**REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE**

**وزارة التـــعـليـــم العـــــالي والبـــحث العـــــلـمـــي**

**Ministère de l'Enseignement Supérieur et de la Recherche Scientifique**

**جـــــــــــامعة سعيدة – د. الطاهر مولاي –**

Université Saïda – Dr. Tahar Moulay –

Faculté de Technologie

# MEMOIRE

Présenté pour l'obtention du **Diplôme** de **MASTER en** Télécommunications

**Spécialité** : Réseaux et Télécommunications

**Par** : Mr. Benabderrahmane Younes Akram

Mr. Chahri Mostapha

# Communication entre les objets IoT par le systéme Zigbee et ESP

Soutenu, le 23 /06/ 2024, devant le jury composé de :

| | | |
|---|---|---|
| Dr. Guendouz Mohamed | MCA | Président |
| Dr. Ouis Esma | MAB | Encadreur |
| Dr. Belhadj Salima | MAB | Examinateur |

**2023 / 2024**


بسم الله الرحمن الرحيم

# *Remerciements*

*Nous remercions avant tout ALLAH qui nous a permis d'accomplir ce travail. Dieu soit loué, nous adressons nos sincères remerciements à toutes les personnes qui nous ont aidé, directement ou indirectement, dans l'élaboration de ces humbles notes. Nos sincères remerciements vont à notre encadrante, Dr Ouis Esma, pour ses conseils et instructions, et à Mr Yahi Youcef, pour ses conseils son soutien nous leur sommes très reconnaissants pour l'excellent encadrement nous tenons également à remercier tous les professeurs qui ont contribué à notre formation, nous remercions chaleureusement les familles Chahri et Benabderrahmane et Nouicer pour leur aide morale et matérielle tout au long de la période de préparation.*

# *Dédicace*

*La joie du succès est incomplète si nous ne la partageons pas*

*Avec ceux qu'on aime*

*Nous dédions cet humble travail aux personnes qui nous sont les plus chères*

*Nos parents qui nous ont beaucoup soutenus à l'époque*

*Les plus difficiles sont ceux qui ont partagé nos joies et nos peines*

*Que dieu les protège*

*A nos chers frères et sœurs*

*Et*

*Pour toute notre famille Nouicer*

*À tous nos amis*

*À tous nos collègues*

*Nous consacrons cet humble travail.*

# Résumé

**Abstract**

Our dissertation explores the efficiency of communications between IoT devices using ZigBee and ESP32 technologies, integrating a Raspberry Pi as a central administrator. The study highlighted the advantages of ZigBee, such as low power consumption and the ability to form mesh networks, as well as the versatility of ESP32. The simulations and tests carried out confirmed the reliability of this architecture for data transmission in IoT environments.

The results obtained show that this configuration is effective for practical applications in various fields, including health, industry, and home automation. This work contributes significantly to the understanding and improvement of communication and data management in IoT systems, proposing practical methods to optimize the interconnection of devices.

**Keywords:** zigbee, ESP32, MAX 30102, LM 35, Logiciel Arduino, ESP 8266**.**

**ملخص**

تستكشف أطروحتنا كفاءة الاتصالات بين أجهزة إنترنت الأشياء باستخدام تقنيات ZigBee وESP32، ودمج Raspberry Pi كمسؤول مركزي. وسلطت الدراسة الضوء على مزايا ZigBee، مثل انخفاض استهلاك الطاقة والقدرة على تشكيل شبكات متداخلة، بالإضافة إلى تعدد الاستخدامات .ESP32 وأكدت عمليات المحاكاة والاختبارات التي تم إجراؤها موثوقية هذه البنية لنقل البيانات في بيئات إنترنت الأشياء.

وتظهر النتائج التي تم الحصول عليها أن هذا التكوين فعال للتطبيقات العملية في مختلف المجالات، بما في ذلك الصحة والصناعة والأتمتة المنزلية. يساهم هذا العمل بشكل كبير في فهم وتحسين الاتصالات وإدارة البيانات في أنظمة إنترنت الأشياء، ويقترح طرقًا عملية لتحسين التوصيل البيني للأجهزة.

**الكلمات المفتاحية :** زيجبي , MAX 30102, ESP32 , LM35 ,برنامج الاردوينو ,ESP 8266 **.**

**Résumé**

Notre mémoire explore l'efficacité des communications entre les dispositifs IoT en utilisant les technologies ZigBee et ESP32, intégrant un Raspberry Pi comme administrateur central. L'étude a mis en évidence les avantages de ZigBee, tels que la faible consommation d'énergie et la capacité à former des réseaux maillés, ainsi que la versatilité de l'ESP32. Les simulations et les tests réalisés ont confirmé la fiabilité de cette architecture pour la transmission des données dans des environnements IoT**.**

Les résultats obtenus montrent que cette configuration est efficace pour des applications pratiques dans divers domaines, notamment la santé, l'industrie, et la domotique. Ce travail contribue de manière significative à la compréhension et à l'amélioration de la communication et de la gestion des données dans les systèmes IoT, proposant des méthodes pratiques pour optimiser l'interconnexion des dispositifs**.**

**Mots clés :** zigbee , ESP32 , MAX 30102, LM 35, Logiciel Arduino , ESP 8266**.**

# Table des matières

# Table des matières

# Table des matières



## Chapitre 2 Objets connectés

# Table des matières

# Table des matières

# Liste des abréviations

# *Liste des abréviations*

**AMQP** **A**dvanced **M**essage **Q**ueuing **P**rotocol

**API** **A**pplication **P**rogramming **I**nterface

**ARP** **A**ddress **R**esolution **P**rotocol

**AWGN** **A**dditive **w**hite **G**aussian **n**oise

**DMP** **D**ossier **M**édical **P**artagé

**DSE** **D**ossiers de **S**anté **E**lectroniques

**DVD** **D**igital **V**ersatile **D**isc

**ECG** **E**le**c**tro **C**ardio **G**ramme

**EDGE** **E**nhanced **D**ata Rates for **G**SM **E**volution

**EDI** **E**space de **D**éveloppement **I**ntégré

**EKG** **E**lectro cardio graphy

**ETSI** **E**uropean **T**elecommunications **S**tandards **I**nstitute

**FCA** **F**ournisseurs de **C**ontenus et d'**A**pplications.

**GPIO** **G**eneral **P**urpose **I**nput/**O**utput

**HTTP** **H**yper**T**ext **T**ransfer **P**rotocol

**IBM** **I**nterntional **B**usiness **M**achine corporation

**IBSG** **I**nternet **B**usiness **S**olution **G**roup

**IDC** **I**nternational **D**ata **C**orporation

**IoT** **I**nternet **O**f **T**hing

**IEC** **I**nternationa**l** **E**lectrotechnical **C**ommission

**IEEE** **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers

**IETF** **I**nternet **E**ngineering **T**ask **F**orce

**IIoT** **I**ndustry **I**nternet **O**f **T**hing

**IP** **I**nternet **P**rotocol

**IPS** **I**nternet **P**rotocol **S**écurité

**IPv4** **I**nternet **P**rotocol **V**ersion **4**

**IPV6** **I**nternet **P**rotocol **V**ersion **6**

**IrDA** **I**nf**r**ared **D**ata **A**ssociation

**ISBG** **I**nternet **B**usiness **S**olutions **G**roup

**IIC** **I**nter **I**ntegrated **C**ircuit

## Liste des abréviations

**LTE** **L**ong **T**erm **E**volution

**MCU** **M**ultipoint **C**ontrol **U**nit

**MIT** **M**assachusetts **I**nstitute of **T**echnology

**MQT** **M**essage **Q**ueue **T**elemetry **T**ransport

**MTC** **M**achine **T**ype **C**ommunication

**M2M** **M**achine **T**o **M**achine

**NAT** **N**etwork **A**ddress **T**ranslation

**NDP** **N**eighbor **D**iscovery **P**rotocol

**NFC** **N**ear **F**ield **C**ommunication

**OMS** **O**rganisation **M**ondiale de la **S**anté

**OQPSK** **Q**uadrature **P**hase **S**hift **K**eying

**PN** **P**seudo **N**oise

**XMPP** **E**xtensible **M**essaging and **P**resence **P**rotocol

**2D** Bidimensionnelle

**3D** Tridimensionnel

**3G** **T**hird **G**enerations

**3GPP** **3rd G**eneration **P**artnership **P**roject

**4G** **F**ourth **G**eneration

**5G** **F**ifth **G**eneration

**6loWPan** **6 L**oW **P**ower **W**ireless **A**rea **N**etworks

# Liste des figures

# *Liste des figures*

## Chapitre 1



## Chapitre 2

## Chapitre 3

# Introduction générale

## Introduction générale

L'internet des objets (IoT), est élargisse les horizons de l'internet traditionnel, forge un écosystème interconnecté d'appareils intelligents. Ce mémoire vise à explorer l'efficacité des communications entre ces dispositifs en utilisant des technologies avancées telles que ZigBee et ESP32, ainsi que l'intégration d'un Raspberry Pi en tant qu'administrateur central. L'accent est mis sur l'amélioration des interactions et de la gestion des données au sein de cet environnement réseau complexe**.**

Notre étude a implémenté des communications entre ZigBee et ESP32 pour faciliter la transmission de données dans un environnement IoT. En outre, la communication entre différents modules ESP a été établie, renforçant l'efficacité du réseau. Le rôle du Raspberry Pi en tant qu'administrateur central a été crucial, orchestrant les flux de données et assurant une gestion transparente des informations. Cette configuration a permis l'intégration de capteurs d'oxygène et de température utilisant la technologie ZigBee, dont les données sont ensuite stockées de manière efficace et sécurisée sur le Raspberry Pi**.**

Cette architecture avancée, combinant ZigBee, ESP32, et Raspberry Pi, illustre une approche innovante de la gestion des réseaux IoT, offrant des perspectives prometteuses pour l'amélioration de l'interconnexion et de la gestion des appareils dans divers contextes applicatifs. Ce travail de recherche contribue à la littérature existante en proposant des méthodes pratiques pour améliorer la communication et la gestion des données dans les systèmes IoT complexes, ouvrant la voie à des développements futurs dans ce domaine dynamique**.**

# Chapitre 1
# Concepts fondamentaux sur l'internet des objets

## 1 Introduction :

La technologie Internet des Objets (IoT) est une innovation majeure, avec de nombreuses applications et évolutions qui simplifient la communication entre les habitants en connectant les objets à Internet. L'Internet des objets permet le transfert d'informations entre les objets et l'environnement, ouvrant ainsi de nouvelles possibilités de communication. Dans ce chapitre, nous explorons les définitions, le développement, la fonction et la localisation de l'Internet des objets à l'aide de la technologie 5G et de ses appareils.

### 1.1 Définition :

La première partie de la section présente l'internet des objets (IoT) comme concept introductif de Kevin Ashton, expliqué à travers la communication entre les objets qui va au-delà des identifiants uniques. Cette communication, qui utilise des objets interchangeables tels que des appareils électroniques, constitue la définition de la technologie Internet des objets depuis le début de notre nouveau développement et son développement continu, afin que le conducteur puisse utiliser « l'interface utilisateur ». Ces appareils, qui regroupent une variété de tout ce qui est connecté à l'électronique et aux véhicules connectés, basiques pour le contrôle à distance de la maison ou fonctionnant dans la dimension « objet » des TIC, l'Internet des objets permet aux utilisateurs de Mossoul de ne pas importer l'objet à aucun moment **[1].** L'évolution de l'Internet des objets est un concept promu par Cisco depuis 2011 **[2].**

L'internet des objets (IoT) annonce une nouvelle ère de connectivité où les appareils intelligents interagissent de manière transparente pour améliorer notre vie quotidienne,comme illustré dans la figure suivante :

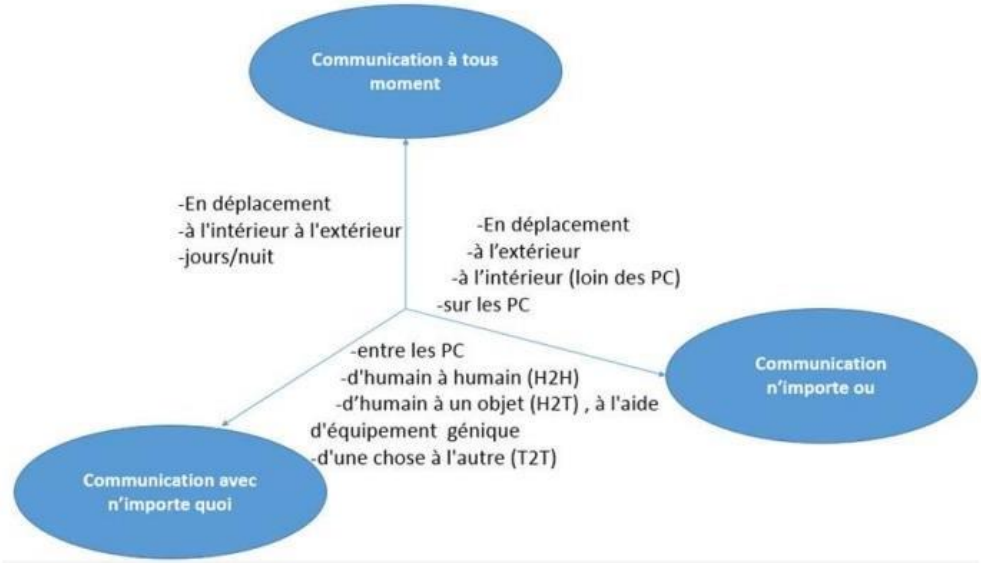



**Figure 1.1 :** Une nouvelle dimension pour l'internet des objets (IoT) **[3].**

### 1.2 Historique :

Le terme d'Internet des objets a été évoqué pour la première fois en 1995 par Bill Gates, fondateur de Microsoft, dans son ouvrage (The Road Ahead). Bien qu'il y ait présenté ce concept novateur il n'a pas immédiatement capté l'attention du public, l'Internet étant encore à ses balbutiements. L'origine de l'IoT est souvent attribuée au Massachusetts Institute of technology (MIT), plus précisément au sein du groupe Auto-ID Center qui a joué un rôle clé dans le développement de cette idée. Selon le Cisco Internet Business Solution Groupe (IBSG), l'IoT a véritablement pris son envol au moment où le nombre d'objets connectés à Internet a surpassé celui de personnes connectées**.**

En 2003, avec une population mondiale d'environ 6,3 milliards de personnes et 500 millions d'appareils connectés à Internet, le ratio d'appareils par personne était de 0,08, ce qui indique moins d'un appareil connecté par personne **[3].** A cette époque, selon la définition de Cisco IBSG, l'Internet des objets (IoT) n'était pas encore une réalité en raison du nombre limité d'objets connectés. De plus, les appareils populaires d'aujourd'hui, tels que les smartphones, commençaient tout juste à apparaître sur le marché**.** L'énorme augmentation de l'utilisation des smartphones et des tablettes a entraîné une augmentation considérable du nombre d'appareils connectés à Internet, atteignant 12,5 milliards en 2010, tandis que le nombre moyen d'appareils connectés par personne a dépassé un, atteignant spécifiquement 1,84 **[3].**

