir une grande portée malgré leur basse consommation.[11]

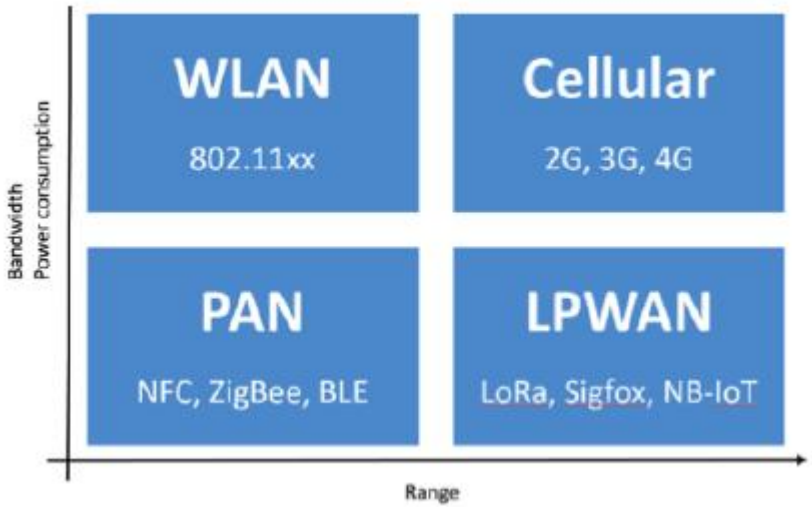


Figure 13:Différent types de réseaux sans fil selon leur portée et leur bande passante

Le réseau LoRaWAN utilise la technologie LoRa pour les communications. Il s'agit d'une technologie propriétaire développé par Semtech. Néanmoins, un réseau LoRaWAN n'est pas propriétaire et peut être déployé librement comme réseau privé ou public. LoRaWAN peut être déployé partout dans le monde et permet de gérer son propre réseau sans devoir passer des réseaux externes. LoRaWAN utilise la couche physique de LoRa. Elle définit la couche de liaison du système de réseau. Chaque trame Lora contient dans son PHY payload la couche MAC LoRaWAN. Il y a deux types de message communiqué en LoRaWAN, les uplinks et les downlinks. Un uplink est un message transmis d'un appareil et un downlink est un message envoyé vers l'appareil. Cela montre qu'une communication avec un appareil n'est pas vraiment symétrique.[11]

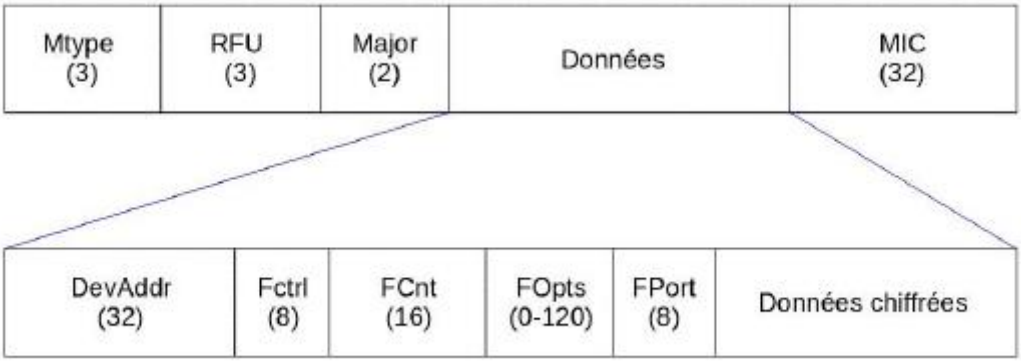


Figure 14:Trame LoRaWAN

Figure 15:Trame Ethernet

En observant une trame LoRaWAN et une trame Ethernet, on retrouve quelque similitude comme l'Adresse MAC source de l'Ethernet qui est le DevAddr dans une trame LoRaWAN et les données de la trame. LoRaWAN utilise une double encryptions dans sa trame avec les données chiffrées ainsi que le MIC (Message Integrity Control). Cela permet de compenser le manque d'adresse de destination de LoRa. En effet, un appareil LoRa transmet des messages en broadcast et n'importe quel autre appareil peut réceptionner le message. Ce double

chiffrement permet d'authentifier le destinataire qui possède les mêmes clés de chiffrement pour déchiffrer la trame LoRaWAN.

Structure d'un réseau LoRaWAN

Un réseau LoRaWAN est composé de 4 éléments principaux : les appareils LoRa, les passerelles, le Network Server (serveur réseau) et l'Application Server (serveur applicatif).

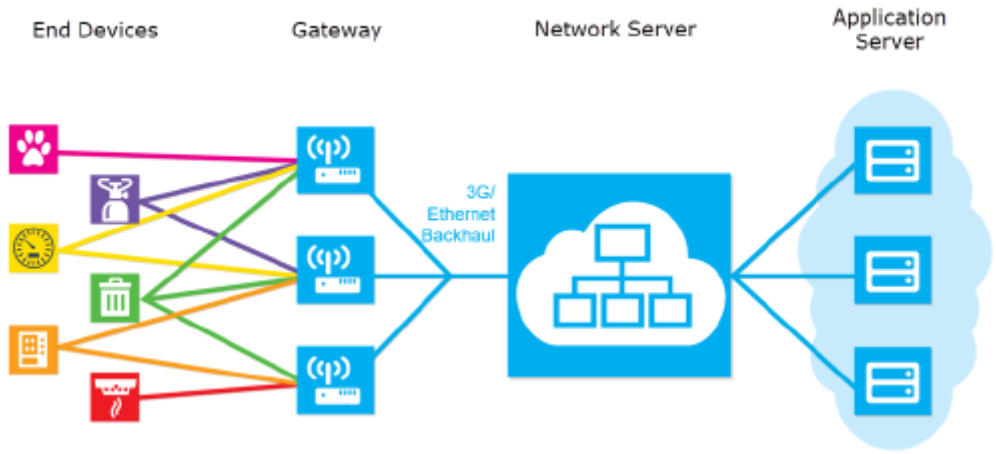


Figure 16:Architecture du réseau LoRaWAN

La passerelle, le Network Server et l'application server

- ✓ La passerelle

La passerelle joue le rôle d'intermédiaire entre le Network Server et les nœuds. Elle s'occupe de transmettre tous les paquets qu'elle reçoit des nœuds vers le Network Server auquel elle est rattachée. La communication entre une passerelle et un nœud se fait en LoRa alors qu'entre une passerelle et son Network Server, ça sera une communication par TCP/IP. La liaison peut donc être faite via Wi-Fi, Ethernet ou 4G. Il peut aussi y avoir plusieurs passerelles dans une installation de réseau LoRaWAN ce qui peut permettre d'augmenter sa portée et ainsi pouvoir placer des appareils plus loin.

Une passerelle peut tout aussi bien être un simple microcontrôleur ou un Raspberry avec un module LoRa spécifique. Ces passerelles peuvent alors communiquer via un Uplink et un Downlink s'il s'agit d'un module normalement créé pour un nœud. Des shields LoRaWAN existent pour les Raspberry leur permettant de fonctionner comme une réelle passerelle avec les 8 Uplinks maximum possible d'une passerelle. Il existe aussi des passerelles LoRaWAN proposées par Cisco, Kerlink.[11]

- ✓ Le Network Server

Le Network Server peut être vu comme le cœur du réseau LoRaWAN. Il trie les paquets reçus des passerelles en supprimant les doublons dans le cas où d'autres passerelles LoRa du même réseau transfèrent le paquet. Il décode aussi ces paquets avec les clés à sa connaissance des appareils de son réseau. Lorsqu'une trame arrive d'un appareil configuré pour un autre réseau LoRaWAN, ce dernier ne peut être décodé car les clés d'authentifications ne correspondent pas avec ceux du Network Server. Les nœuds LoRa sont authentifiés par le Network Server grâce à une clé AES 128bits. [11]

Le Network Server peut se trouver dans notre propre réseau interne ou dans le Cloud en étant hébergé. Les passerelles doivent connaitre l'adresse IP du Network Server pour transférer le message. De son côté, le Network Server détermine l'adresse IP de ses passerelles après avoir reçu leur message.

- ✓ L'application Server

L'application gère les données transmises des nœuds et fait le lien entre le client et le serveur. C'est à travers l'Application Server que l'utilisateur peut interagir avec ses appareils. Il pourra y récolter les données envoyées des appareils ou leur transmettre des commandes.[11]

La technologie LoRa

Long Range ou LoRa dans son diminutif est un protocole de liaison sans fil à faible consommation développé par l'entreprise Semtech. LoRa utilise une modulation qui permet une communication à longue portée entre des appareils pourvus de ce protocole pouvant aller à plusieurs kilomètres. LoRa est la communication entre deux nœuds LoRa ou un nœud LoRa et une passerelle. LoRaWAN est l'architecture permettant à des nœuds de communiquer avec un serveur LoRaWAN. Le nœud utilise le protocole LoRa pour le type de modulation. Si nous nous basons sur le modèle OSI, nous pouvons donc observer que LoRa correspond à la couche physique et LoRaWAN à la couche de liaison de données.

LoRa utilise des fréquences libres de transmissions qui sont différentes selon les régions du monde tournant autour de 868MHz et 433MHz. Le type de signal radio émis est l'étalement de spectre sous la forme d'un Compressed High Intensity Radar Pulse (CHIRP). Cette modulation est composée de deux paramètres supplémentaires pour définir la transmission. En premier lieu, il y a la largeur de la bande passante. LoRa utilise des largeurs de bandes passantes à 125kHz, 250kHz et 500kHz. Le second paramètre est le Spreading Factor (SF) ou le facteur d'étalement

du spectre. Le paramètre de facteur va de 7 à 12. Un SF élevé permet d'envoyer à plus longue portée, mais en échange le débit envoyé est bien plus faible. Avec un SF élevé, les données envoyées devront alors avoir une taille plus faible et le récepteur aura plus de possibilité de capter le message. Il est donc important de déterminer quel type de SF nous voulons utiliser selon la situation donnée. Dans le cas d'appareils LoRa qui se trouvent à plusieurs kilomètres de distance, il convient par exemple d'utiliser un SF élevé pour éviter des pertes de paquets. Le temps de transmissions est aussi plus grand.