Étapes de développement des réseaux informatiques vers l'Internet des Objets (IoT) comme illustré dans la figure suivante **:**

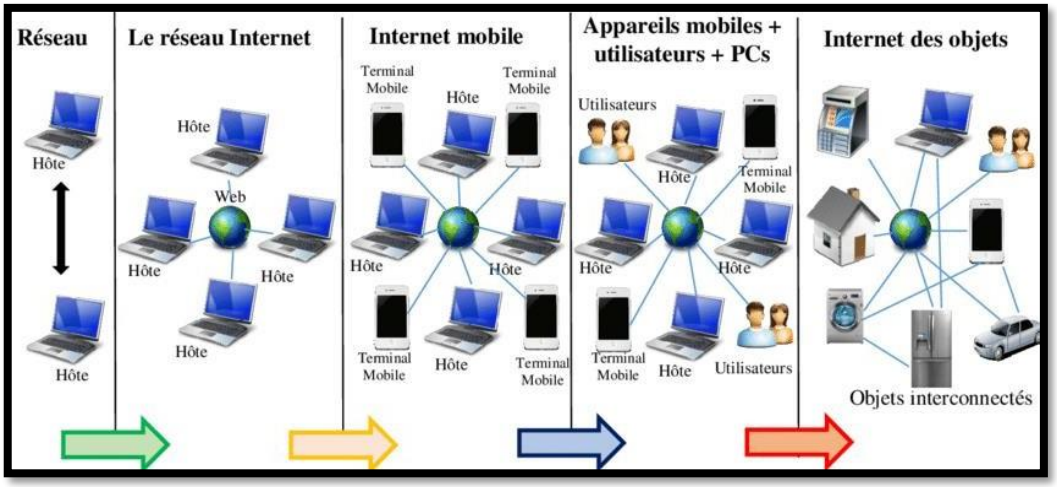



**Figure 1.2 :** Évolution des réseaux informatiques vers l'internet des objets (IoT) **[4].**

Cisco IBSG prévoit que 50 milliards d'appareils seront connectés à Internet d'ici 2020. Il est important de souligner que ces estimations ne tiennent pas compte des progrès rapides d'Internet ni des avancées technologiques et se basent uniquement sur des données concrètes qui existent à l'époque **[3]**, comme illustré la figure suivante **:**

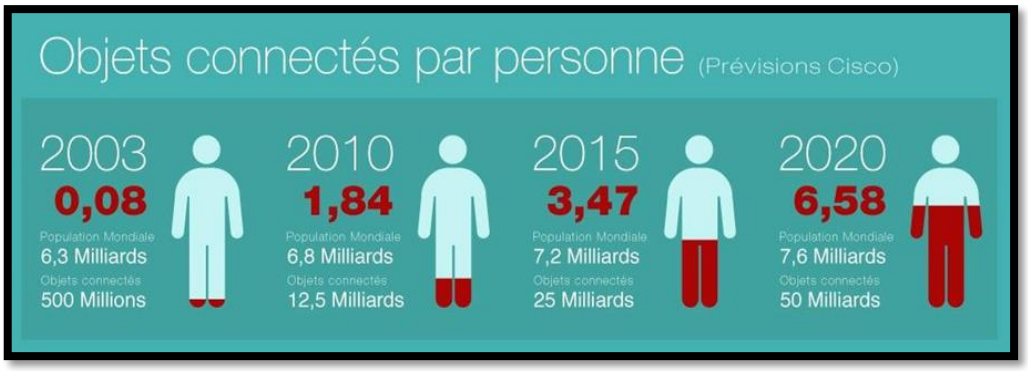



**Figure 1.3 :** Le développement de l'internet des objets selon cisco en 2011 **[3].**

### 1.3 Principe de fonctionnement :

L'Internet des objets (IoT) se compose de divers éléments complémentaires, chacun possédant ses propres caractéristiques. Grâce aux systèmes d'identification électronique normalisés et aux dispositifs mobiles sans fil, il est possible d'identifier de manière directe et non ambiguë des objets physiques, ainsi que de récupérer stocker transférer et traiter de manière continue les données qui leur sont associées **[4].** L'IoT combine des innovations technologiques récentes avec des solutions déjà existantes. Chaque objet est doté d'une identification électronique unique qui lui permet de lire des informations et de les transmettre via un protocole sur le réseau Internet. Il est également nécessaire de définir la nature de l'objet ses fonctionnalités sa position spatiale l'historique de ses déplacements etc. Pour établir ce lien entre le monde physique et le virtuel le dispositif technique doit pouvoir modéliser des contextes réels et les virtualiser **[5].**

### 1.4 Interopérabilité et communication dans l'IoT :

Un des principes clés de l'Internet des Objets (IoT) est la capacité des objets à communiquer entre eux indépendamment de leur nature, leur provenance ou leur localisation. L'interopérabilité et l'ouverture sont essentielles dans ce domaine. Bien que certains estiment que l'utilisation du protocole IP pourrait suffire pour réaliser cette communication la réalité est beaucoup plus complexe. Cette approche soulève d'importants défis en matière de standardisation, montrant que la mise en œuvre effective de l'IoT va bien au-delà de la simple adoption d'un protocole technique. La communication entre les objets connectés (IoT) via le système Zigbee et les modules ESP (comme l'ESP8266 ou l'ESP32) représente une approche

intéressante et efficace pour créer des réseaux domestiques intelligents et d'autres applications IoT. Voici une introduction à la manière dont ces technologies peuvent travailler ensemble pour réaliser des solutions IoT innovantes. Zigbee est une spécification de haut niveau pour les réseaux sans fil utilisés pour créer des réseaux de communication personnels avec de petits appareils numériques à faible puissance, permettant une communication sécurisée avec une consommation d'énergie réduite. Voici les aspects clés de la technologie Zigbee **[5].**

### 1.5 Origine et standardisation :

- **IEEE 802.15.4 :** Zigbee est basé sur cette norme pour les réseaux sans fil à faible débit de données**.**
- **Zigbee Alliance :** Un groupe d'entreprises qui maintient et publie la spécification Zigbee.

#### 1.5.1 Caractéristiques techniques :

- **Fréquence de fonctionnement :** Principalement 2,4 GHz (mondialement), mais peut aussi fonctionner sur 868 MHz en Europe et 915 MHz en Amérique du Nord.
- **Portée :** Typiquement entre 10 et 100 mètres mais la portée peut être étendue grâce à la création de réseaux maillés**.**
- **Topologie de réseau :** Peut prendre en charge plusieurs topologies de réseau y compris point à point, point à multipoint, et maillage.
- **Réseau maillé :** Zigbee peut former des réseaux maillés où chaque dispositif peut transmettre et relayer des données pour d'autres dispositifs, ce qui augmente la portée et la robustesse du réseau**.**
- **Sécurité :** Utilise des clés de chiffrement AES-128 pour sécuriser les communications.

#### 1.5.2 Applications :

- **Automatisation résidentielle :** Commande des appareils électroménagers, des systèmes chauffage et de refroidissement des systèmes de sécurité et del'éclairage.
- **Santé :** Suivi des patients et gestion des médicaments dans les environnements de soins de santé**.**
- **Industrielle :** Surveillance et contrôle des processus industriels.
- **Éclairage intelligent :** Réseaux de lumière qui peuvent être contrôlés de manière flexible et efficace**.**

#### 1.5.3 Avantages :

- **Faible consommation d'énergie :** Conçu pour les dispositifs alimentés par batterie qui peuvent durer plusieurs années sur une seule charge.
- **Facilité d'utilisation et d'installation :** Les réseaux Zigbee sont relativement faciles à configurer et à gérer**.**

- **Interopérabilité :** Zigbee vise à permettre l'interopérabilité entre les produits dedifférents fabricants**.**

**1.5.4 Défis et considérations :**

- **Interférences :** Comme il fonctionne sur la bande des 2,4 GHz, il peut subir des interférences de la part du Wi-Fi, du Bluetooth, et d'autres appareils utilisant la même bande**.**
- **Complexité du maillage :** Bien que le réseau offre des avantages, il peut également rendre la conception et le déploiement du réseau plus complexes**.**

**"Zigbee"** continue d'évoluer avec de nouvelles spécifications et fonctionnalités pour s'adapter aux besoins changeants des applications IoT et de la communication entredispositifs**.**

**"ESP"** fait généralement référence à une famille de microcontrôleurs à bas coût avec Wi-Fi et parfois Bluetooth intégrés développés par Espressif Systèmes. Les deux modèles les plus populaires sont l'ESP8266 et l'ESP32, qui sont largement utilisés dans les projets de bricolage (DIY), les produits commerciaux IoT, et l'enseignement en raison de leur facilité d'utilisation et de leur faible coût**.**

## 1.6 Normes et standards utilisés dans l'internet des objets (IoT) :

Dans cette section, nous examinerons quelques normes clés de l'Internet des Objets **:**

### 1.6.1 Wifi :

Relevant de la famille des standards IEEE 802.11 le Wifi est intégré à tous les nouveaux smartphones et est principalement utilisé par les réseaux locaux sans fil. Il offre des vitesses de transfert pouvant atteindre des dizaines de mégabits par seconde mais est également connu pour sa consommation énergétique relativement élevée réduisant l'autonomie des appareils qui l'utilisent **[6].**

### 1.6.2 Bluetooth :

Présent dans la plupart des appareils intelligents, le Bluetooth est également adopté par de nombreux objets communicants. Défini par le groupement d'intérêt Bluetooth, il est utilisé pour les réseaux sans fil personnels. Historiquement, le Bluetooth offre une portée limitée et un débit inférieur au Wifi, avec des vitesses de quelques centaines de kilobits par seconde. Toutefois, sa version **4.2**, axée sur les objets communicants, promet des vitesses jusqu'à **2,5** fois supérieures à celles des versions antérieures et une faible consommation d'énergie. Des objets comme les montres connectées équipées de cette version peuvent communiquer directement avec un routeurvia le protocole 6LowPan d'IPv6, sans passer par un smartphone **[6].**

### 1.6.3 Zigbee :

Basé sur le standard **IEEE 802.15.4** pour les couches physiques et de liaisons, Zibée est défini par la Zigbee Alliance. Conçue pour des appareils à faible consommation d'énergie, elle offre un débit très bas ne dépassant pas 250 kilobits par seconde et une taille de paquet limitée à **127** octets. Zigbee utilise un Protocole de routage mesh , permettant une connectivité étendue au-delà de la portée radio par le biais de nœuds intermédiaires servant de relais et adopte un plan d'adressage spécifique. Une version plus récente, Zigbee IP, est compatible avec les standards 6LowPan d'IPv6, ce qui facilitel'interopérabilité avec d'autres réseaux **[6].**

### 1.6.4 5G :

La technologie 5G est un élément important dans le développement de l'Internet des objets (IoT) en offrant des vitesses de données massives (10 Gbit/s) et la possibilité de connecter des milliards d'appareils intelligents. Ces nouvelles capacités permettent le développement d'applications innovantes dans divers secteurs, encourageant les entreprises à investir massivement dans des solutions de gestion de la connectivité 5G pour améliorer les systèmes IoT existants. L'Internet industriel des objets (IIoT) est également confronté à de multiples défis tels que l'évolution des exigences en matière de produits et l'évolution des modèles commerciaux. et l'intégration des technologies de communication avancées. Bien que les réseaux cellulaires existants ne répondent pas toujours aux besoins de communications de machine à machine (MTC), la technologie 5G-IoT offre des solutions prometteuses en offrant des vitesses de données exceptionnelles, une latence plus faible et une couverture améliorée pour les communications MTC **[4].**

## 1.7 Architecture de l'internet des objets :

L'architecture de l'Internet des Objets (IoT) est fréquemment discutée dans les travaux de recherche sur le sujet. Une architecture en cinq couches est couramment reconnue comme étant la plus représentative pour décrire l'IoT**.** Voici une description des cinq couches de cette architecture comme illustré dans la Figure **1.4 :**

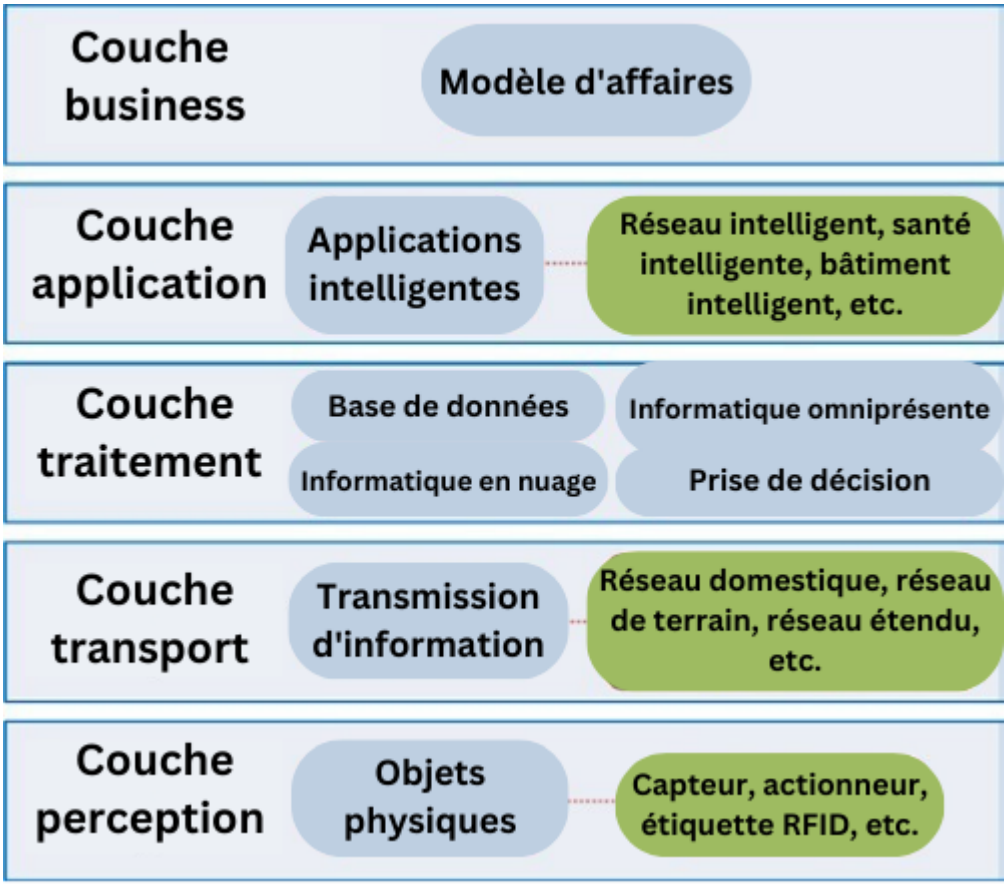



**Figure 1.4 :** L'architecture en cinq couches de l'internet des Objets (IoT) **[7].**

- **Couche de business :** La couche supérieure qui gère l'ensemble du système IoT y compris là Gestion des applications, les services et les politiques de sécurité. Elle est également responsable de la génération de modèles de revenus et de l'analyse des données pour optimiser les processus commerciaux et améliorer les prises de décision**.**
- **Couche application :** Cette couche offre la possibilité d'utiliser les informations traitées par la couche traitement et les services des objets présentés par cette dernière, pour développer diverses applications de l'IoT. Ces applications seront ensuite directement été utilisées par des utilisateur finaux **[7].**
- **Couche traitement ^couche Middleware ^ :** Cette couche est chargée de gérer et de relier les informations collectées aux bases de données, puis d'appliquer des traitements et des calculs afin de prendre des décisions automatiques. Cela permet également à un développeur d'applications IoT d'utiliser des services sans prendre en compte l'interopérabilité des objets ou une plate-forme matérielle spécifique **[8].**
- **Couche de transport :** Cette couche assure le transfert des données collectées par la couche de perception vers les plateformes de traitement de données via des réseaux, tels que l'internet, les réseaux LAN ou les réseaux cellulaires**.**