Les appareils LoRa

Les appareils sont les dispositifs que l'on peut mettre en place dans le réseau LoRaWAN. Il peut s'agir de senseur thermique, de système de traçage ou encore des systèmes d'alarme. Ces appareils doivent être pourvus d'antenne LoRa, sans laquelle il leur est impossible de communiquer. Il peut y avoir un ou plusieurs appareils dans un même réseau. Il existe trois catégories d'appareils LoRa. Elles dépendent principalement de leur temps d'activité et d'écoute via leur radio LoRa. Le choix des appareils selon la situation nécessaire peut être envisagé en ciblant les classes d'appareils.[11]

- ✓ Classe A

Un appareil de classe A est la catégorie principale des dispositifs. En effet, chaque appareil est au moins de classe A pour pouvoir fonctionner en LoRa. Dans le cas de transmission d'informations d'une classe A vers un autre appareil ou passerelle LoRa, le transmetteur peut recevoir un retour du récepteur durant un certain délai. Hors de ce délai, le transmetteur ne recevra pas de retour et les messages retours seront ignorés.

- ✓ Classe B

L'appareil de classe B utilise le même principe que la classe A et il ajoute une fonctionnalité en plus qui est la réception périodique de message venant d'une passerelle. Cela fait qu'entre les envois de trames de l'appareil de classe B, ce dernier peut recevoir durant son temps de pause des Downlinks à intervalle régulier.

- ✓ Classe C

Un appareil de classe C est en écoute constante sur leur fréquence entre les envois qu'il fait. Cela permet d'envoyer un message en tout temps à l'appareil depuis un serveur. L'appareil en revanche aura une autonomie sur batterie nettement moindre comme il sera constamment actif.

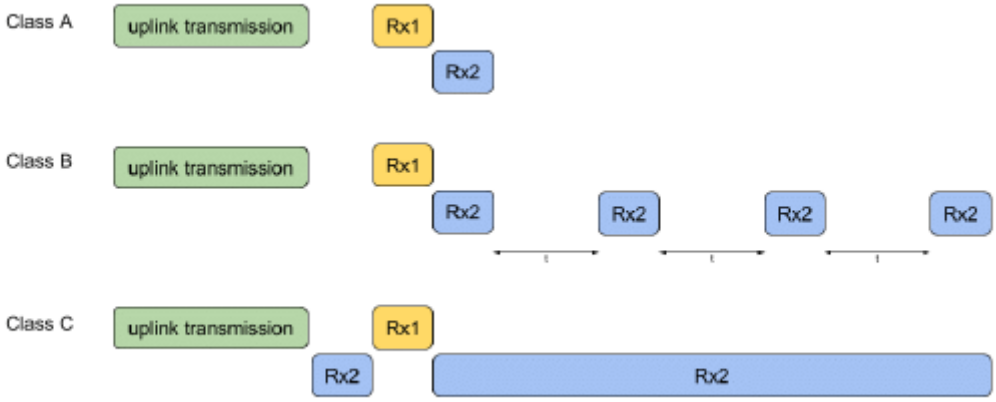


Figure 17:Classes d'appareil LoRa

3.3 Le protocole Nb-IoT

Arrivé sur le marché bien plus tard que les technologies précédemment décrites, NB-IoT a été proposé par l'organisme de standardisation 3GPP dans sa version 13 (*3rd Generation Partnership Project, Release 13)* comme une extension de LTE en juin 2016 .Il s'agit d'un standard qui sera utilisé par des opérateurs déjà existants (Orange ou Free en France…) sur des bandes de fréquences règlementées. À ce jour, le réseau est opérationnel dans plusieurs pays d'Europe, ainsi qu'au Brésil, en Chine et aux États-Unis. Ce standard est basé sur une forte réutilisation des technologies maitrisées dans les précédentes versions du standard 4G, autant au niveau des terminaux que du réseau d'infrastructure des opérateurs. [12]

Structure de trame et unité de ressource dans NB-IOT.

Les communications NB-IoT s'inscrivent dans le cadre des communications LTE. Les allocations LTE sont définies en fonction d'unités de ressources, qui seront décrites dans cette section.

Décrivons dans un premier temps le découpage fréquentiel utilisé tel que standardisé pour les communications NB-IoT. Le schéma d'accès utilisé pour les transmissions LTE montantes, c'est-à-dire des terminaux aux stations sol est le schéma dit single-carrier FDMA, ou SC-FDMA (de l'anglais *Single-Carrier Fréquence Division Multiple Access*). Celui-ci repose sur l'utilisation de plusieurs sous-porteuses, qui seront utilisées conjointement pour la transmission des données. Ces sous-porteuses sont d'une largeur de 15 kHz. Les allocations accordées par la station sol sont décrites par le nombre de sous-porteuses utilisées. Dans le cadre des communications LTE pour les terminaux non NB-IoT, la bande LTE entière peut être d'une largeur allant jusqu'à 20 MHz. Les allocations fréquentielles sont des multiples de 180 kHz,

soit 12 sous-porteuses de 15 kHz, ce qui correspond à la taille minimale d'un bloc de ressource physique (PRB, de l'anglais *Physical Resource Block*).

Cependant, dans le but d'améliorer le bilan de liaison pour fournir un service aux terminaux en bordure de couverture, les communications NB-IoT utilisent une structure fréquentielle différente, permettant d'utiliser sur le lien montant un nombre de sous porteuses inférieur ou égal à 12. La bande fréquentielle allouée aux terminaux NB-IoT est d'une largeur de 180 kHz. Cette valeur est héritée du standard relatif aux terminaux LTE classiques, correspondant à la valeur d'un PRB.

Intéressons-nous maintenant au découpage temporel des communications NB-IoT. Celui-ci est hérité des communications LTE à fort débit, qui fonctionnent de manière synchrone : un tramage est mis en place afin de définir la durée des allocations. La trame LTE traditionnellement utilisée par les terminaux IoT est décrite dans la figure suivante.

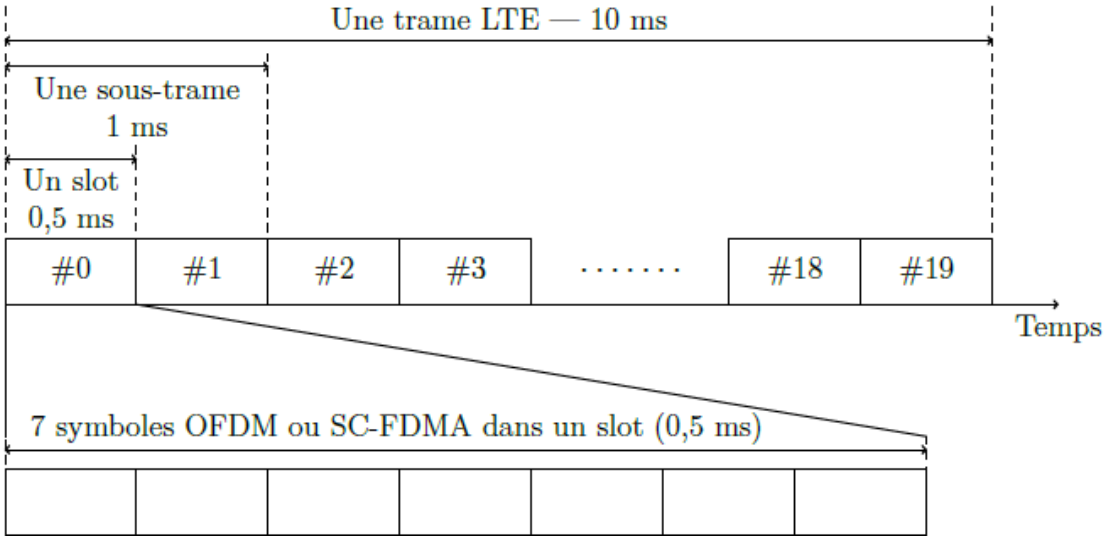


Figure 18:Representation d'une trame LTE

Notons qu'il s'agit de la structure de trame relative au mode TDD (*Time Division Duplex*). Quand la station de base LTE (aussi appelée eNB, pour *eNodeB*) reçoit des demandes d'allocation de ressource, elle peut gérer ces demandes afin de maximiser le service proposé à tous les utilisateurs. L'allocation est modulable en fonction de la charge du canal, de la qualité du lien du terminal et de la quantité d'information à transmettre. L'allocation se caractérise en partie par l'utilisation d'unités de ressources (ou RU, de l'anglais *Resource Unit*). L'unité de ressource est la plus petite allocation qu'un terminal peut recevoir. L'allocation accordée aux terminaux est alors décrite en *f*onction :

— du nombre d'unités de ressource, entre 1 et 10 ;

— de la modulation et du taux de codage, nombre de bits utiles entre 16 et 1000 ;

— du nombre de sous-porteuses utilisées, égal à 1, 3, 6 ou 12.

Le nombre d'unités de ressource et le couple modulation et taux de codage ne peuvent pas être choisis indépendamment.

NB : le tableau suivant représente un tableau comparatif des protocoles SigFox, lora et NB-IoT. Ce tableau nous montre que même s'il y'a des similitudes entre les protocoles du point de vue de la durée de vie des appareils NB-IoT se démarque par le fait qu'il est plus robuste en sécurité mais consomme aussi beaucoup plus d'énergie.

La technologie Lora présente une structure dont la communication entre objets est plus simple, elle consomme moins d'énergie et a une durée de vie des appareils qui peut atteindre plus de 10ans.

En comparant lora et SigFox, nous constatons qu'elles sont presque similaires. Par contre SigFox gère la mobilité des objets et les interférences.

Protocole	Commentaire entre périphériques finaux	Gestion de la mobilité : Handover	Largeur bande passante	Consommation d'énergie	Durée de vie des appareils	Gestion de la sécurité	Gestion des interférences
Sigfox	Les périphériques finaux de SigFox pour l'échange de données entre eux nécessitent l'intervention d'un réseau externe (internet).	oui	100Hz-600Hz pour une liaison montante. 1,5KHz pour une liaison descendante.	---	8-10ans varie en fonction de la transmission.	---	Gère les interférences
NB-IoT	La communication dans NB-IoT repose sur le FDMA de l'anglais Single-Carrier Fréquence Division Multiple Access qui repose sur l'utilisation des sous porteuses.	oui	180khz	+	10ans	+	Gère les interférences
lora	Les périphériques finaux de lora peuvent communiquer entre eux sans l'intervention d'un réseau externes	non	Peut varier Entre 125KHz et 5KHz	---	10ans ou +	---	Ne gère pas les interférences

4 Les réseaux sans fil longue portée, haut débit

Ce type de réseau concerne les réseaux qui émettent sur une grande échelle et des débits pouvant atteindre des gigabits/s c'est l'exemple du 3G, 4G, 5G.