- **Couche réseau :** Cette couche s'occupe du transport de la donnée vers le centre de traitement de l'information. Le moyen de transmission peut être filaire ou non et les principales technologies utilisées dans cette couche sont la 3G, Wifi, ZigBee etc. C'est au niveau de cette couche que se trouvent les protocoles de communication tels que 6LowPan qui sont nécessaires pour l'adressage de millions d'objets connectés **[8].**
- **Couche perception :** C'est la première couche on l'appelle aussi couche objets. Elle représente les objets physiques de l'IoT qui ont pour but la collecte et le traitement basique de l'information et qui fournissent différentes fonctionnalités comme donner la position physique la température le poids le mouvementent etc. Cette couche collecte et numérise les données d'un certain environnement et les envoie à la couche supérieure via des canaux sécurisés**.**

## 1.8 Technologies fondatrices de l'IoT :

L'Internet des Objets (IoT) permet l'interconnexion des objets intelligents via Internet. Pour fonctionner, il nécessite plusieurs systèmes technologiques. Parmi celles-ci, on peut citer des solutions techniques telles que RFID, TCP/IP et les technologies mobiles. Ces technologies permettent d'identifier des objets, de capturer, stocker, traiter et transférer des données dans des environnements physiques, ainsi qu'entre des contextes physiques et virtuels. Bien qu'il existe de nombreuses technologies utilisées dans l'IoT, nous nous concentrerons sur quelques-unes qui sont essentielles pour son fonctionnement : RFID et WSN. Ces technologies sont définies ci-dessous**.**

### 1.8.1 RFID (Radio Frequency IDentification) :

Un système RFID est constitué d'un ou plusieurs lecteurs et d'un ensemble d'étiquettes, également connues sous les noms de tags, marqueurs, identifiants ou transpondeurs, à faible puissance. Ces étiquettes sont de petits dispositifs dotés d'une puce contenant des informations et d'une antenne pour la communication radio. Elles sont fixées sur les objets que l'on souhaite identifier ou tracer de manière unique. Les étiquettes peuvent prendre différentes formes et peuvent être passives ou actives. **[8].**

#### 1.8.1.1 La RFID passive :

Les étiquettes passives ne disposent d'aucune source d'énergie et attendent à ce qu'un signal électromagnétique leur arrive et munit de l'énergie pour pouvoir envoyer leurs propres signaux**.**

#### 1.8.1.2 La RFID active :

Les étiquettes actives sont équipées d'une batterie, elles diffusent des signaux automatiquement et d'une façon autonome**.** Les étiquettes passives sont plus déployées que celles qui sont actives car leur usage est beaucoup plus flexible avec un cout nettement réduit

(comparé au cout relatif aux étiquettesactives qui est nettement élevé). Une autre spécificité pas moins importante dans les étiquettes passives qui est la durée de vie. Par le fait d'être passive, la durée de vie de l'étiquette est importante (elle reste valable tant qu'elle garde son bon état), ce qui n'est pas le cas pour une étiquette active ou la durée de vie est restreinte (s'achève avec l'épuisement de la batterie) **[9].**

Les étiquettes RFID permettent une identification et un suivi automatisés des objets à l'aide d'ondes radio, facilitant ainsi la gestion et la logistique. Comme illustré la figure suivante **:**

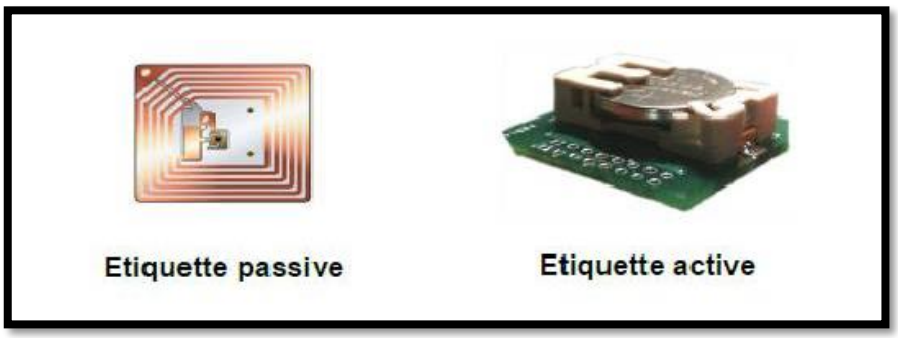



**Figure 1.5 :** Les étiquettes RFID **[8].**

### 1.8.2 Les réseaux de capteurs sans fil :

Les réseaux de capteurs sans fil **(WSN)** se composent généralement d'un grand nombre de nœuds de capteurs miniatures, qui peuvent être fixes ou mobiles, et sont souvent déployés de manière aléatoire dans un bassin versant. Ce champ de captage constitue souvent un environnement hostile, isolé ou difficile à contrôler. La tâche principale de chaque nœud de capteur est de collecter indépendamment des informations précises sur l'environnement de déploiement. Selon le type de nœud de capteur, les données collectées peuvent inclure la température, l'humidité, la pression, la lumière ou d'autres paramètres. Les nœuds de capteurs d'un WSN communiquent entre eux via des liaisons radio pour transmettre les données collectées à un nœud central appelé « point de collecte », également appelé station de base ou puits. Cette station peut être connectée à un appareil puissant appelé gestionnaire de tâches en ligne ou par satellite. De plus, le réseau peut être configuré de manière à ce que l'utilisateur puisse envoyer des requêtes spécifiques aux capteurs, spécifiant les informations requises et ciblant les nœuds de capteurs concernés **[8],** comme illustré dans la figure suivante **:**

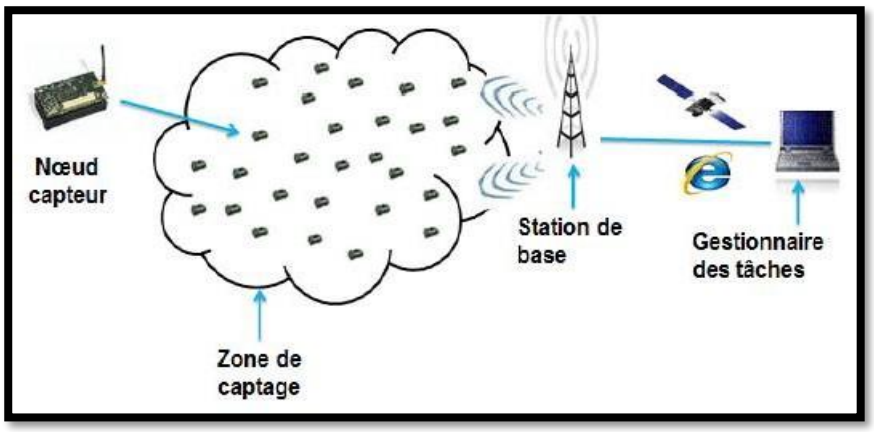



**Figure 1.6 :** Architecture de communication d'un réseau de capteur sans fil **[8].**

Les RCSFs jouent un rôle très intéressant dans l'Internet des objets. En effet, les capteurs permettent la représentation des caractéristiques dynamiques (température, humidité, pression, mouvements, . . .) des objets et des endroits du monde réel dans le monde virtuel représenté par le réseau Internet global. Ainsi, avec l'incorporation des réseaux de capteurs dans l'Internet, Les capteurs deviennent des serveurs (fournisseurs de services) dans ce que l'on désigne par le web des objets (dit WoT pour Web of Things) Ainsi, les services (applications) des RCSFs se rajoutent à l'ensemble des services et applications de l'Internet de futur qui réunira une variété de réseaux fortement hétérogènes (que _ ca soit sur le plan matériel ou logiciel), soumis à des contraintes différentes et qui sont déployés pour diverses applications, afin d'en avoir un monde réel très sophistiqué. En plus de ces deux technologies principales (RFID et RCSFs), on trouve également d'autres technologies qui contribuent à la concrétisation du principe de l'Internet des objets. On parle alors des systèmes embarqués et la nanotechnologie (rétrécissement et incorporation des capteurs et autres dispositifs miniatures dans les objets à faire connecter à Internet) **[8]**, comme montré dans la figure suivante **:**

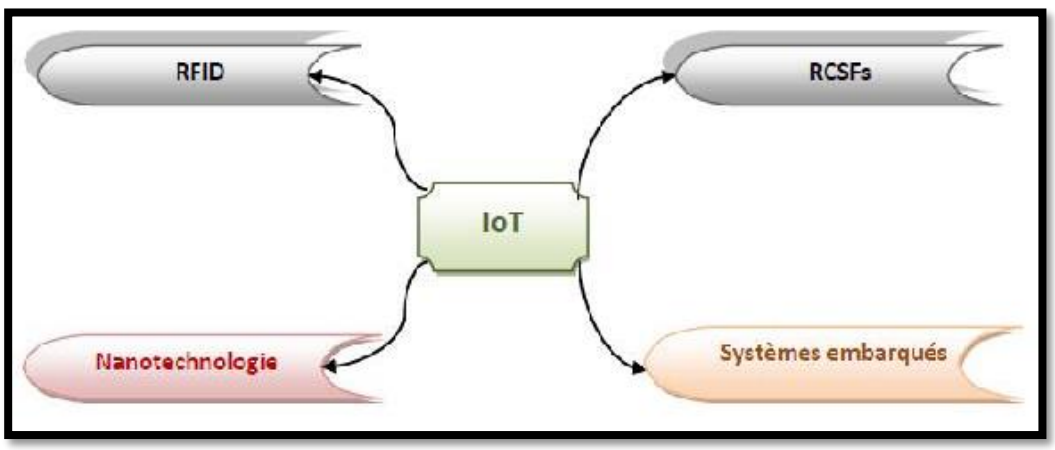



**Figure 1.7 :** Technologies fondatrices de l'internet des objets **[8].**

## 1.9 Protocoles de fonctionnement de L'IoT :

De nombreuses normes IoT ont été proposées pour faciliter et simplifier les tâches des programmeurs d'applications et des fournisseurs de services. Divers groupes ont été créés pour fournir des protocoles, y compris les efforts menés par le W3C, l'IETF, Global EPC, l'IEEE et l'ETSI. L'objectif de l'Internet des objets est de permettre à chaque système de communiquer avec tous les autres systèmes en utilisant des protocoles communs. La mise en œuvre à grande échelle du concept IoT repose en grande partie sur la standardisation de la communication entre les objets, appelée M2M (Machine to Machine) **[1].**

- Au niveau de la couche de liaison, le standard **IEEE 802.15.4** est plus adapté que l'Ethernet aux environnements industriels difficiles.
- Au niveau réseau, le standard 6loWPan a réussi à adapter le protocole IPV6 aux communications sans fil entre nœud à très faible consommation.
- Au niveau routage, l'IETF a publié en 2011 le standard RPL.
- Au niveau de la couche application le protocole CoAP qui tente d'adapter http, beaucoup trop gourmand aux contraintes des communications entre nœuds à faible consommation.

### 1.9.1 CoAP (Constrained Application Protocol) :

Il s'agit d'un protocole de couche application pour les applications IoT. Il définit un protocole de transport Web basé sur la fonctionnalité HTTP et se lie par défaut à UDP (et non à TCP), ce qui le rend plus adapté aux applications IoT. De plus, CoAP modifie certaines fonctionnalités de HTTP pour répondre aux exigences de l'IoT telles qu'une faible consommation d'énergie et un fonctionnement en présence de liaisons avec perte et bruyantes**.** CoAP est construit sur REST, qui est un moyen plus simple d'échanger des données entre clients et serveurs via HTTP. CoAP vise à permettre aux petits appareils dotés de faibles capacités de consommation, de calcul et de communication d'utiliser les interactions RESTful avec CoAP**.**

### 1.9.2 MQTT (Message Queue Telemetry Transport) :

MQTT est un protocole de messagerie idéal pour les communications IoT et M2M. Il est conçu pour connecter des appareils et des réseaux embarqués à des applications et des middlewares. Il est idéal pour les appareils aux ressources limitées qui utilisent des liaisons peu fiables ou à faible bande passante. Construit sur le protocole TCP, MQTT se compose de trois composants principaux : les abonnés, les éditeurs et les médiateurs. De nombreuses applications utilisent MQTT, telles que les soins de santé, la surveillance, les compteurs d'énergie et les notifications Facebook. En conséquence, MQTT permet de diriger des appareils petits, de faible consommation et à faible mémoire vers des zones vulnérables et des réseaux à faible bande passante **[1].**

### 1.9.3 XMPP (Extensible Messaging and Presence Protocol) :

XMPP Est une Norme de messagerie instantanée IETF (IM) qui est utilisé pour les conversations Multipartis, les appels vocaux et vidéo et la télé présence. Il permet aux utilisateurs de communiquer entre eux en envoyant des messages instantanés sur Internet quel que soit le système d'exploitation qu'ils utilisent. XMPP permet aux applications de messagerie instantanée d'accéder à l'authentification, au contrôle d'accès, à la mesure de la confidentialité, au cryptage hop-by-hop et à la compatibilité avec d'autres protocoles. Beaucoup de fonctionnalité XMPP en font un des protocoles Préfères par la plupart des applications de messageries instantanées et pertinentes Dans le cadre de l'IoT. Il fonctionne sur une variété de plateformes basées sur Internet de manière décentralisé. XMPP est sécurisé et permet d'ajouter de Nouvelles applications au-dessus des protocoles de base **[10].**

### 1.9.4 AMQP (Advanced Message Queuing Protocol) :

AMQP est un protocole de couche d'application ouvert standard pour l'IoT, axé sur les environnements orientés messages. Il nécessite un protocole de transport sécurisé comme TCP pour l'échange de messages. Il prend en charge une communication fiable via des primitives de garantie de livraison de messages, et en définissant un protocole au niveau du fil, les implémentations AMQP peuvent interagir entre elles. AMQP prend également en charge le modèle de communication publié**.**

Les communications sont gérées par deux composants principaux **:**

- **Échanges et files d'attente de messages :** Les échanges sont utilisés pour acheminer les messages vers les files d'attente appropriées.
- **Routage :** Le routage entre les échanges et les files d'attente de messages repose sur certaines règles et conditions prédéfinies. Les messages peuvent être stockés dans les files d'attente, puis envoyés au récepteur ultérieurement.

## 1.10 Domaines d'utilisation :

Le marché des objets connectés est promis à une grande croissance dans les années à venir car il a une valeur immense dans les différents domaines d'objets connectés pour les professionnels. Cependant, seules quelques applications sont actuellement déployées**.** Les domaines d'application de l'IoT sont très nombreux, et touchent pratiquement tous les axes de la vie quotidienne des individus, Parmi ces domaines, nous citons quelques exemples **[7],** comme illustré dans la figure suivante **:**

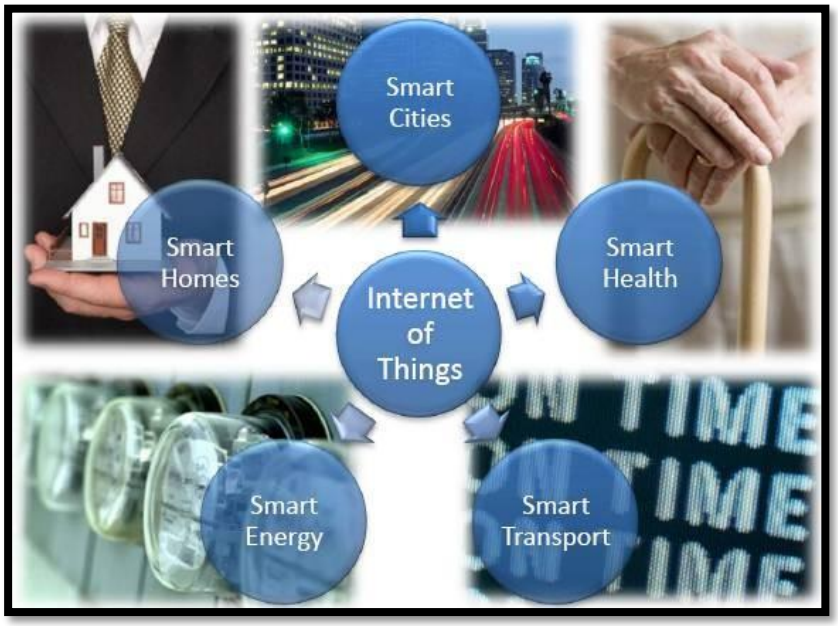



**Figure 1.8 :** L'internet des objets et la création d'espaces intelligents **[3].**

### 1.10.1 L'internet des objets dans le domaine de la santé :

Les objets connectés peuvent servir à réduire quelque élément de dépenses pour les remplacer par d'autres il permet aussi de favoriser l'hospitalisation à domicile, qui assurera le contrôle et le suivi des signes cliniques des patients par la mise en place des réseaux personnels de surveillance, ces réseaux seront constitués de bio-captures posés sur le corps des patients ou dans leurs lieux d'hospitalisation. Cela facilitera la télésurveillance des patients qui permettras de réduire les erreurs médicales, optimiser la consommation de médicaments ou encore leur prise régulière, et même encourager la prévention de certaines maladies, l'internet des objets permettre aussi de suivre sa tension, son rythme cardiaque, la qualité de sa respiration ou encore sa masse graisseuse, et d'autres objets connectés médicaux, brosse à dent connectée ou encore, le scanner ui calcule le nombre de calories dans votre assiette **[1],** comme illustré dans la figure suivante **:**


**Figure 1.9 :** L'IoT dans le domaine de la santé **[9].**

### 1.10.2 L'internet des objets dans le domaine d'éducation :

Dans le domaine de l'éducation, les solutions mobiles adapteront le processus d'apprentissage aux besoins de chaque élève, améliorant les niveaux de compétence générale, tout en reliant les salles de classe virtuelles et physiques pour rendre l'apprentissage plus pratique et accessible **[11]**. Comme montré dans la figure suivante **:**

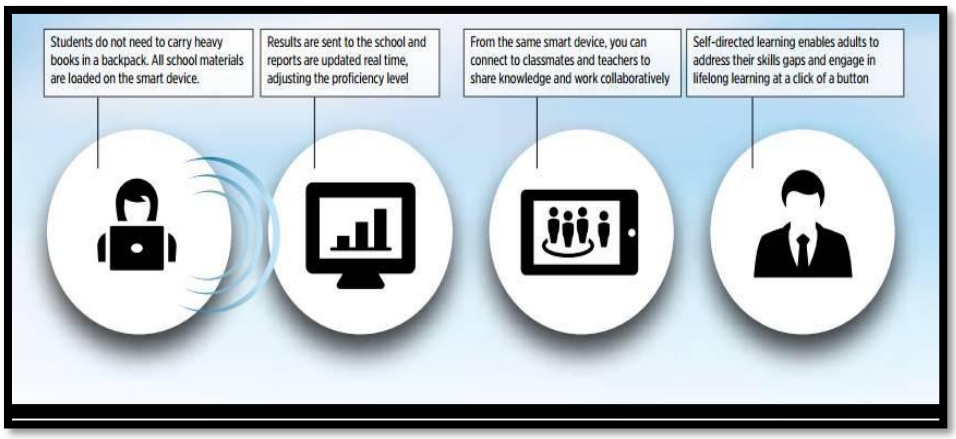



**Figure 1.10 :** L'IoT dans le domaine d'éducation **[11].**

### 1.10.3 L'internet des objets dans le domaine de l'industrie :

Le déploiement de L'IoT dans l'industrie sera certainement un grand support pour le développement de l'économie et le secteur des services, puisque L'IoT permettra d'assurer un suivi total des produits, de la chaine de production, jusqu'à la chaine logistique et de distribution en supervisant les conditions d'approvisionnements. Cette traçabilité de bout en bout facilitera la lutte contre la contrefaçon, la fraude et les crimes économiques transfrontaliers**.** Pour les entreprises, la capacité de l'IoT à combiner les innovations en matière d'analyse de données, d'impression 3D et de capteurs améliorera la productivité en permettant un changement radical dans la qualité de la prise de décision, l'efficacité de la production, la personnalisation de la distribution et la productivité de la production alimentaire **[11],** Comme montré dans la figure suivante **:**

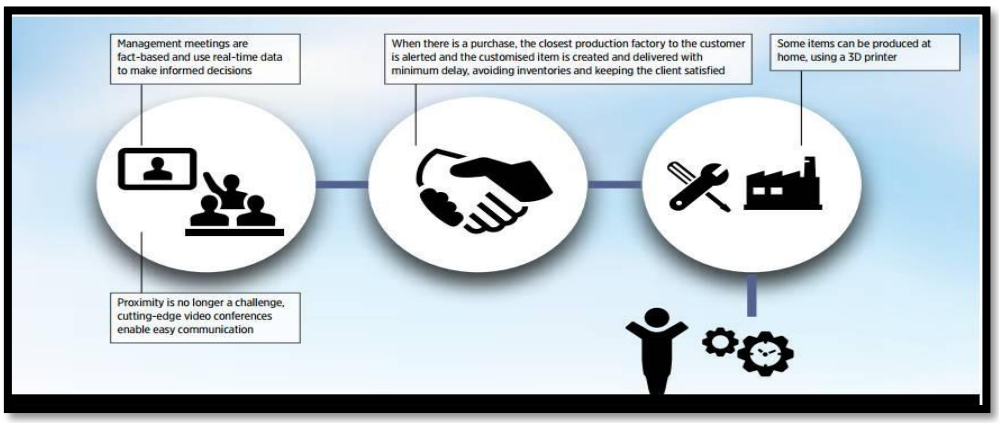



**Figure 1.11 :** L'IoT dans le domaine de l'industrie **[11].**

## 1.11 Exigences relatives à la mise en œuvre de L'IoT :

Les exigences d'implémentation de l'IoT sont considérées comme des exigences critiquespour les prochaines architectures d'IoT, qui sont décrites dans les sous sections suivantes **:**

### 1.11.1 Évolutivité :

Avec le grand nombre d'objets connectés à l'infrastructure IoT , on considère que chaqueobjet connecté a sa propre représentation virtuelle. Par conséquent, l'exigence d'évolutivité est souhaitable pour étendre la fonctionnalité des normes ouvertes aux futures applications IoT . En outre, alors que l'expansion de l'IoT se développe grâce à l'adoption généralisée de nouvelles applications, les futures architectures d'IoT doivent répondre aux exigences d'évolutivité **[12].**

### 1.11.2 Interopérabilité :

La nécessité d'habiliter les communications entre divers objets par différents fournisseurs de services est très importante dans les futures architectures d'IoT. Par conséquent, les architectures d'IoT exigent des normes d'interopérabilité pour créer des plates-formes parallèles ou ouvertes qui prennent en charge le potentiel global de la pratique de connexion transparente entre tous les types d'applications et de dispositifs IoT. En outre, pour permettre les pratiques de communication entre toutes les choses dans les futures architectures d'IoT, quelle que soit leur origine**.**

### 1.11.3 Sécurité :

Le renforcement de la sécurité est un aspect important des applications IoT, en raison de la tâche difficile de protéger les informations sensibles transmises et traitées dans les environnements hostiles entourant l'IoT. Ainsi, on peut vraiment considérer qu'il s'agit d'une exigence clé future des déploiements d'applications IoT pour éviter que ces grandes échelles d'applications IoT ne soient contrôlées par des parties non autorisées. En outre, les mécanismes de sécurité de la stratégie de conception de l'IoT devraient être suffisamment légers en raison des ressources limitées dont disposent les dispositifs IoT. En conséquence, l'absence de politique de sécurité des futures architectures d'IoT peut menacer la confiance de l'utilisateur, ce qui conduira à l'échec de la technologie dans son ensemble **[12].**

### 1.11.4 Contrôle et gestion des ressources :

L'accessibilité et la configuration des objets intelligents participants parmi les applications IoT doivent être réalisées à distance. Cela aidera à contrôler efficacement les ressources si les administrateurs ne sont pas disponibles à certains endroits. En outre, des contraintes redondantes en matière de ressources peuvent affecter les systèmes IoT, qui doivent équilibrer la charge pour une utilisation appropriée des ressources **[12].**

### 1.11.5 Efficacité énergétique :

La durée de vie est l'appréhension de durabilité la plus fonctionnelle dans les objets intelligents que la participation parmi les applications IoT. Par conséquent, la sensibilisation à l'énergie est très importante pour réduire les contraintes de ressources en éliminant la consommation d'énergie redondante. En conséquence, la stratégie de conception de l'architecture IoT devrait être de minimiser la consommation d'énergie par le développement de propriétés légères des techniques et méthodes de communication**.**

### 1.11.6 Qualité de service (QoS) :

La capacité de fournir un service satisfaisant aux utilisateurs est une exigence importante des architectures de systèmes IoT. La QoS est un facteur d'installation non fonctionnel, qui peut être obtenu en organisant les services fournis et en les récupérant. Par exemple, les applications de traitement en temps réel imposent une priorité élevée aux performances typiques. En conséquence, seules les informations obligatoires doivent être récupérées en réponse à la demande adressée **[12].**

## 1.12 Conclusion :

Il est évident que les applications des IoT deviennent de plus en plus prépondérantes. Nous avons fixé l'objectif de développer des applications sécurisées dans cette technologie,nous allons commencer par une étude des IoT. Tout au long de ce chapitre, nous avons délibérément choisi des définitions simples concernant l'internet des objets dans le but d'enlever l'ambigüité et de démystifier certaines confusions. Ce premier chapitre nous a permis de comprendre certaines généralités sur la technologie "IoT", de lui donner une définition d'un point de vue globale, une meilleure vision sur ce réseau et il nous permet de visionner son domaine d'utilisation, ainsi son mode de fonctionnement ont été présentés, son architecture et enfin les exigences que peut représenter un tel réseau. Tous cela nous donne un aperçu général sur la technologie IoT, et nous permet d'avancer au chapitre suivant et nous essayer d'expliquer comment connecter les objets à internet**.**

# Chapitre 2
# Les objets IoT

**2 Introduction :**

L'internet des objets (IoT) est un environnement hyper-connecté qui permet des interactions infinies entre les objets physiques et leurs représentations virtuelles. Ce chapitre résume les fondements de base des objets connectés et passe en revue les défis auxquels est confronté le développement de l'IoT, tels que la sécurité des réseaux, la reconnaissance des objets, le déploiement d'IPv6, la consommation d'énergie, la confidentialité et l'authentification. Cela explique également la différence entre l'IoT et le M2M (communication de machine à machine)**.**

**2.1 Identification de la technique utiliser :**

**2.2 Définition d'un objet :**

Un objet est, avant toute chose, une entité physique ; par exemple, un livre, une voiture, une machine à café électrique ou un téléphone mobile. Dans le contexte précis de l'Internet des objets, cet objet possède au minimum un identifiant unique attaché à une identité exprimantd'une part ses propriétés immuables (type, couleur, poids, etc.) et son état c'est-à-dire l'ensemble de ses caractéristiques pouvant évoluer au cours du temps (position, niveau de batterie, etc.)**.** Dans le langage courant, ce sont les termes « objet connecté », parfois « objet intelligent »et parfois « objet interactif » qui sont les plus utilisés12 tandis que dans les travaux de recherche universitaire, on retrouve plutôt la terminologie « objet communicant » **[15].**

Le dictionnaire Larousse propose pour les différents mots entrant dans la composition de ces expressions, les définitions suivantes **:**

- **Objet :** « Chose solide considérée comme un tout, fabriquée par l'homme et destinée à un certain usage »**.**
- **Connecter :** « Unir, lier des choses entre elles » et au sens technique « Établir une liaison électrique, hydraulique, entre divers organes ou machine » ou « Etablir une liaison avec un réseau informatique ».
- **Intelligent :** « Se dit d'un bien dont la maintenance ou le fonctionnement sont assurés par un dispositif automatisé capable de se substituer, pour certaines opérations, à l'intelligence humaine »**.**
- **Interactif :** « Support de communication favorisant un échange avec le public »
- **Communication** « Se dit d'une chose qui communique avec une autre » **[15].**