4.1 Le réseau 3G

Le réseau 3G (appelé UMTS), est la troisième génération de réseau mobile, est certainement le plus populaire et le plus connu du grand public, puisqu'il a marqué l'avènement et l'essor des smartphones à la fin des années 2000. Les abonnés à ce réseau sont alors en mesure de surfer sur le web, d'accéder à leur courrier électronique, d'envoyer des photos et des vidéos grâce à un débit convenable de 1,9Mb/s, soit une vitesse 5 à 10 fois supérieure aux générations précédentes. Le réseau 3G fonctionne sur les bandes de fréquences 900 et 2100 Mhz. Ce réseau vous permet d'accéder à l'Internet en haut débit [14].

- Le réseau H+ ou 3G+

Avec un débit moins important que la 4G, soit 42Mb/s, mais tout de même confortable, il est alors possible d'échanger des données à une vitesse relativement rapide. Le réseau H+, fonctionnant grâce à deux bandes de fréquences UMTS, est considéré comme l'évolution du réseau mobile 3G.

4.2 Le réseau 4G

La technologie 4G commence à se démocratiser partout dans le monde, avec ce réseau mobile 4G (ou 4G LTE), les fournisseurs permettent à leurs abonnés de naviguer sur Internet avec une grande rapidité. En 2016, c'est d'ailleurs une tendance forte, puisque tous les grands noms de la téléphonie mobile en ont fait leur cheval de bataille. En effet, le 4G offre un débit maximum de 150 Mb/s et vous permet d'utiliser votre smartphone avec une excellente fluidité de navigation. Ce réseau a été déployé par les quatre grands opérateurs sur la bande de fréquences la plus puissante, celle de 800MHz, et sur les bandes 1800MHz et 2600MHz. Il vous assure ainsi un débit en réception beaucoup plus important.

- Le réseau 4G+

Le réseau 4G+, également appelé 4G LTE Advanced, est une petite évolution du réseau 4G, en permettant des débits légèrement supérieurs puisqu'ils peuvent atteindre en théorie 450 Mbit/s. Aujourd'hui, la plupart des fournisseurs proposent des forfaits 4G+ dans leurs offres, même si

souvent ils ne seront nommés que compatibles 4G : la 4G+ est bien diffusée. Elle fonctionne sur les deux fréquences 1800 Mhz et 700 Mhz et tous les smartphones commercialisés en 2022 sont compatibles avec la 4G et 4G+. Il suffit donc d'avoir un téléphone compatible avec ce réseau, une offre mobile offrant la 4G+ et se trouver dans une zone couverte par ce réseau LTE Advanced [17].

4.3 Le réseau 5G

Le réseau 5G constitue la nouvelle avancée des réseaux mobiles, puisqu'il permet à ses abonnés de profiter de l'ultra haut débit, tout en limitant la consommation d'énergie des smartphones. Son débit maximal théorique est de 1Gbit/s pour les téléchargements et 500Mbit/s pour uploader des fichiers. Aujourd'hui, le réseau 5G est en cours de déploiement dans le monde, et les premiers forfaits 5G sont apparus en décembre 2020. Pour en bénéficier, vous devez d'abord investir dans un smartphone compatible 5G mais aussi vous situer dans une zone couverte par votre opérateur. Le réseau 5G est principalement déployé sur la bande des 3,5GHz (3,4GHz-3,8GHz) qui correspond aux nouvelles fréquences 5G mais aussi sur la bande des 700MHz et 2,1 GHz (et dans quelques années sur la bande millimétrique des 26GHz).

NB : es le tableau suivant est un récapitulatif des réseaux étudier précédemment en présentant quelques details de ces derniers tel que : l'acronyme, la génération, le débit et les fréquences [14].

Tableau 4:Tableau de details portant sur les réseaux 3G, 4Get 5G.

Réseau	Débit	Fréquence	Acronyme	Génération
3G	1,9Mbit/s	1900 et 2100 MHz	UMTS	Troisième génération
3G+	42Mbit/s	1900 et 2100 MHz	HSPA+	Troisième génération
4G	150Mbit/s	800, 1800 et 2600 MHz	LTE	Quatrième génération
4G+	1Gbit/s	800, 1800 et 2600 MHz	LTE Advanced	Quatrième génération
5G	10 Gbit/s	700, 2100 et 3500 MHz	Non communiqué	Cinquième génération

5 Proposition pour un choix de réseau

Les types réseaux sans fils étudié précédemment présentent chacun des caractéristiques important pour la mise en place d'un système IoT. Cependant pour se faire, fin de choisir le réseau le plus adapté pour un système à mettre en place, il faudra considérer différents

paramètres, dont la portée, le débit, le coût de déploiement ou encore la consommation en électricité.

- Si l'**autonomie** et la **transmission fréquente de données** sont les facteurs les plus importants dans un futur système et que vous souhaitez couvrir de vastes zones, il convient de partir sur l'utilisation de réseaux sans fil à longue portée et à faible débit tel que LoRaWAN, NB-IoT ou SigFox
- Si la **nature des données** à transmettre, la **couverture de zones** sont les facteurs primordiale et que la **consommation d'énergie** ne pose pas un problème dans ce cas les réseaux sans fils à longue portée et haut débit et le plus adapté.
- Si dans le futur système IoT l'**identification** et le seul facteur important dans ce cas les réseaux sans fil à courte portée et faible débit serait adéquat.
- Si dans un système IoT **la transmission de données à proximité** est le seul caractère à prendre en compte dans ce cas les réseaux à courte portée et haut débit.

Conclusion

Avec ce chapitre portant sur les technologies de communication dans l'Internet des objets, nous avons étudié les types réseaux sans fil qui sont : les réseaux sans fil courte portée haut débit, Les réseaux sans fil longue portée haut débit, les réseaux sans fil longue portée et faible débit. Dans chaque type de réseau aussi on a apporté des exemples de protocoles qui ont aussi fait l'objet d'étude. Tous ces protocoles on chacun une grand importance mais LoRaWAN se démarque du fait qu'il permet d'augmenter l'autonomie d'un appareil déployé, qui n'est pas possible avec un réseau cellulaire qui consomme plus d'énergie. Elle convient donc aux appareils ne nécessitant pas d'envoyer de grande quantité de données et à longue portée. Ces appareils peuvent ainsi rester actifs bien plus longtemps.

Nous allons dans le chapitre suivant traiter un cas pratique dans lequel nous allons utiliser un capteur DHT11 associé au réseau LoRa.

CHAPITRE 4 : Cas pratique - Utilisation du capteur de température DHT11 avec le réseau LoRaWAN.

Introduction

La mise en place d'un système IoT nécessite des configurations à faire au préalable, nous allons dans ce chapitre avec un cas pratique faire la configuration qui permettra la réception de données à partir d'un capteur de température DHT11 et les envoyer vers un serveur de sauvegarde en utilisant la technologie LoRaWAN et expliquer le fonctionnement du système.

1 Conception du système

1.1 Analyse des besoins du système

Nous présentons, dans cette section les besoins matériels et fonctionnels du cas pratique a réaliser, les choix hardwares et softwares effectués ainsi que le fonctionnement.

1.2 Description de l'objet connecté à réaliser

Notre objectif dans ce travail est de réaliser la réception de données à partir d'un capteur vers un système de sauvegarde.

Pour la réalisation de ce système, le tableau suivant constituent les besoins matériels et logiciels:

Besoins matériels	Besoin logiciels
Capteur de température dht11	**Le logiciel arduino**
Microcontrôleur : carte Arduino UNO	**Le logiciel de sauvegarde : Things network**
Modem dragino : lps8	
fils de liaison : câbles USB de type A-B	

Nous allons utiliser pour notre cas la carte Arduino UNO. Les motivations qui nous ont incités à choisir Arduino UNO sont :

-Le prix (réduits) : les cartes Arduino sont relativement peu coûteuses comparativement aux autres plates-formes. La version UNO est la moins chère des versions du module Arduino qui peut être assemblée à la main.

- Multi plateforme : le logiciel Arduino, écrit en C, tourne sous les systèmes d'exploitation Windows, Macintosh et Linux. Tandis que la plupart des systèmes à microcontrôleurs sont limités à Windows.

-Logiciel Open Source et extensible : Le logiciel Arduino et le langage C (pour la programmation de la carte) sont publiés sous licence open source.

-Disponibilité : les cartes Arduino sont disponibles dans le marché contrairement aux autres microcontrôleurs.

1.3 Modélisation du système d'objets connectés

Dans ce qui suit, nous présentons la modélisation du système d'objets connectés, représentée par quelques diagrammes UML décrivant ainsi les vues statique et dynamique du système.

1.3.1 Diagramme de cas d'utilisation

La figure 18 représente le diagramme de cas d'utilisation décrivant les fonctionnalités du système d'objets connectés.

- Identification des cas d'utilisation : nous identifions, vis-à-vis les besoins fonctionnels cités plus haut, les cas d'utilisations suivants :

✓ Détection de la température.

✓ Envoi de données via la carte arduino dans le Cloud.

✓ Gestion, control et affichage dans le Cloud.