**2.3 Définition d'un objet connecté :**

C'est un dispositif permettant de collecter, stocker, transmettre et traiter des données issues du monde physique**.** Un objet connecté doit être adopté à un usage, il a une certaine forme d'intelligence **[16].** Identifiés et Identifiables de façon unique et ayant un lien direct ou indirect via un concentrateur « Gateway » avec Internet **[10].**

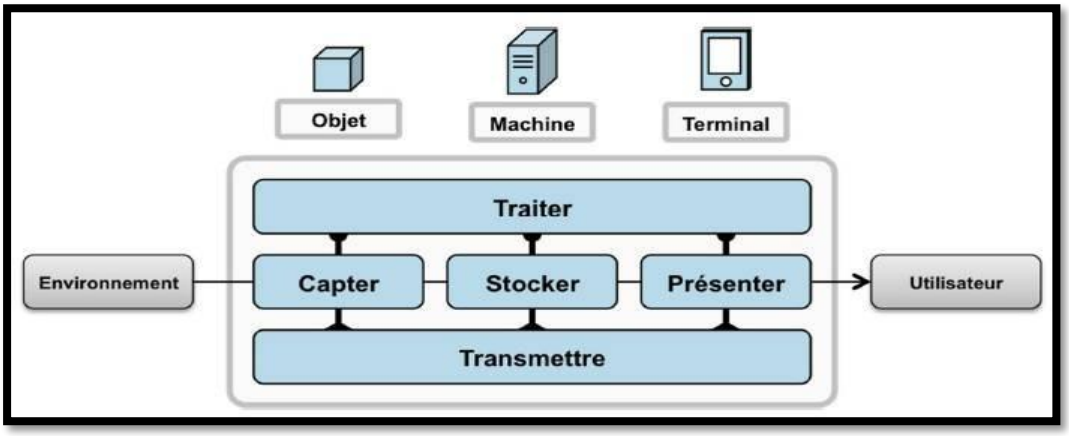



**Figure 2.1 :** Collecte de données **[10].**

L'objet connecté, intelligent, interactif ou communiquant est donc un artefact fabriqué par l'homme pour établir une liaison afin de pouvoir transmettre des informations à un autre objet connecté de manière automatisée et en favorisant ainsi un échange avec l'utilisateur **[15].**

Cette définition générale ne spécifie pas comment et par quels moyens techniques les objets communiquent ainsi elle englobe « n'importe quel objet relié au réseau électrique ». C'est par cette distinction que l'on peut différencier les objets connectés de première génération tels que l'ordinateur, le Smartphone ou la tablette simplement reliés à Internet, de la seconde génération d'objets connectés entre eux via l'Internet des Objets **[15],** Comme montré dans la figure suivante **:**


**Figure 2.2 :** Deux générations d'objets connectés **[15].**

Un objet connecté peut interagir avec le monde physique de manière indépendante sans intervention humaine. Il possède plusieurs contraintes telles que la mémoire, la bande passante ou la consommation d'énergie, etc. Il doit être adopté à un usage, il a une certaine forme d'intelligence, une capacité de recevoir, de transmettre des données avec des logiciels grâce aux capteurs embarqués **[16].** Un objet connecté a une valeur lorsqu'il est connecté à d'autres objets et briques logicielles, par exemple : une montre connectée n'a d'intérêt qu'au sein d'un écosystème orienté santé/bien-être, qui va bien au-delà de connaître l'heure.

Un objet connecté à trois éléments clés **:**

- Les données produites ou reçues, stockées ou transmises.
- Les algorithmes pour traiter ces données.

- L'écosystème dans lequel il va réagir et s'intégrer **[17].**

Objets connectés Comme montré dans la figure suivante **:**

**Figure 2.3 :** Quelques exemples d'objets connecter **[8].**

## 2.4 Types d'objets :

### 2.4.1 Les objets passifs :

Ils utilisent généralement un tag (puce RFID, code barre 2D). Ils embarquent une faible capacité de stockage (de l'ordre du kilo-octet) leur permettant d'assurer un rôle d'identification. Ils peuvent parfois, dans le cas d'une puce RFID, embarquer un capteur (température, humidité) et être réinscriptibles **[10].**

### 2.4.2 Les objets actifs :

Ils peuvent être équipés de plusieurs capteurs, d'une plus grandecapacité de stockage et être doté d'une capacité de traitement ou encore être en mesure de communiquer sur un réseau **[10].**

## 2.5 Classification des objets :

Les objets, choses ou things issus de l'Internet des Objets (Internet of Things) vont s'influencer les uns les autres en fonction de leurs capacités fonctionnelles (par exemple, la puissance de calcul, la connectivité réseau, la puissance disponible, etc.) ainsi que du contexte et des situations **[18].**

Expliquer le fonctionnement de l'Internet des objets, qui n'est ni plus ni moins qu'un équipement connecté à un réseau de communication **[4],** Comme montré dans la figure suivante **:**

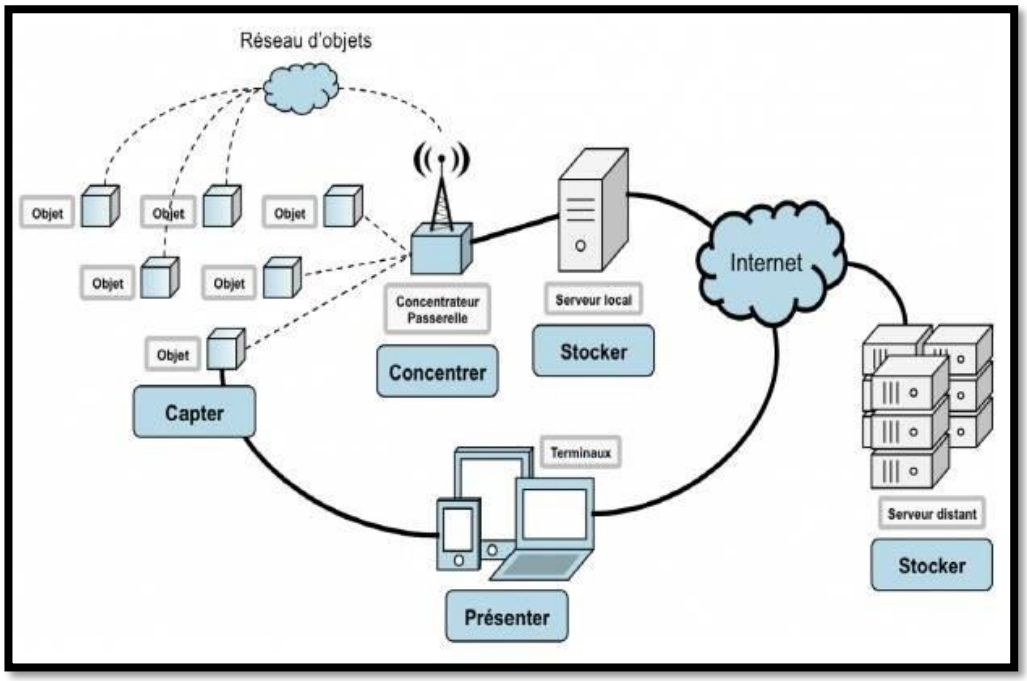



**Figure 2.4 :** Mode d'opération des IoT **[4].**

## 2.6 Précisons le rôle des différents processus présentés sur ce schéma :

- **Capter :** Désigne l'action de transformer une grandeur physique analogique en un signal numérique**.**
- **Concentrer :** Permet d'interfacer un réseau spécialisé d'objet à un réseau IP standard (ex. Wifi) ou des dispositifs large public**.**
- **Stocker :** Qualifie le fait d'agréger des données brutes, produites en temps réel, méta taguées, arrivant de façon non prédictible**.**
- **Présenter :** Indique la capacité de restituer les informations de façon compréhensible par l'Homme, tout en lui offrant un moyen d'agir et/ou d'interagir **[10].**

Un objet connecté peut être contrôlé à distance et remplit généralement deux rôles **:**

- Un rôle de capteur pour surveiller l'apparition d'un événement ou d'une mesure spécifique (capteur de présence, capteur thermique, mesure du nombre de pas…).
- Un rôle d'actionneur pour réaliser une action suite à un événement spécifique mesuré ou détecté (déclenchement d'une alarme en cas d'intrusion, ouverture d'une porte à distance,) **[19].**

## 2.7 Cycle de vie d'un objet connecté dans l'IoT :

Dans l'IoT, les objets intelligents passent par trois étapes :

La phase préparatoire (bootstrapping), la phase opérationnelle et la phase de maintenance**,** comme le montre la figure suivante **:**

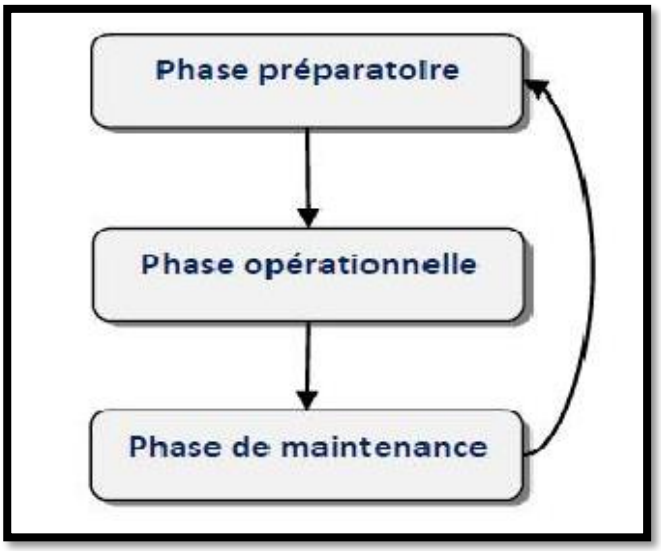



**Figure 2.5 :** Cycle de vie de l'objet **[8].**

- **La phase préparatoire (bootstrapping) :** Déploiement des objets (capteurs, tags), leur configuration avec les informations nécessaires, par exemple les identificateurs, les clés de sécurité, etc.
- **La phase opérationnelle :** dans la phase opérationnelle, l'objet connecté se met à réaliser sa mission qui diffère d'une application à une autre**.**
- **La phase de maintenance :** Effectuer des mises à jours, régler les problèmes en faisant d'éventuelles réparations des objets en cas de défaillances par exemple. Il est même possible de remplacer carrément des objets et redémarrer à nouveau à partir de la phase préparatoire **[8].**

### 2.8 Les types de relation entre objets :

L'interaction sociale entre deux individus reflète le rattachement entre eux et qualifie la relation qui les unie. Le type de relation traduit le lien social entre les interlocuteurs, et l'intensité de parenté qui les lie. Il peut influer fortement sur la nature de leurs interactions **[20].** Par analogie aux types de relation entre les individus, des travaux ont proposé une classification des types de relation relative aux objets communicants, sur la base des cinq types de relations suivantes **:**

#### 2.8.1 Relation de Co-localisation :

Lorsque des objets sont présents simultanément au même endroit (sur une machine, dans un atelier, une maison, une ville,)

#### 2.8.2 Relation de Co-travail :

Lorsque des objets coopèrent ensemble dans une même application ou un même processus, pour réaliser une tâche ou un but collectif**.**

### 2.8.3 Relation de parenté :

Lorsque des objets appartiennent à une même famille (objets similaires, même catégorie, construits dans une même période, par le même fabricant, appartenant à un même lot) **[20].**

### 2.8.4 Relation de propriété :

Lorsque des objets appartiennent au même propriétaire et interagissent entre eux. L'objet peut être porté par son propriétaire (une personne, une machine ou un autre objet). Le propriétaire peut stimuler l'interaction des objets**.**

### 2.8.5 Relation sociale :

Lorsque des objets se rencontrent et entrent en contact, de façon sporadique ou continue, au travers de la rencontre physique de leurs propriétaires respectifs. L'aspect social de l'interaction entre objets décline de l'interaction sociale entre leurs propriétaires **[20].**

## 2.9 Caractéristiques fondamentales de l'internet des Objets

Les objets connectés se définissent en termes d'identité, d'inter connectivité, de « Shadowing» de sensibilité et d'autonomie… **[21].**

### 2.9.1 Sensibilité à son environnement :

Un objet peut transmettre des informations non seulement sur son propre état, mais aussi sur les caractéristiques de son environnement. Il peut ainsi avoir des capteurs signalant les niveaux de température, d'humidité, de vibrations, d'emplacement ou de bruit. Il peut enfin être en mesure d'enregistrer et/ou de diffuser des informations audio ou vidéo, si la bande passante disponible est suffisante **[21].**

### 2.9.2 L'inter connectivité :

Tous les objets présents dans l'Internet des Objets peuvent être connectés à l'infrastructure mondiale de l'information et de la communication (Union Internationale des télécommunications, 2012). Parmi les formes de connectivités les plus connues entre L'IoT et internet, nous retrouvons l'Ethernet. Cependant, tous les appareils peuvent se connecter via une large variété de mode de connexion et de technologies, qu'elles soient avec (Ethernet) ou sans fil. Comme le précise IBM Journal (2018), nous pouvons retrouver dans les options sans fil les technologies : ANT+, Bluetooth, EDGE, GPRS, IrDA, LTE, NFC, RFID, Weightless, WLAN, ZigBee, et ZWave **[18].**

### 2.9.3 Les changements dynamiques :

L'état des dispositifs (par exemple, connecté/déconnecté) change de manière dynamique tout comme le contexte dans lequel ces dispositifs fonctionnent qu'il soit relié au cadre spatio-temporel, comme le précise l'Union Internationale des télécommunications (2012) ou également

dans le cadre de la vitesse ou encore de la localisation comme l'indiquent Patel & Patel (2016). Il est importantde noter que leur nombre est également susceptible d'évoluer lui aussi **[18].**

### 2.9.4 Représentation virtuelle (shadowing) :

La notion de shadowing désigne le fait qu'un programme logiciel puisse tout connaître d'un objet physique et agir en son nom. Grâce à cela, même un objet physique « muet » peut avoir une représentation virtuelle relativement intelligente. Ceci est parfois désigné sous le nom de cyber-objet ou d'agent virtuel. Par exemple, une bouteille de lait peut avoir un identifiant unique et la capacité d'indiquer sa présence à un capteur local, situé dans le réfrigérateur. Dans un autre endroit, un programme (l'agent virtuel de la bouteille de lait) possède d'autres informations sur la bouteille (où elle a été achetée, quand elle se périme, etc.). Ce programme peut communiquer à son tour avec le frigidaire et indiquer ces informations à l'utilisateur **[22].**

### 2.9.5 Autonomie :

Les objets sont traités de manière individuelle, en général d'un point isolé, et opérés indépendamment d'un contrôle à distance. La notion d'apatridie est ici extrêmement importante il ne doit pas y avoir d'intelligence centrale contrôlant l'ensemble des objets individuels de manière totalitaire. Au contraire, chaque objet est en quelque sorte autonome et indépendant, avec la capacité d'être interrogé et d'interagir avec d'autres objets du réseau lorsque nécessaire **[22].**

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 et entre les objets physiques et leur représentation virtuelle **[21].**

### 2.9.6 La flexibilité :

Un objet peut interagir avec d'autres objets à n'importe quel moment (Any time), n'importe où (Any where), et n'importe comment (Any how), et fait des calculs pour n'importe quel objet (Anything), pour n'importe qui (Anyone), et pour n'importe quel service (Any service) **[23].**

## 2.10 Infrastructure de communication :

Dans leur majorité, les objets ne se connectent pas directement à internet mais via une passerelle ou un hub numérique **[19].**

L'infrastructure réseau la plus souvent mise en œuvre peut se représenter comme cela **:**

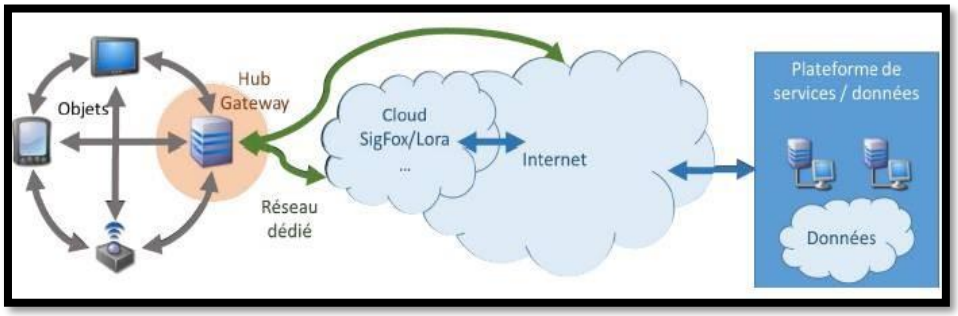



**Figure 2.6 :** Infrastructure réseau communément mise en œuvre pour les objets connectés**[19].**

Les objets connectés communiquent entre eux, ou avec les serveurs de traitement, prioritairement par le réseau Internet. Néanmoins, les types de liaison peuvent différer suivant les situations et les environnements : des objets peuvent partager directement entre eux des informations sur leur environnement pour interagir sans échanger avec des serveurs ; ou bien peuvent avoir besoin d'agréger les données avant de les transmettre à un serveur de traitement. Ils peuvent aussi être dans des zones à faible couverture avec un débit faible ou très éloignés d'un point d'accès réseau et dans ce cas utilisé un réseau dédié **[19].**

## 2.11 La sécurité du réseau :

Selon une étude de Hewlett Packard (2014), 70% desappareils IoT ont un manque crucial de sécurité. En effet, l'internet des objets est vulnérable à de nombreuses attaques pirates pour différentes raisons. Tout d'abord, à cause de la multitude de composantes, ces dernières ne pouvant être constamment sous surveillance et étant donc facilement sujettes à des attaques. Ensuite, les objets de L'IoT sont constamment connectés à l'internet au moyen de communications sans fil : ces dernières sont sécurisées dans l'Internet au moyen de cryptages, c'est à dire de clés qui permettent de crypter les informations transmises par les Objets. Le problème est qu'actuellement les appareils de L'IoT ne sont pas encore assez puissants pour supporter ceschiffrements. Il est dès lors important de développer de nouveaux algorithmes plus efficients et requérant moins de puissance **[24].**

## 2.12 L'identification des objets connectés :

Le souci d'identification unique de tous les Objets connectés pose aussi problème. En effet, un des composants principaux à la sécurité d'un réseau est le principe d'identification unique des appareils. L'identification est l'action d'attribuer un numéro unique, appelée IP, à un objet pour empêcher toute confusion entre eux. Malheureusement, depuis le 03 février 2011, toutes les adresses IPv4 (4-bit) sont épuisées. Or cela représente un énorme frein au développement de l'internet des objets car ce dernier met justement en relation une multitude d'objet nécessitant une identification. Heureusement, des solutions sont déjà en cours de développement, telles qu'une nouvelle méthode d'adressage l'IPv6 **[24].** Dans l'IoT, la gestion de l'identité exige la

prise en compte d'une variété stupéfiante de types d'identité et de relations, qui doivent tous suivre quatre principes d'identité objet **:**

- L'identité d'un objet n'est pas la même que celle de ses mécanismes sous-jacents. L'appareil à rayons X du service de radiologie peut avoir une adresse IP, mais il devrait aussi avoir sa propre identité pour le distinguer des autres appareils.
- Un objet peut avoir une identité de base et plusieurs identités temporaires qui changent en fonction de son rôle.
- Un objet peut s'identifier grâce à son identité ou à ses particularités.
- Les objets connaissent l'identité de leurs propriétaires. Appareil qui contrôle la glycémie d'un utilisateur devrait savoir comment cette information s'inscrit dans l'état de santé générale de l'utilisateur.
- Les objets peuvent aussi se trouver dans des groupes, que certains mécanismes doivent gérer. unemaison peut avoir plusieurs appareils électroménagers que seuls certains résidents et visiteurs peuvent utiliser à des moments précis. Le réfrigérateur pourrait se verrouiller après minuit à tout résident ou adolescent en visite, mais rester ouvert pour les adultes **[25].**

La preuve d'identité est un élément important de la gestion de l'identité. Lorsque les développeurs créent un réseau mondial d'objets, ils doivent construire une infrastructure qui permet l'authentification mutuelle des objets. Il doit y avoir un équilibre entre une gestion centralisée et une approche distribuée et hiérarchique. Les mécanismes d'anonymisation et la création de pseudonymes sont également des éléments constitutifs importants. Comme l'IoT traite de contextes multiples, il est peu probable qu'une entité révèle son identité tout le temps. Dans un réseau de véhicules, par exemple, une voiture de police peut révéler son identité aux voitures et au personnel du poste de police, mais garder son identité cachée pendant le travail d'infiltration, sauf si elle interagit avec d'autres voitures de police **[25].**

### 2.13 Le déploiement du protocole IPv6 :

Le protocole IPv6 a été développé dans les années 1990 afin de succéder à l'IPv4 dont les capacités d'adressage apparaissaient insuffisantes pour faire face au développement de l'Internet. Il est devenu un standard officiel de l'IETF en 1998 et a fait l'objet de nombreux perfectionnements depuis **[9],** La figure correspondante illustrait le format d'adresse IPv6 **:**


**Figure 2.7 :** Format d'adresse IPv6 **[12].**

**IPv6** *(*Internet Protocol version 6*)* est un protocole réseau sans connexion de la couche 3 du modèle OSI *(*Open Systems Interconnection*)*. Grâce à des adresses de 128 bits au lieu de 32bits, IPv6 dispose d'un espace d'adressage bien plus important qu'IPv4. Cette quantité d'adresses considérable permet une plus grande flexibilité dans leur attribution et une meilleure agrégation des routes dans la table de routage d'Internet. La traduction d'adresse, qui a été rendue populaire par le manque d'adresses IPv4, n'est plus nécessaire. Avec ses 128 bits utilisés pour l'adressage des hôtes, ce système offre une espace quasi- inépuisable ($3,4*10^{38}$ adresses) pouvant soutenir l'attribution d'identifiants uniques à chaque nœud de l'Internet des Objets. Un autre avantage d'adopter ce système d'adressage pour les objets de l'Internet est celui de pouvoir tirer parti de nombreux protocoles existants sous IP, et effectuer des communications de bout-en-bout sans nécessiter de traduction (à travers un dispositif comme NAT) **[25].**

Une première approche consiste à utiliser la même architecture du monde Internet, avec sa pile de protocoles de communication, et de l'appliquer tout simplement au monde des objets communicants. En effet, le succès de l'utilisation du protocole IP, dans sa version IPv4, provient du fait qu'il a permis à des systèmes informatiques hétérogènes de dialoguer ensemble et d'être accessibles à distance à l'échelle planétaire. Malheureusement, aujourd'hui on arrive à l'épuisement de son espace d'adressage, limité à quatre milliards d'adresses. IPv4 ne pourra donc pas satisfaire les besoins des réseaux des objets communicants et attribuer une adresse IP à chacun d'entre eux. Devant cette pénurie, IPv6 semble être le standard adéquat qui permettrait de répondre aux besoins du monde de ces nombreux objets connectés. Avec IPv6, l'adressage des objets sera quasi illimité **[6].** Il est donc possible de créer des milliards de milliards d'adresses (2128) différentes en IPv6alors que l'IPv4 plafonne à quatre milliards d'adresses environ (232). Ceci permet de se passer du mécanisme de traduction d'adresse et du protocole NAT (Network Address translation) qui permet de regrouper plusieurs adresses privées autour d'une même adresse IPv4 publique. Ceci élimine un degré de complexité en permettant un adressage direct des abonnés **[12].** Simultanément, l'IPv6 remédie à certains inconvénients de l'IPv4 il utilise des entêtes de longueur fixe (40 octets) alors que celles de l'IPv4 varient de 20 à 60 octets, ce qui simplifie le routage. La fragmentation éventuelle des datagrammes ne se fait plus au niveau des

routeurs mais au niveau des machines émettrices qui reçoivent, éventuellement, un message d'alerte "Packet too big"**.** IPv6 incorpore également dans sa spécification le protocole sécurisé IPsec. Le protocole bien connu de couche 2 de l'IPv4, l'ARP (Address Resolution Protocol), permettant à un nœud de découvrir et d'identifier les autres nœuds situés sur un même segment, est remplacé par le protocole NDP (Neighbor Discovery Protocol) qui peut être sécurisé par une méthode cryptographique (SEND – Secure Neighbor Discovery Protocol), remédiant ainsi aux vulnérabilités du protocole ARP**.**

L'IPv6 n'a pas été développé pour répondre aux besoins de l'Internet des objets. Il offre cependant des atouts précieux pour répondre aux exigences de L'IoT **:**

- Un adressage sans limites permettant l'identification unique de chaque objet et l'extensibilité de n'importe quelle architecture.
- Le non recours au protocole ARP qui rompt dans l'ipv4, la connexion point à point**.**
  Environ **37 %** des connexions au serveur de Google se font en IPv6, comme illustré dans la figure suivante **:**

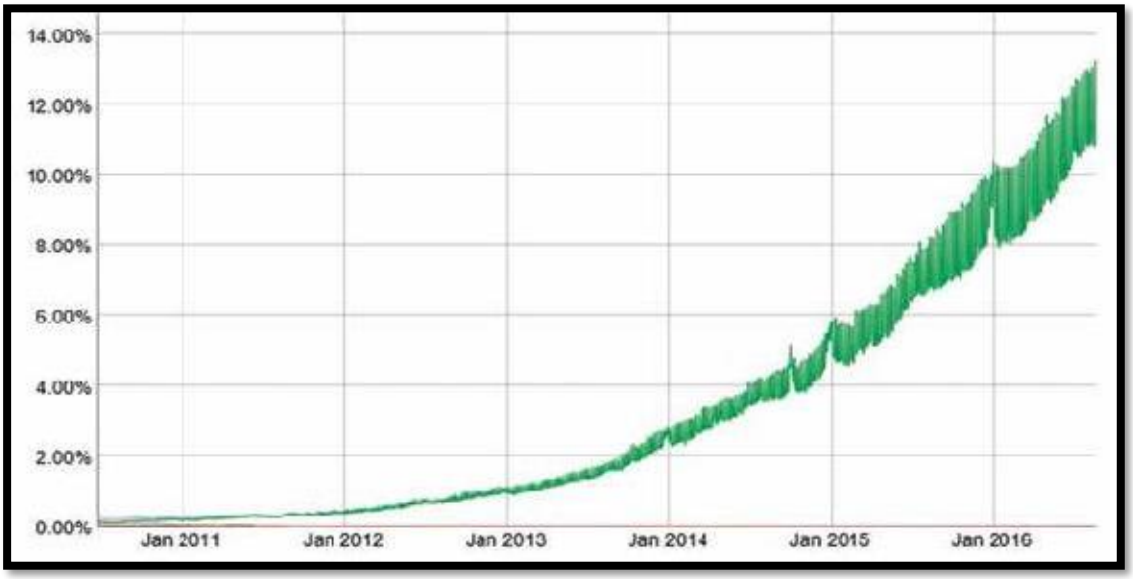



**Figure 2.8 :** Pourcentage des connexions aux serveurs de google s'effectuant en IPv6 **[12].**

### 2.14 La consommation énergétique « :

Ceci accentue un autre souci **:**

La consommation énergétique. L'IPv6 est un ensemble de protocoles complexes coûteux en mémoire et qui dès lors requiert une plus grande consommation électrique or l'alimentation électrique n'est à l'heure actuelle pas encore suffisante pour permettre au composants de L'IoT de supporter de tels schémas de sécurité.Il faudrait donc rendre les capteurs autosuffisants sans cela, le plein potentiel de l'internet des objets ne pourrait être exploité car il faudrait continuellement changer les « piles » de milliards de capteurs. Différentes recherches sont

continuellement menées dans le but de Trouver les technologies adéquates en terme d'autosuffisance et de prix. Actuellement, « American Chemical Society2 » a proposé une première solution intéressante pour le monde de la santé : les nano générateurs. Ce sont de petites puces flexibles qui génèrent de l'électricité sur base des mouvements du corps **[24].** Pour que L'IoT puisse démonter tout son potentiel, les capteurs devront être autosuffisants. Sinon on devait changer les batteries de milliards d'appareils déployés aux quatre coins de la planète et même dans l'espace, cela serait évidemment impossible, nous devons donc trouver un moyen pour générer de l'électricité en puisant dans l'environnement, par exemple en utilisant les vibrations, la lumière et les courants d'air. D'ailleurs, des scientifiques ont annoncé la création d'un nano générateur, il s'agit d'une puce flexible capable de générer de l'électricité à partir de mouvements corporels tels qu'un pincementde doigt**.**

### 2.14.1 Usages :

Le marché des objets connecté se développe à partir d'usages très varié, dont une part de plus en plus importante concerne des dispositifs autonomes et sans-fil : les capteurs pour la maison connectée, les objets portables (wearable technology), les balises de géolocalisation, les capteurs environnementaux, les systèmes embarqué non intrusifs, etc. Ces équipements disposent de leur propre source d'alimentation (batteries rechargeables ou piles) et communiquent par des protocoles radios optimisant la consommation énergétique**.** Le principe général. Est de permettre à l'équipement de fonctionner « en veille » la plupart du temps et de réveiller ses fonctions consommatrices uniquement lorsque l'usage prévu le nécessite, par exemple **:** la transmission de données à fréquence régulière ou l'envoi d'une alerte sur un évènement critique. Les contraintes d'usage peuvent nécessiter de concevoir des systèmes à même d'être opérationnels pendant une ou plusieurs années, sans remplacement ou recharge de batterie **[26].**