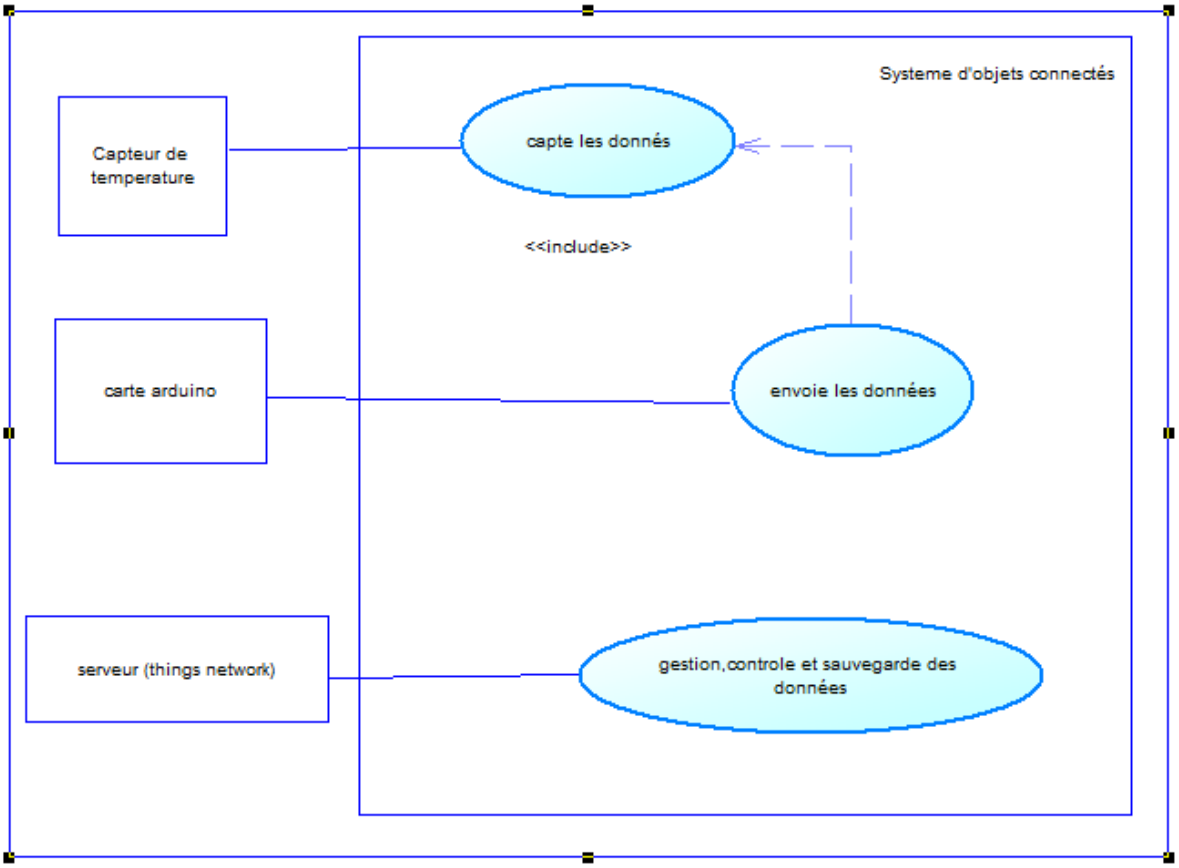


Figure 19:diagramme de cas d'utilisation

- Description textuelle

Cas d'utilisation : détection de la température

Tableau 5:description textuelle du cas d'utilisation "prélèvement de la température.

Cas d'utilisation :	détection de la température
Acteurs	Capteur température DHT11
Préconditions	Le capteur doit être capable de recueillir la température
Poste conditions :	La température est recueillie
Scénario nominal :	Le capteur récupère la température de son milieu

Cas d'utilisation : envoi des données via la carte arduino dans le Cloud

Tableau 6:description textuelle du cas d'utilisation « envoi des données via la carte arduino dans le Cloud».

Cas d'utilisation :	envoi des données via la carte arduino dans le Cloud
Acteurs	Carte Arduino
Préconditions	Le carte doit être fonctionnel et connecté à internet pour pouvoir envoyer les donnés
Poste conditions :	La carte devient fonctionnelle
Scénario nominal :	Si l'envoi n'est pas effectif la carte doit renvoyer les données

Cas d'utilisation : Gestion, control et affichage dans le Cloud

Tableau 7:description textuelle du cas d'utilisation « Gestion, control et affichage dans le Cloud »

Cas d'utilisation :	Gestion, control et affichage dans le Cloud
Acteurs	Serveur (Things network dans notre cas)
Préconditions	Matériel fonctionnel, la connexion est établit
Poste conditions :	Les données sont reçues
Scénario nominal :	Les donnes son reçues et sauvegardées

1.3.2 Diagramme de séquence

La figure 19 représente le diagramme de séquences décrivant les interactions du système d'objets connectés mis en place.

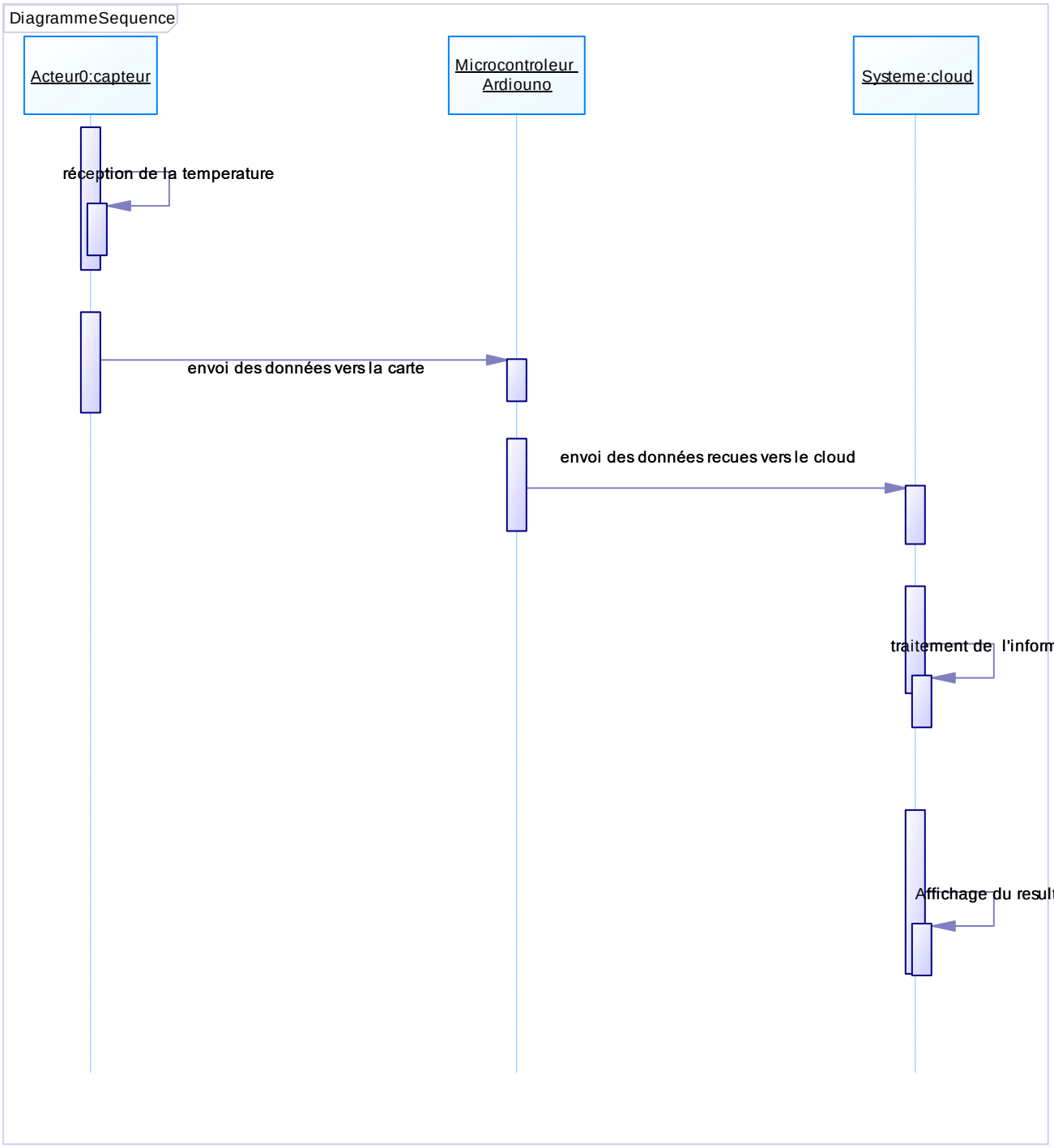


Figure 20:Diagramme de séquence

1.4 Architecture du système d'objets

Dans cette section nous allons définir l'architecture de notre système tout en décrivant les composants matériels que nous avons utilisé et son rôle.

1.5 Le capteur de température dht11

Dans cette partie on va essentiellement parler du capteur de température DHT11 mais n'empêche il existe d'autres capteurs de température tels que le capteur lm 35… Le capteur

DHT11 est un capteur de température capable de mesurer des températures de 0 à +50°C avec une précision de + /- 2°C et des taux d'humidité relative de 20 é 80% avec une précision de + /- 5%.une mesure peut être réalisé toutes les secondes.il est a note aussi que le capteur communique avec le microcontrôleur (carte arduino dans notre cas) via une unique broche sortie /entrée [13].

Le brochage est le suivant :

- ✓ La broche 1 est la broche d'alimentation,
- ✓ La broche 2 est la broche de communication. Celle-ci doit impérativement être relie à l'alimentation via une résistance de tirage de 4,7 ohms
- ✓ La broche 4best la masse du capteur (GND).

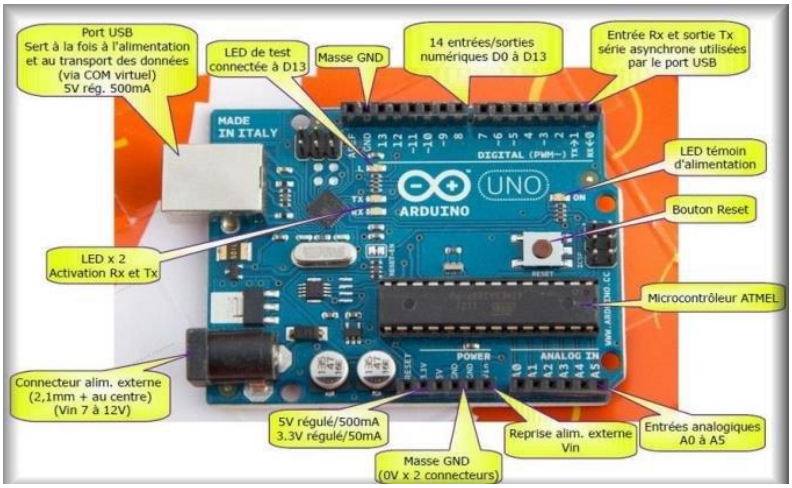
Le tableau suivant est un résumé de ses caractéristiques :

Tableau 8:caracteristiques du capteur de température DHT11

Caractéristiques	Capteur DHT11
humidité	20 - 80%
Précision (humidité)	+ /- 5%.
Température	0 - 50°C
Précision (température)	+ /- 2°C
Fréquence mesure maximale	1Hz (1 mesure par seconde)
Tension d'alimentation	3-5volts
Stabilité à long terme	+ /-1%. Par An

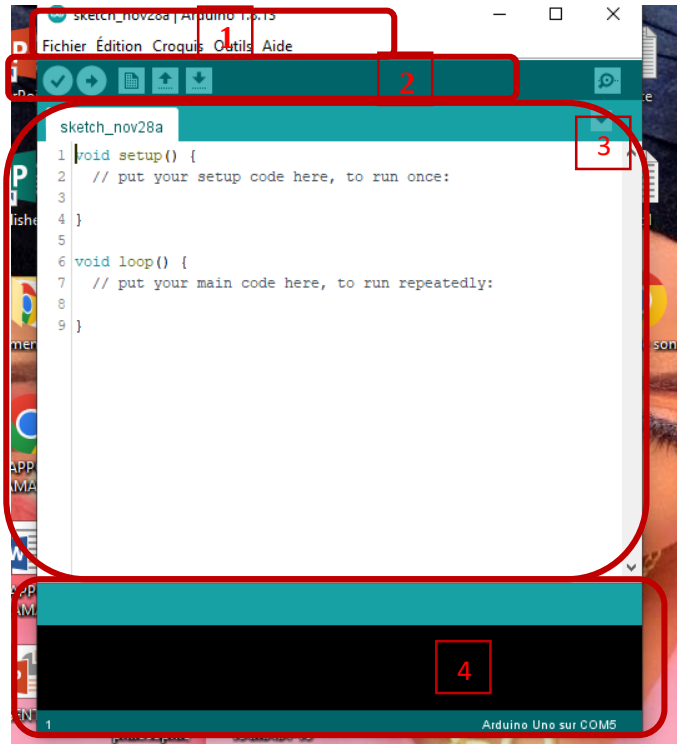
1.6 La carte Arduino

La carte Arduino est un microcontrôleur système embarqué qui ressemble à un ordinateur) Open source permettant toutes sortes de réalisation diverse, rendant ainsi accessible tout ce qui nécessitait avant l'électronique compliqué [18]. La carte possède une mémoire, un processeur, des interfaces. Elle se relie à l'ordinateur par un câble qui lui permet à la fois de de s'alimenter et de faire la communication en série.



1.7 Le logiciel Arduino

Arduino IdE est logiciel de programmation des modules Arduino. Elle est faite en java et est libre et multiplateforme. Elle nous sert d'éditeur de code mais aussi de compilateur. Son téléchargement se fait à partite de la page de téléchargement du site arduino.cc.il est téléchargeable sous Windows, sous linux comme sous Mac os. Au lancement du logiciel nous avons l'interface suivant que nous allons découper en cadre pour plus que nous allons expliquer :



- ✓ Le cadre 1 comporte les options de modification du logiciel.

- ✓ Le cadre 2 comprend respectivement les boutons compilations téléversement, création, ouverture, enregistrement de nouveaux fichiers et le bouton qui permet d'ouvrir le moniteur de série.
- ✓ Le cadre 3 est la partie qui contient le programme à exécuter.
- ✓ Le cadre 4 est le débogueur car c à partir de là qu'on va voir les erreurs.

1.8 Le modem dragino (lps8)

Le lps8 est une passerelle LoRaWAN Open source.il permet de relier un réseau sans fil lora a un réseau via wifi, Ethernet. Le sans-fil lora permet d'envoyer des données et d'atteindre des plages extrêmement longues à des débits de données bas.

Les caractéristiques du lps8 sont les suivants :

- ✓ Système open source.
- ✓ Gere par une interface graphique web, SSh via WAN ou wifi accès à distance.
- ✓ Une passerelle LoRaWAN.
- ✓ 10chemins de démodulations parallèles programmables.
- ✓ Il peut autoriser la personnalisation des paramètres régionaux.
- ✓ Prend en charge la connexion de différents niveaux.

1.9 Le serveur de sauvegarde (Things network)

C'est un serveur de réseau LoRaWAN qui est le composant essentiel de toute solution lorawan.il est utilisé dans beaucoup de système IoT car il gère en toute sécurité les applications, les périphériques finaux et les passerelle.il fournit un ensemble d'outils ouvert et un réseau mondial pour la construction d'application IoT à faible cout et une sécurité maximale.

2 Mise en œuvre

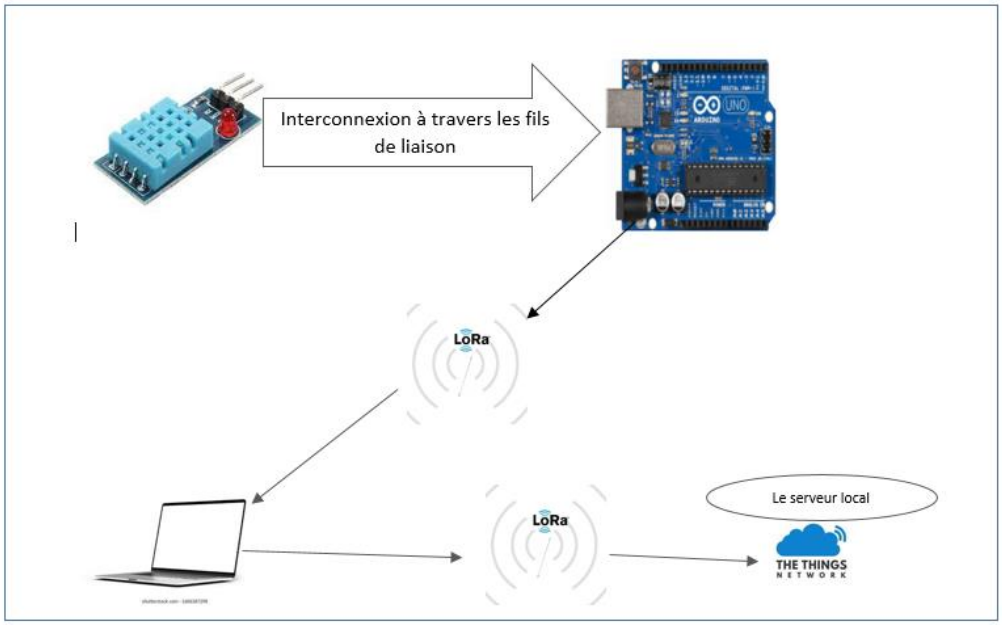
2.1 Description du système

Le système d'objets connecte fonction selon le principe suivant :

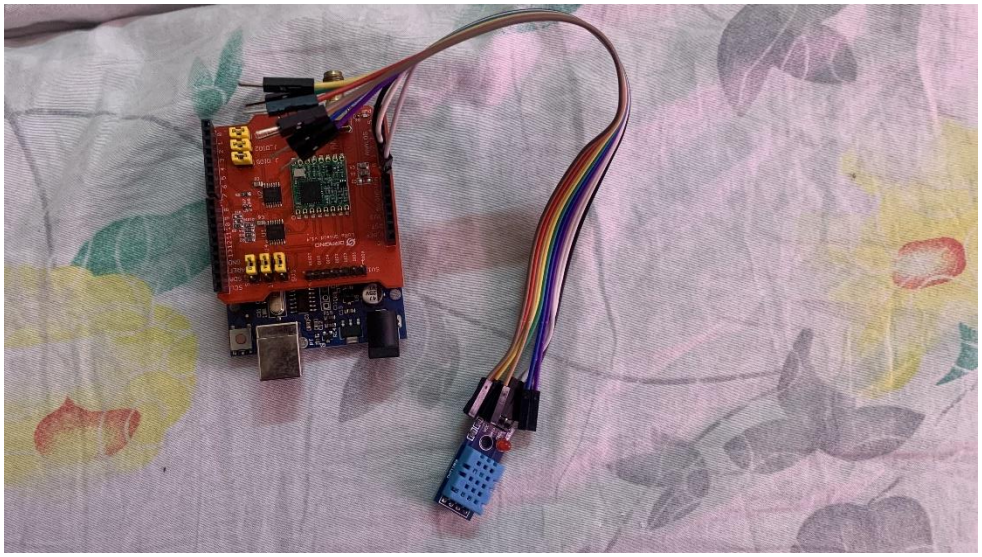
Le capteur dht11 branché au microcontrôleur Arduino qui va, à partir du code qui a été écrit et téléversé dans la carte, récupérer la température du milieu dans lequel il se trouve. Ces données récupérées, sont affichées dans le moniteur de série puis sont par la suite envoyées vers le Cloud via le réseau lora mis en place. Les données sont stockées dans le Cloud qui est un serveur dans notre cas (Things network).

A partir du Cloud l'administrateur qui s'est connecté pourra voir en temps réel l'échange de données et la communication qui se fait depuis entre la carte et le serveur dans le Cloud

La figure suivante représente l'architecture de notre système d'objets connectés.



2.2 Branchement de capteur



Cette image représente le branchement du capteur de température dans la carte arduino ou sera télé versé un code pour gérer les informations recueillis.

2.3 Configuration du modem dragino (lps8)

Au premier démarrage du modem wifi encore appelé lps8 il générera automatiquement un réseau appelé dragino avec un mot de passe dragino+dragino. Nous allons par la suite utiliser ces paramètres pour se connecter à ce réseau et faire des configurations.il faut aussi noter qu'après connexion on aura une adresse IP du genre 10.130.1.xxx tout en sachant que l'adresse IP par défaut et le 10.130.1.1.