### 2.14.2 Technologies :

Les solutions permettant de répondre à ces enjeux impliquent d'avoir une approche globale lors de la conception du système, en partant de l'analyse précise des usages, des fonctionnalité requises et des différents organes techniques mis en œuvre. Des simulations, puis des tests de consommation d'énergie, sont effectué sur des prototypes pour valider ou ajuster la conception. Les axes d'optimisation les plus courants impliquent en particulier **:**

- De maximiser la réserve énergétique embarqué (la batterie), dans la limite des contraintes physiques**.**
- De limiter les phases de fonctionnement les plus consommatrices (optimisation des scénarios opérationnels et de l'algorithmique embarqué**.**

- De réduire la consommation lors des communications sur le réseau local ou distant **[26].**

### 2.15 Confidentialité des utilisateurs :

Le piratage informatique sera un problème majeur, L'IoT devrait croître de plus de 12 milliards d'appareils en 2016 et 50 billions en 2020. Chaque appareil est un point d'accès potentiel pour une attaque du réseau par les pirates. Dans une enquête faite là l'organisation Forester, partout dans le monde, 47 % des organisations industrielles qui utilisent ou envisagent d'utiliser l'IoT avait précédemment connu des violations de la sécurité dans leurs applications industrielles**.**

Pour ce qui est de la confidentialité, en robotique par exemple et ses divers utilities mettent à nu la vie privée de l'individu et ses pensées les plus profondes, ce qui peut être considérer comme une violation de la vie privée des personnes **[27].**

### 2.16 L'authentification :

Plusieurs obstacles importants restent à combler pour la réalisation de la vision de L'IoT dont le principal est la sécurité. La plupart des études et recherches Tendent à rendre leurs solutions applicables et utiles. Dans le domaine de la sécurité, Les chercheurs ont proposé diverses solutions pour permettre des communications Sécurisées entre les objets**.** L'authentification est une fonctionnalité importante et critique dans le contexte de L'IoT pour permettre une communication sécurisée entre les périphériques. En effet, un service d'authentification fournit la preuve que l'identité d'un Objet ou le sujet a l'identité qu'elle prétend avoir. Le terme "authenticité" désigne la propriété qui garantit qu'un partenaire de communication est bien celui qu'il prétend être. L'authentification est la première barrière de sécurité qui permet d'empêcher un utilisateur non autorisé d'accéder aux nœuds. Une personne non autorisée pourrait très bien accéder à un nœud donné, sans attendre qu'il envoie des données à un nœud puits. Il est donc requis d'avoir une authentification forte auprès de chaque nœud. Les mécanismes d'authentification sont capables d'empêcher les Utilisateurs d'accéder aux données des nœuds capteurs et de garantir la sécurité des données de manière efficace. L'authentification consiste à permettre à l'utilisateur légitime d'accéder aux ressources ainsi que de les refuser à une personne malveillante. Apres l'authentification, on a le contrôle d'accès qui permet de restreindre l'accès à l'utilisateur authentifie aux seules données dont il a les privilèges **[27].**

#### 2.16.1 Solutions :

Les solutions à considérer pour assurer l'authentification sont **:**

- **Mitiger les attaques par deni de service :** Il s'agit d'un gros problème dans les réseaux de capteurs dû aux ressources limitées des capteurs. Les faibles ressources des capteurs posent d'énormes problèmes dans tous les domaines de recherche sur les WSNs, dont la sécurité bien

sûr. Le Déni de Service abusant justement des ressources des systèmes semble être l'attaque parfaite pour une personne malintentionnée **[27].**

- **Détection et révocation de nœuds compromis :** L'authentification des utilisateurs doit mettre en place des mécanismes pour d´détecter activement et ainsi révoquer un nœud compromis**.**
- **Assurer la disponibilité des capteurs :** Les faibles ressources des capteurs posent d'énormes problèmes dans tous les domaines de recherche, dont la sécurité bien sûr. Le Déni de Service abusant justement des ressources des systèmes semble être l'attaque parfaite pour une personne malintentionnée. On a déjà du mal `à se protéger des dénis de service distribues avec les serveurs web **[27].**

### 2.17 La différence entre le M2M et L'IoT :

Le M2M et L'IoT sont des solutions qui proposent des accès à distance, à des objets ou des capteurs, comme illustré dans la figure suivante **:**

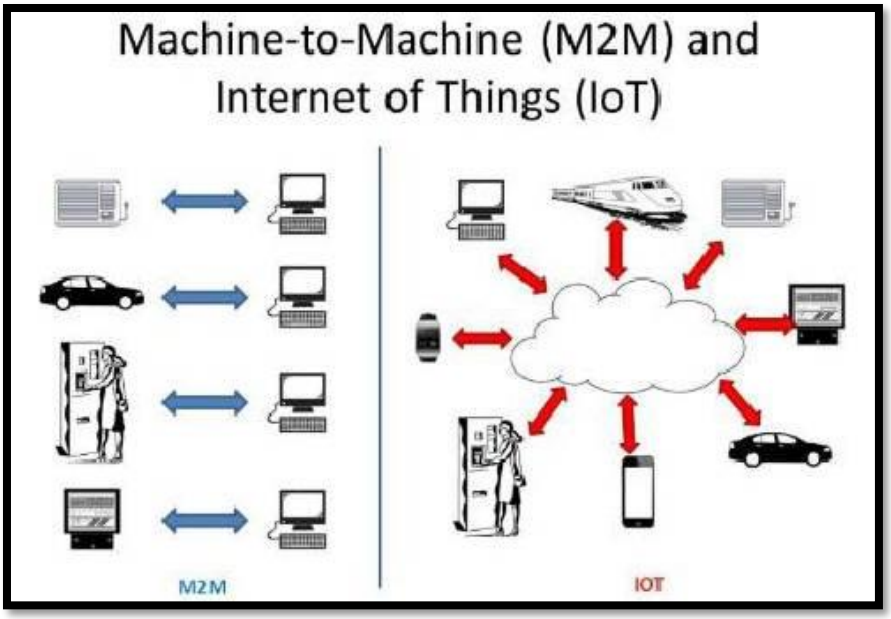



**Figure 2.9 :** Comparaison entre M2M et IoT **[14].**

**Le M2M** se définit traditionnellement par un réseau de télécommunication point à point utilisant un module cellulaire ou Wifi intégré, pour connecter des machines ou des objets à un réseau. L'intervention humaine n'est pas nécessaire, les informations circulent d'un endroit à un autre et peuvent être relayées via un serveur vers un logiciel **[14].**

**L'IoT** est considéré comme un système de système où chaque objet est identifié et communique avec une plateforme Cloud. Il induit une standardisation, des normes communes dans son fonctionnement. La plupart des objets connectés sont par exemple identifiés par une adresse IP, à l'instar d'un ordinateur raccordé à Internet. Le but est de récupérer, traiter, analyser

les informations, les données et de les stocker**.** Attention à ne pas confondre l'Internet des Objets et le Machine to Machine (M2M). Mêmesi la nuance est ténue, le M2M est considéré comme un sous-ensemble de L'IoT avec les particularités suivantes **:**

- Le M2M utilise les technologies de communication cellulaires qui sont des communications radio à débits et distances importants.
- Avec le M2M, il n'y a pas d'échanges entre les machines/objets distants, les flux d'informations se font en étoile, à partir, ou vers des serveurs centraux **[14].**

**2.18 Conclusion :**

Il existe donc de nombreux types d'objets connectés pouvant être utilisés par les entreprises ou les particuliers. On les trouve aujourd'hui principalement dans les secteurs de l'industrie, de l'énergie, de la santé et du bien-être, du transport, de la logistique et de l'automobile. Dans ce chapitre nous avons vue certaines notions des objets connectés nous avons aussi fait une partie un peu détailler sur les principales caractéristiques de l'IoT, leurs obstacles afin de bien comprendre la différence entre L'IoT et le M2M**.**

# Chapitre 3

# Simulation et interprétation des résultats

## 3 Introduction :

Dans ce chapitre, nous explorons la conception et la mise en œuvre d'un système de communication utilisant la technologie ZigBee pour interfacer un Raspberry Pi avec un ESP32 afin de transférer des données entre différents appareils. Le système comprend un ensemble de composants qui fonctionnent ensemble pour obtenir une transmission de données fiable et efficace, notamment la génération de nombres aléatoires, la simulation de canaux de communication bruyants, la réception et la transmission de données et le calcul des taux d'erreur de transmission. Chaque étape est illustrée à travers des modèles Simulink, fournissant une vue complète du processus de communication et garantissant des performances optimales du système.

### 3.1 Simulation pour un système de communication utilisant la technologie Zigbee :

### 3.2 Le schéma de simulation :

Nous avons choisi MATLAB comme logiciel de simulation d'un système de communication utilisant la technologie ZigBee, Voici une analyse détaillée des composants et du flux du signal **:**

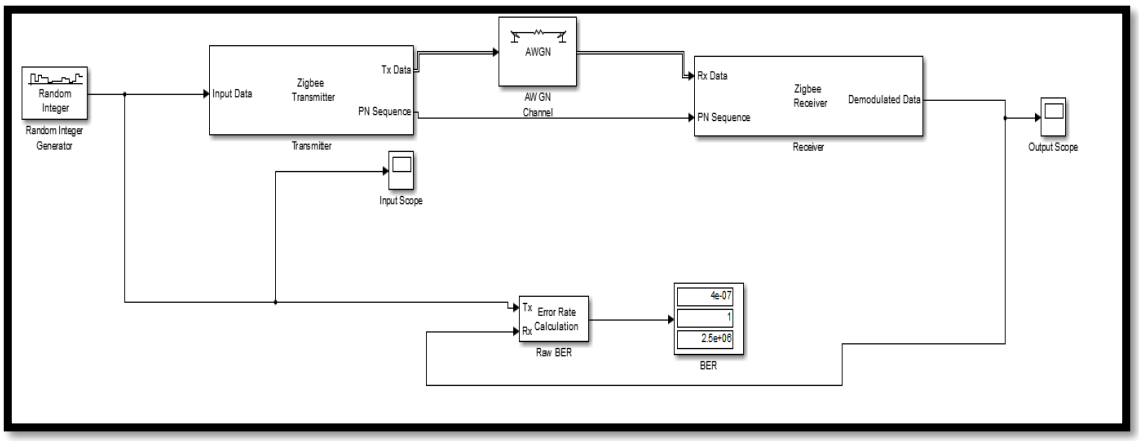



**Figure 3.1 :** Simulation d'un système de communication utilisant la technologie ZigBee**.**

- **Random integer generator :** Cet élément génère une série de nombres entiers aléatoires utilisés comme données d'entrée pour le système. **[28].**
- **Zigbee transmitter :** Cet élément prend les données d'entrée et les transmet sous forme de signal Zigbee**. [29]**
- **AWGN channel :** Ce canal ajoute du bruit à l'onde transmise pour simuler les conditions réelles des réseaux sans fil**. [29].**
- **Zigbee récepteur :** Cet élément reçoit le signal du canal et le démodule pour récupérer les données originales**.**

- **Input scope :** L'oscilloscope d'entrée est un outil de visualisation utilisé dans les systèmes de simulation et d'analyse pour afficher les signaux entrants. Il permet aux utilisateurs de surveiller et d'analyser les formes d'onde des signaux à différentes étapes du traitement pour vérifier leur intégrité et leur conformité aux attentes**. [30].**
- **Output Scope :** L'oscilloscope de sortie est un outil de visualisation utilisé dans les systèmes de simulation et d'analyse pour afficher les signaux de sortie. Il permet aux utilisateurs de surveiller et d'analyser les formes d'onde des signaux après qu'ils aient été traités par le système, afin de vérifier leur intégrité et leur conformité aux attentes. **[30].**
- **Tx Error Rate Calculation :** Le calcul du taux d'erreur de transmission est une méthode utilisée pour évaluer la performance d'un système de communication en mesurant la proportion de bits erronés par rapport au nombre total de bits transmis. Ce calcul est essentiel pour déterminer l'efficacité et la fiabilité d'un canal de communication. **[31].**
- **BER :** Affiche la valeur du taux d'erreur binaire calculé. **[29].**

### 3.3 Bloc de Zigbee transmitter :

Simulation d'un émetteur de signal ZigBee utilisant la modulation par décalage de phase en quadrature décalée (OQPSK), avec analyse détaillée des composants et du flux du signal comme illustré la figure suivante **:**

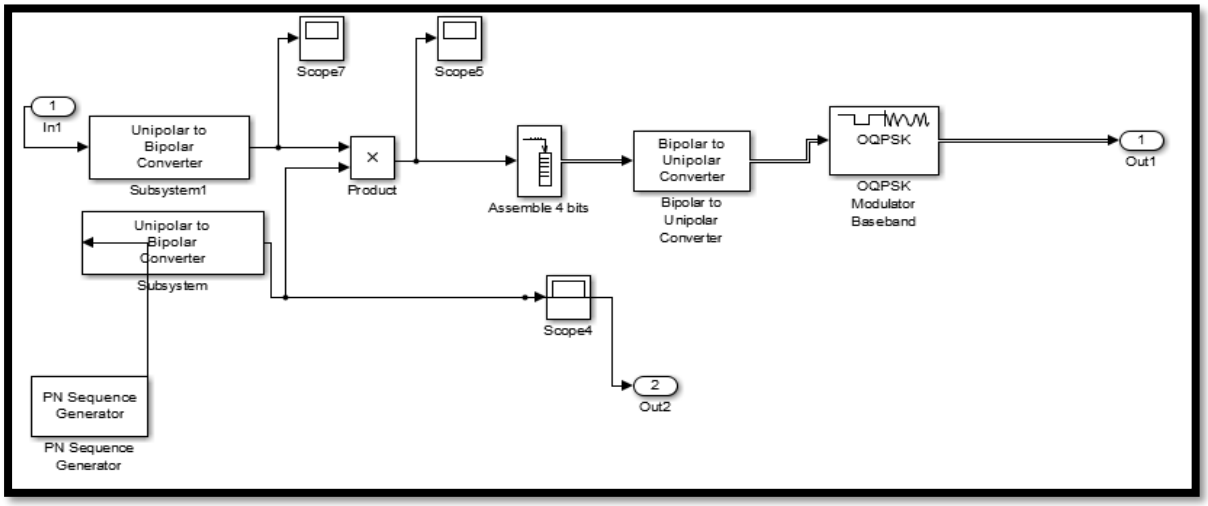



**Figure 3.2 :** Simulation pour un émetteur de signal Zigbee**.**

- **PN Sequence Generator :** Le générateur de séquence est un dispositif ou un algorithme utilisé pour produire une séquence de bits pseudo-aléatoires qui ressemble au bruit blanc mais qui est déterministe. Ces séquences sont utilisées dans divers systèmes de communication et de cryptographie pour des applications telles que l'étalement du spectre, le codage et le chiffrement**. [32].**