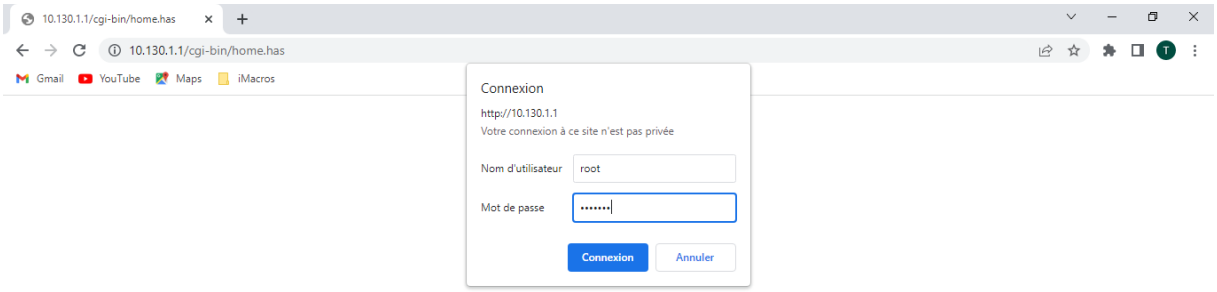
*Configuration accès interface utilisateur web

- ✓ Interface Web

Ouvrer un navigateur sur l'ordinateur connecté et taper l'adresse IP du LPS8 (modem wifi) Http://10.130.1.1/ (accès via la connexion).par la suite on aura l'interface de connexion du lps8 comme l'indique l'image ci-dessus, les details du compte web sont :

Nom d'utilisateur : root

Mot de passe : dragino.



✓ Configuration de réseau type

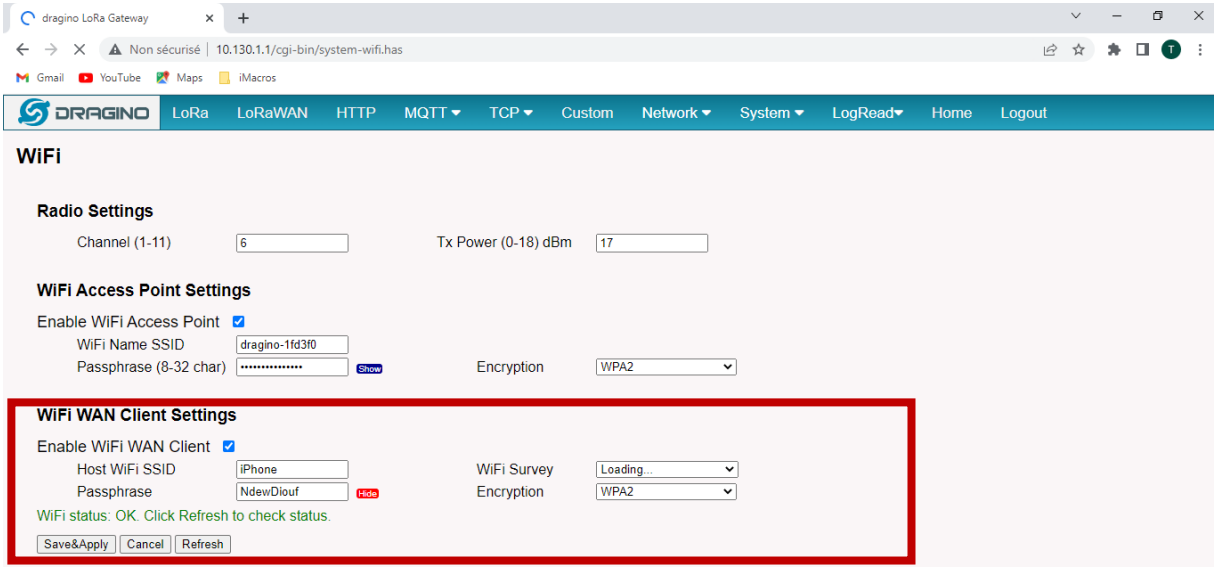
Le lps8 prend en charge la configuration de réseau flexible pour différentes topologies de réseau typique qui peuvent être définies dans lps8 comme le wifi client, l'accès à internet par le port Wan…

✓ Utilisation du port Wan pour accéder à internet

Par défaut, le lps8 est configuré pour utiliser le port Wan pour se connecter à un réseau en amont. Lorsque le port Wan du lps8 est connecté à un routeur en amont, le lps8 aura accès à internet via le routeur en amont.

✓ Configuration accès en tant que client wifi

En mode client wifi, le lps8 agit comme un client wifi et obtient le DHCP d'un routeur en amont via le wifi. Pour paramétrer cela il faut aller dans la partie system du lps8 et modifier les paramètres du client wifi.



Maintenant notre modem est prêt pour nous permettre d'accéder à internet.

2.4 Configuration du système de sauvegarde

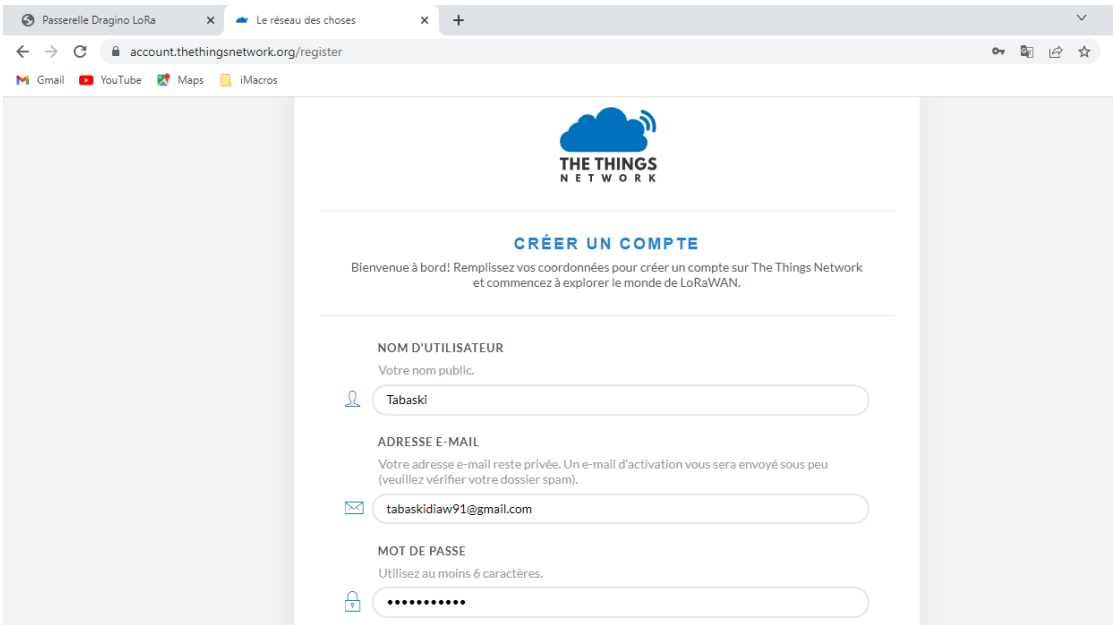
Avant tout il faut noter pour la sauvegarde, la réception des donnes se fera à partir du lps8 qui a un identifiant unique. Le lps8 est entièrement compatible avec le protocole LoRaWAN et il utilise l'ancien transitaire de paquets Semtech pour transférer les paquets LoRaWAN au serveur.

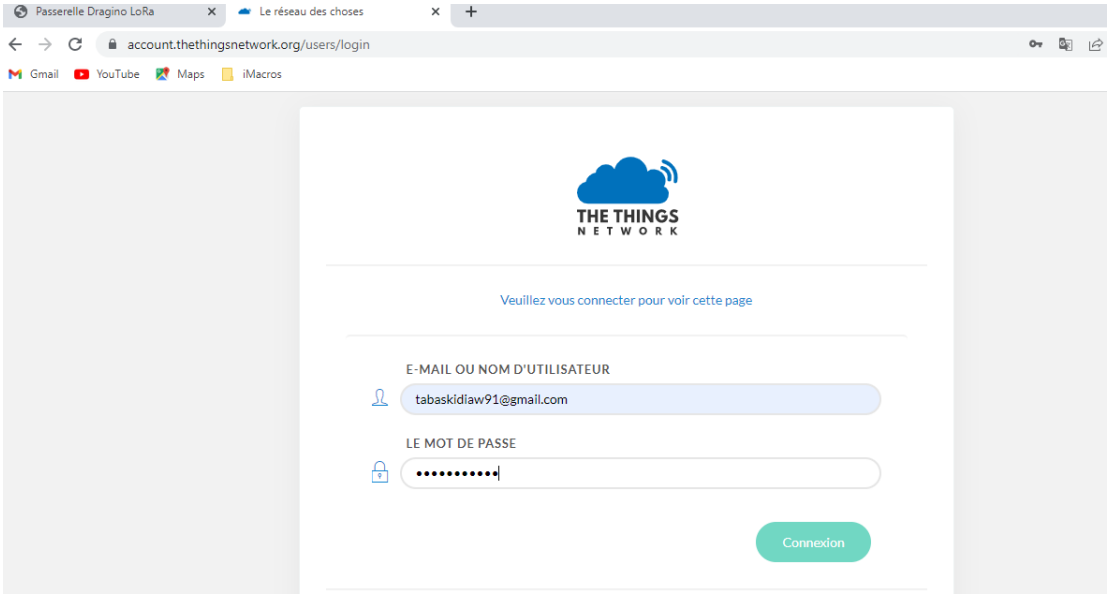
- ✓ Choix du serveur

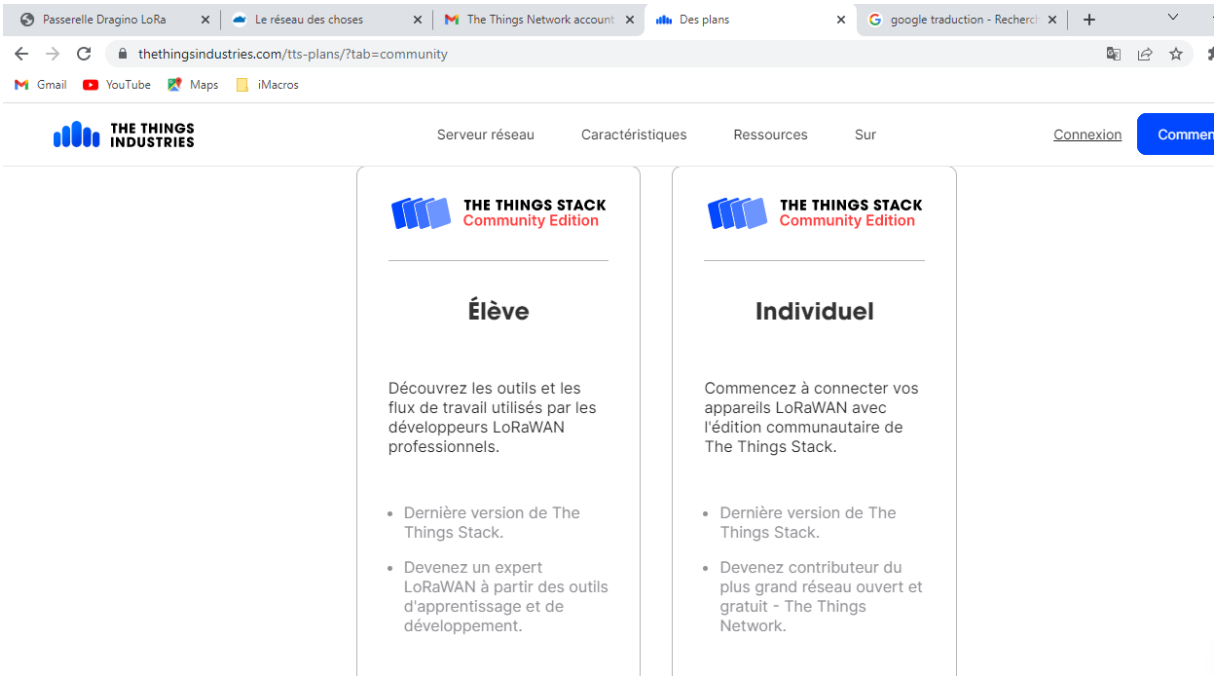
Dans notre travail nous avons utilisé Things network comme serveur car il est serveur réseau LoRaWAN et est un composant essentiel pour toute solution LoRaWAN, il gère en toute sécurité les applications, les périphéries finaux et les passerelles.

Pour utiliser Things Stack il faut d'abord y posséder un compte et cela peut se faire à partir de ce lien **https://account.thethingsnetwork.org/register**.

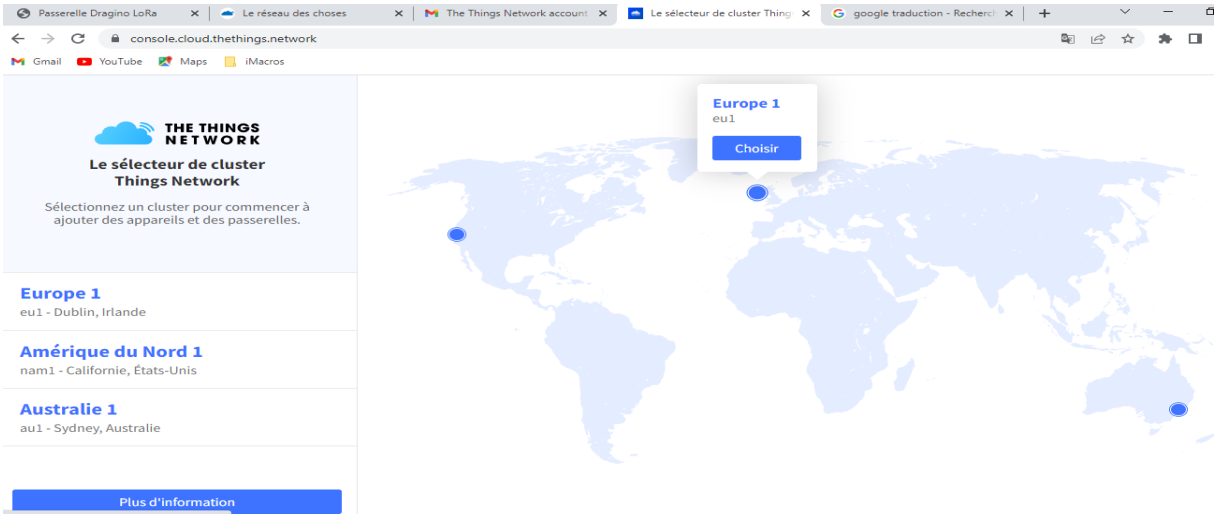
Les images qui suivent montrent la procédure de création du compte utilisé dans ce travail :

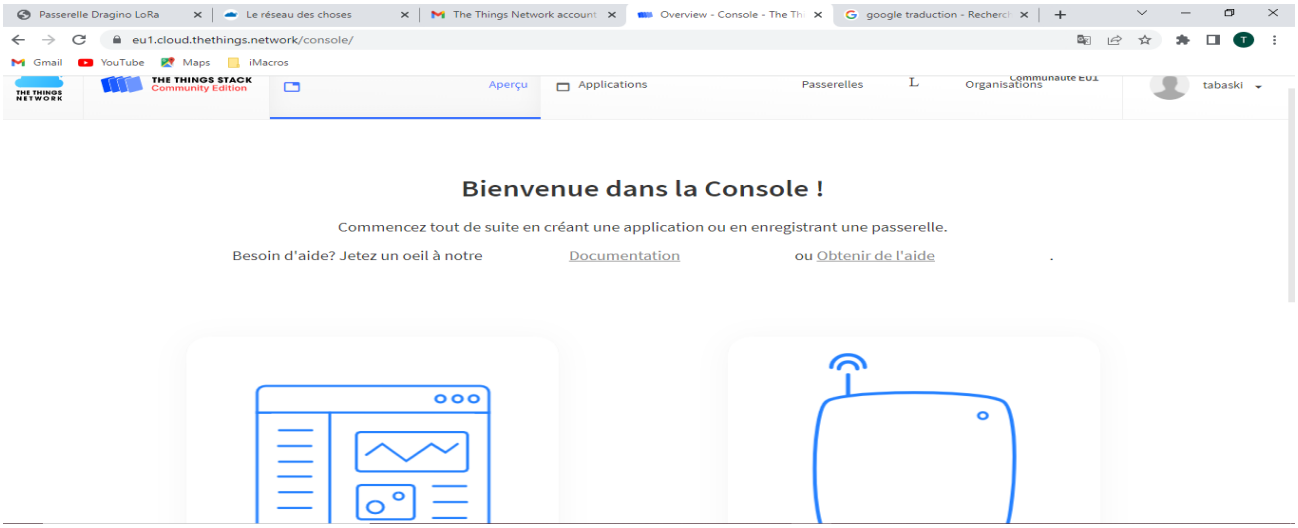






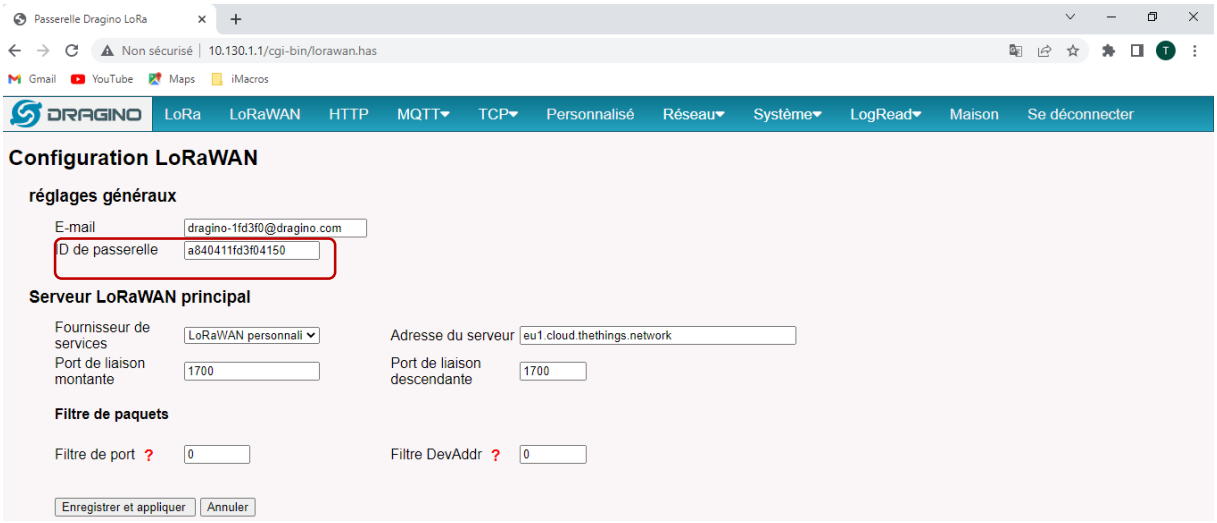
Apres la création du compte on va se connecter avec les paramètres obtenus et créer le projet qui comportera les configurations qui nous permettrons de lier notre serveur au lps8.



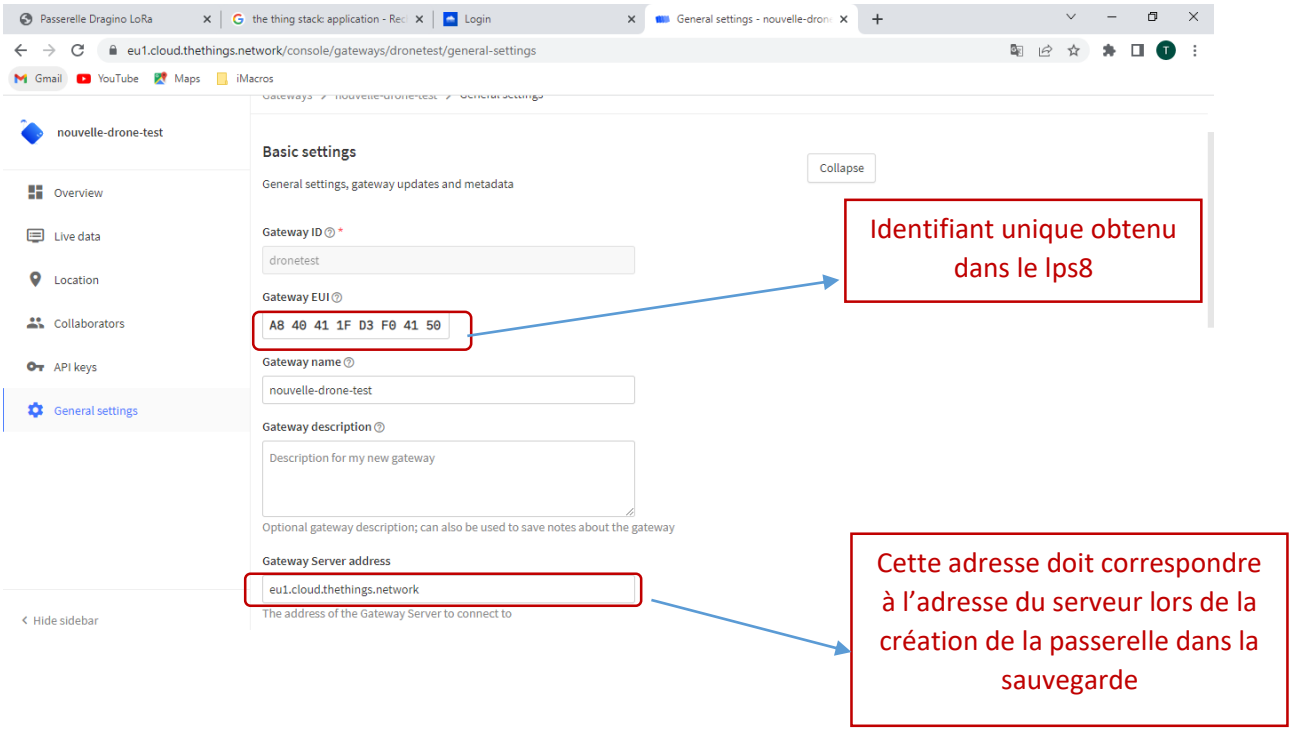


✓ Configuration passerelle

Apres avoir créé un compte de qui jouera le rôle de serveur nous allons maintenant passer à la configuration de la passerelle, pour se faire on va se rendre sur la console et cliquer sur ajouter une passerelle pour ensuite faire les modifications nécessaires.

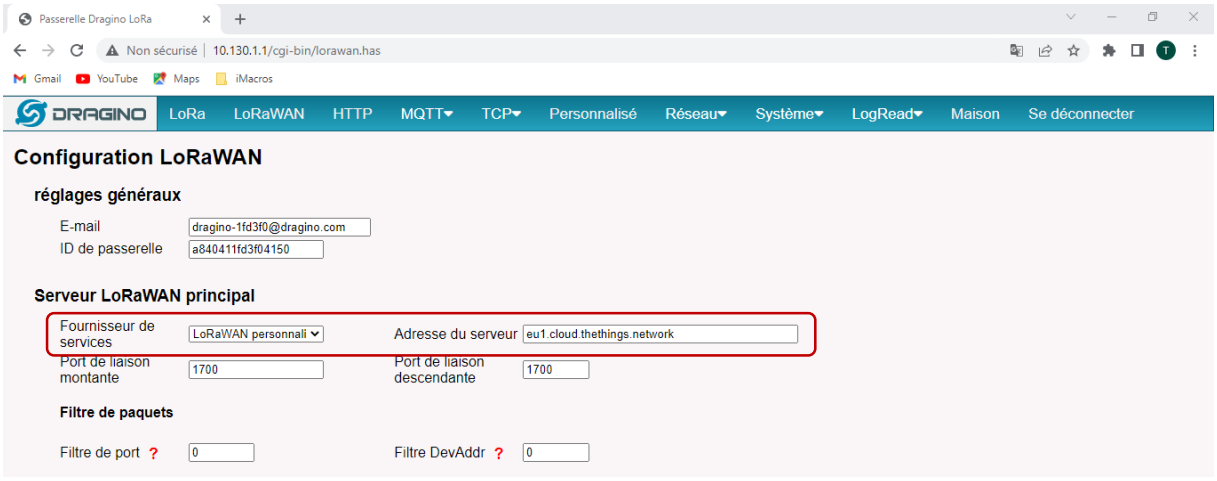


Dans l'image qui précède nous avons mis en gras l'identifiant de la passerelle cette identifiant est unique dans chaque dispositif dans notre cas c'est le a840411fd3f04150 que nous allons utiliser pour la passerelle dans la sauvegarde.

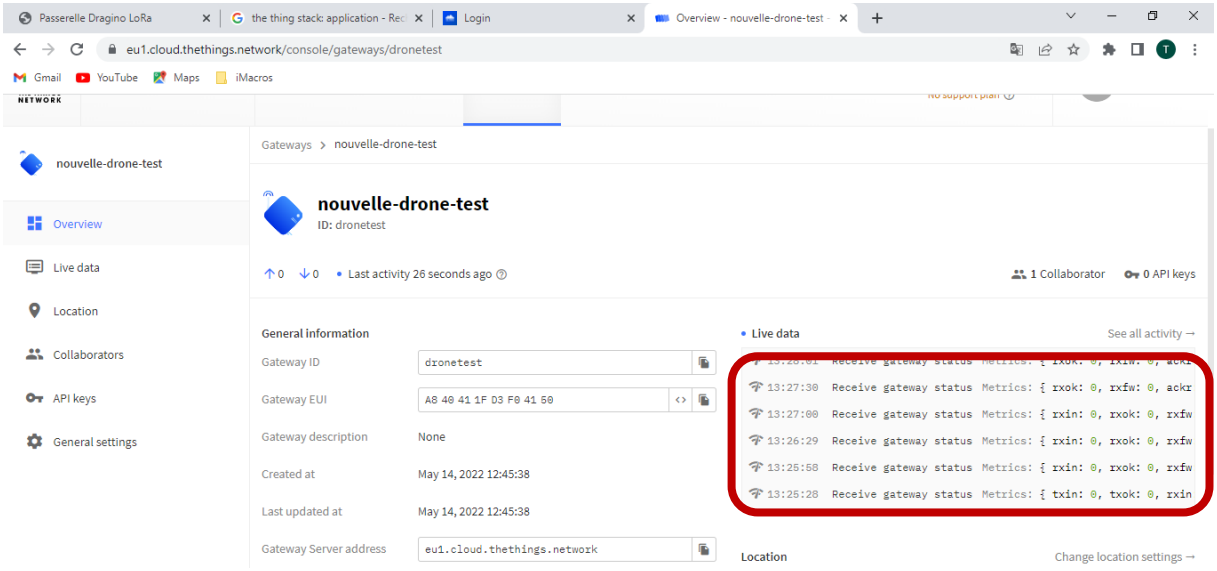


✓ Configuration de la connexion du lps8 au réseau

Dans cette configuration il faudra au préalable vérifier que le lps8 est déjà connecté à internet puis faire modification nécessaires pour permettre au passerelle créer dans le serveur de pouvoir recevoir les informations en temps réels.



Apres configuration on aura le résultat suivant :



Conclusion

Dans ce chapitre nous avons eu à faire la description du système d'objets connectés à réaliser de de manière générale et les configurations nécessaires (la configuration du réseau lora, la configuration de l'accès à internet et la configuration du système de sauvegarde) pour que notre système d'objet connecté soit prêt et fonctionnels.

Conclusion générale

Dans un monde « hyper connecté » via des objets connectés où les usagers sont à la fois émetteurs et récepteurs des données, l'IOT ouvre des champs nouveaux à explorer pour les sciences de l'information et de la communication.

Ce mémoire faisant l'objet d'étude des technologies de communication dans l'Internet des objets (IOT) s'est articulé autour de quatre chapitres.

Nous avons eu à traiter dans les chapitres 1 et 2 les concepts de base de l'internet des objets, ses domaines d'application et caractéristiques. De même aussi cette étude nous a permis de manière générale de comprendre l'architecture de l'Internet des objets.

Avec le chapitre 3 nous avons étudié les technologies de communication dans l'IOT en relatant les types de réseaux sans fil existant tel que les réseaux sans fil courte portée haut débit, les réseaux sans fil longue portée haut débit ,les réseaux sans fil longue portée et faible débit et quelques protocoles tel que le 3G/4G/5G, le wifi, le ZigBee, le Bluetooth, protocole SigFox, le protocole LoRaWAN, le protocole Nb-IoT, le protocole Z-WAVE, protocole thread.

Et enfin le chapitre 4 qui boucle se mémoire est un cas pratique avec l'utilisation du capteur de température DHT11 avec le réseau LoRaWAN ou a réalisé la configuration d'un réseau lora et le transfert de donnée à partir de ce dernier.

En perspectives nous prévoyons d'amplifier le travail effectué dans le cas pratique en y ajoutant des systèmes d'alerte et de notifications en temps réels.

Bibliographie

[1] I. Chouk et Z. Mani, « Les objets connectés peuvent-ils susciter une résistance de la part des consommateurs? Une étude netnographique », *Décisions Marketing*, n° 84, p. 19-42, 2016.

[2] N. Meliti et S. Kouah, « Architecture basée agents pour le diagnostic d'un système d'IoT (internet of things) », 2017.

[3] N. Meliti et S. Kouah, « Architecture basée agents pour le diagnostic d'un système d'IoT (internet of things) », 2017.

[4] M. Benboudriou et S. Kouah, « Concéption et réalisation d'un systémes d'IoT (Internet of Things) basé agents pour le suivi des patients dans le cadre E-santé. », 2019.

[5] K. K. Patel, S. M. Patel, et P. Scholar, « Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges », *International journal of engineering science and computing*, vol. 6, n° 5, 2016.

[6] J. Lisein, S. Bonnet, P. Lejeune, et M. Pierrot-Deseilligny, « Modélisation de la canopée forestière par photogrammétrie depuis des images acquises par drone », *Revue française de photogrammétrie et de télédétection*, vol. 206, p. 45-54, 2014.

[7] J. Tournier, « Modélisation de réseaux IoT hétérogènes à des fins d'évaluation de sécurité », PhD Thesis, Université de Lyon, 2021.

[8] M. Thiery, « Objets connectés et vie privée: le long chemin restant », PhD Thesis, Université Grenoble Alpes, 2020.

[9] R. Stanica, Y. Mouline, J.-M. Gorce, C. Goursaud, et O. Iova, « IoT Anywhere-Comment choisir sa technologie d'accès? », PhD Thesis, INSA LYON; SPIE ICS, 2020.

[10] C. Gomez, J. C. Veras, R. Vidal, L. Casals, et J. Paradells, « A sigfox energy consumption model », *Sensors*, vol. 19, n° 3, p. 681, 2019.

[11] S. Cluzel, « Système M2M/IoT par satellite pour l'hybridation d'un réseau NB-IoT via une constellation LEO », PhD Thesis, Toulouse, ISAE, 2019.

[12] O. Kocak, « Elaboration de directives de déploiement d'un réseau LoRa sécurisé à l'usage de PME », PhD Thesis, Haute école de gestion de Genève, 2020.

Webographie

[13] www.carnetdumaker.com.

[14] www.journaldunet.com.

[15] https://eduscol.education.fr.

[16] https://www.ebds.eu/ressources.

[17] www.comparativement.fr.

[18] http://www.arduino.cc/