- **Subsystem1 et Subsystem (Unipolar to Bipolar Converter) :** Le convertisseur unipolaire à bipolaire est un dispositif ou une fonction utilisée pour transformer un signal unipolaire en un signal bipolaire. Un signal unipolaire est un signal où toutes les valeurs sont positives (ou nulles), tandis qu'un signal bipolaire alterne entre des valeurs positives et négatives. Cette conversion est couramment utilisée dans les systèmes de communication pour améliorer certaines caractéristiques du signal, comme la robustesse face au bruit et l'efficacité de la transmission**. [33].**
- **Product (Multiplier) :** Cet élément multiplie les données converties et la séquence PN pour préparer le signal à la modulation**. [34].**
- **Assemble 4 bits :** Cet élément regroupe les bits en blocs de 4 bits pour le traitement ultérieur. **[34]**
- **Bipolar to Unipolar Converter :** Cet élément reconvertit les données bipolaires en données unipolaires. **[34].**

La figure **3.3** comme illustré un motif mobile qui indique le numéro de signal ou la caractéristique du signal du capteur analogique **:**

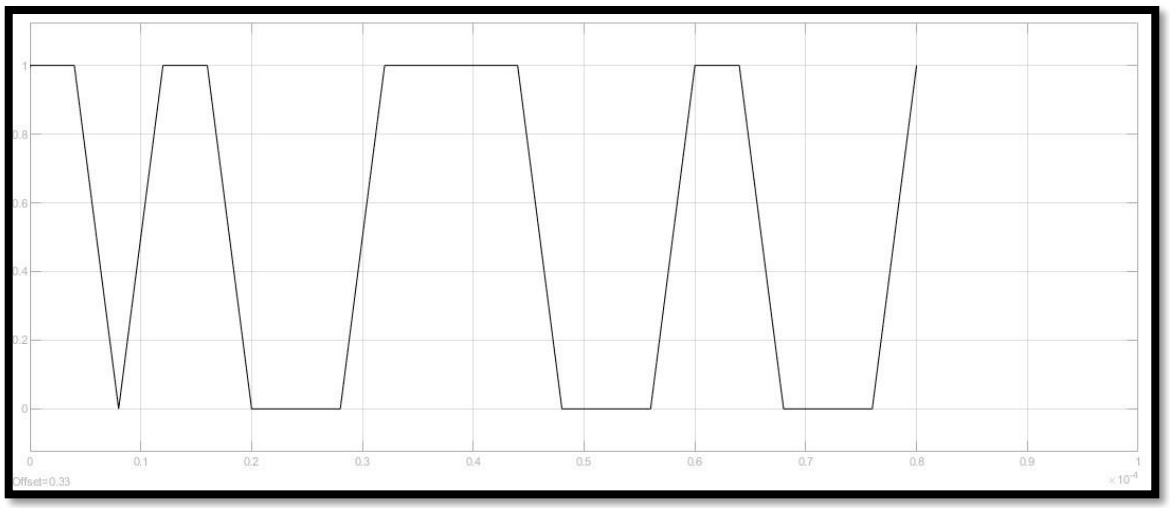



**Figure 3. 3 :** Les données du capteur en direct avant le traitement**.**

- **OQPSK Modulator Baseband :** Le modulateur OQPSK en bande de base est un composant utilisé dans les systèmes de communication pour moduler un signal en utilisant une forme spécifique de modulation de phase. L'OQPSK est une variante de la modulation QPSK (Quadrature Phase Shift Keying) où les transitions de phase sont étagées pour réduire les fluctuations de l'enveloppe du signal, améliorant ainsi la performance sur les canaux à faible bande passante et les environnements à bruit élevé**. [35].**
- **Scopes (Scope4, Scope5, Scope7) :** Les oscilloscopes (oscilloscopes) sont connectés à des seconds oscilloscopes avec l'heure à l'écran. Ils sont spécifiés pour déterminer le format, les

fréquences et l'amplitude des données, permettant ainsi aux ingénieurs de diagnostiquer et de déboguer les données électroniques. **[36].**

- **Out1 et Out2 :** sont deux types de sorties utilisées dans l'ingénierie des circuits électroniques. Elles font partie des conceptions de systèmes nécessitant la conversion de signaux électriques en d'autres types de signaux ou actions**. [37].**

Signal d'entrée de capteur 1 comme illustré dans la figure suivante **:**

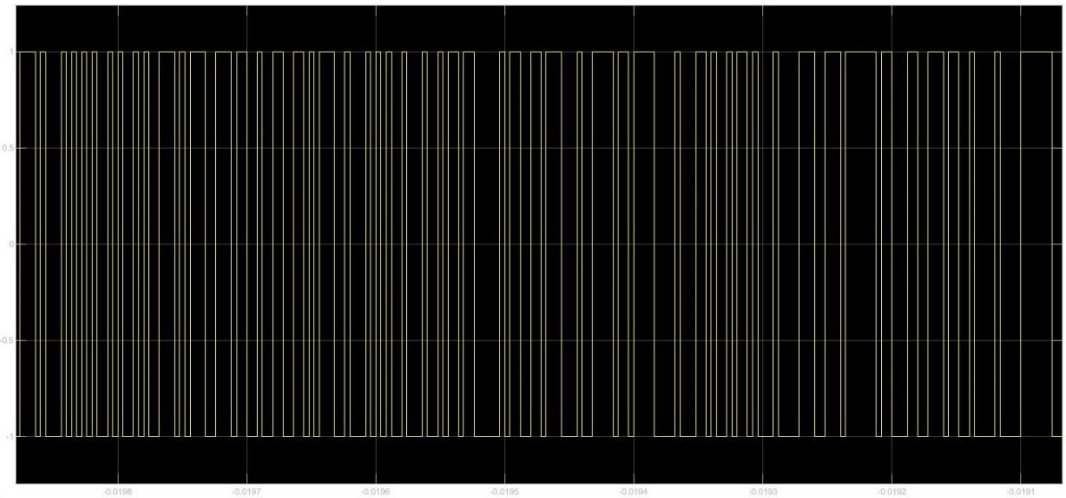


**Figure 3.4 :** Signal d'entrée de capteur 1 (amplitude, fréquence), les données globales dans 60s**.**

### 3.4 Bloc de Zigbee récepteur :

La figure comme illustré le déroulement typique d'un récepteur de communications numériques, commençant par la démodulation du signal OQPSK et se terminant par la conversion vers un format adapté aux systèmes numériques. Chaque bloc joue un rôle spécifique dans la récupération du signal original à partir du signal modifié transmis **:**

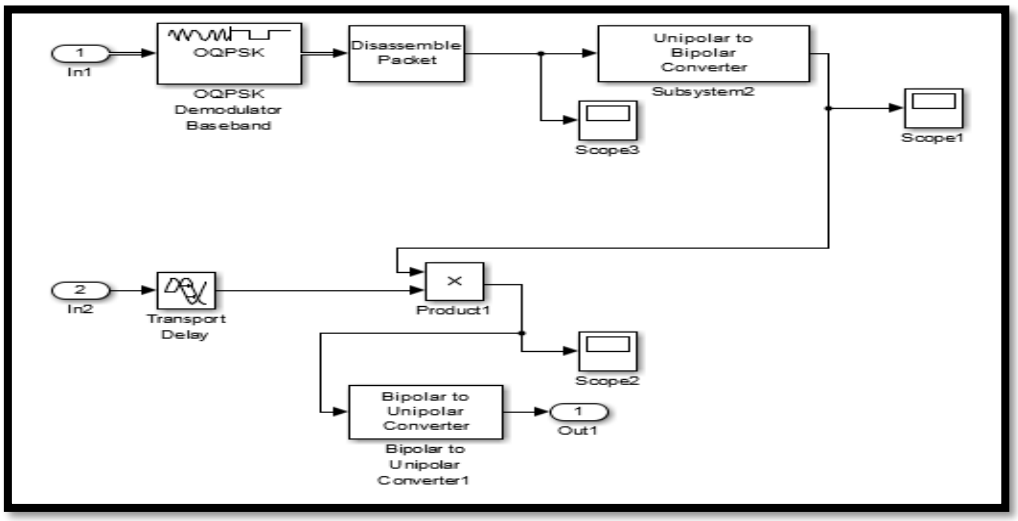



**Figure 3.5 :** Configurez la réception du signal ZigBee**.**

- **In1 et In2 (les entrées) :** Les entrées représentent les signaux traités par le système**.**

- **Bande de base du démodulateur OQPSK :** est la partie du système qui démodule le signal OQPSK pour récupérer les données originales du signal transmis. Dans un système de communication numérique, les signaux sont modifiés pour transmettre des données sur de longues distances. La réception de ces signaux nécessite une démodulation pour séparer les données du signal porteur **[38].**
- **Démonter le paquet :** C'est le processus d'analyse du paquet reçu en ses unités de base ou sous-composants. Dans les systèmes de communication, les données sont collectées sous forme de paquets à envoyer sur un réseau. A la réception, ces paquets doivent être désassemblés pour restaurer les données d'origine ou pour extraire les informations nécessaires des composants du paquet**.**
- **Convertisseur unipolaire vers bipolaire :** Il s'agit d'un dispositif ou d'un circuit utilisé pour convertir les signaux électriques de la forme unipolaire à la forme bipolaire. Dans les signaux unipolaires, le signal est confiné entre zéro et une certaine valeur positive, tandis que dans les signaux bipolaires, le signal se situe entre une valeur négative et une valeur positive, permettant une représentation plus large des signaux **[39].**
- **Sous-système 2 :** Il fait partie d'un système plus vaste défini comme une unité indépendante mais lié au maître. Cette partie profonde remplit certaines fonctions qui contribuent à la performance au travail. Le terme « sous-système » est utilisé dans de nombreux domaines tels que l'électrotechnique, les systèmes de communication et les systèmes de contrôle **[40].**
- **Délai de transport :** C'est le temps qu'il faut pour transmettre du point d'origine au point de destination via le système de transport. Ce terme est utilisé dans divers domaines tels que les réseaux de communication, la logistique et les chaînes d'approvisionnement, et fait référence au temps nécessaire pour transférer des données ou des marchandises d'un endroit à un autre **[41].**
- **Product1 (Multiplier) :** C'est un élément du système qui effectue une multiplication mathématique entre deux signaux. Ce processus est important dans de nombreuses applications de traitement du signal et systèmes électroniques, où le résultat de la multiplication peut être utilisé à diverses fins, telles que la modulation de signaux, le mélange de fréquences et la génération de nouveaux signaux **[42].**
- **Convertisseur bipolaire vers unipolaire :** Un appareil ou un circuit électronique qui convertit les signaux électriques de la forme bipolaire à la forme unipolaire. Dans les signaux bipolaires, le signal se situe entre une valeur négative et une valeur positive, tandis que dans les signaux unipolaires, le signal est confiné entre zéro et une certaine valeur positive **[43].**
- **Scopes (Scope1, Scope2, Scope3) :** Ce sont des instruments de mesure utilisés pour

surveiller et afficher des signaux électriques en fonction du temps. Les oscilloscopes affichent la forme d'onde d'un signal, permettant aux ingénieurs et techniciens d'analyser les caractéristiques du signal telles que la fréquence, l'amplitude et le temps de montée et de descente**. [44].**

- **Les sorties (Out1) :** Il fait référence à la sortie du système qui fournit le signal final après avoir traversé toutes les étapes de traitement au sein du système. Ce signal peut être le résultat d'un processus de traitement complexe comprenant le filtrage, l'amplification, la modulation du signal et d'autres processus**. [45].**

Un signal typique, régulier et récurrent indiquant un transfert de données numériques réussi, comme montré dans la figure suivante **:**

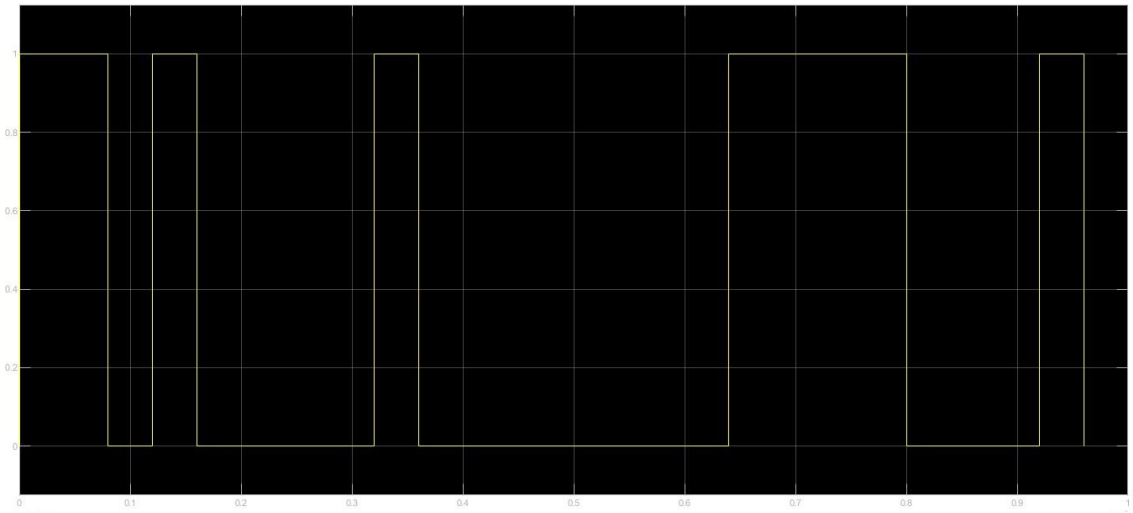


**Figure 3.6 :** Signal de sortie dans un système Zigbee (Récepteur) 5s**.**

### 3.5 Les caractéristiques distinctives de la technologie ZigBee :

ZigBee est un protocole open source, rendant son code librement accessible pour que quiconque puisse le personnaliser, l'améliorer et l'adapter selon ses propres exigences. Cette approche a été adoptée par de nombreux constructeurs de dispositifs connectés, tels que Signify (anciennement Philips Hue) et Legrand, pour intégrer ZigBee dans leurs produits. Cependant, cette ouverture peut conduire à des problèmes de compatibilité entre différents dispositifs utilisant ZigBee, d'où l'importance de vérifier la compatibilité des nouveaux appareils intelligents avant leur acquisition.

- **Bandes de fréquence :** ZigBee opère sur trois principales bandes de fréquence **:**
  - 868 MHz en Europe,
  - 915 MHz en Australie et aux États-Unis,
  - 2,4 GHz globalement (la même que celle utilisée par le WiFi et Bluetooth)

La bande 868 MHz offre une meilleure stabilité mais une vitesse inférieure comparée à la bande internationale de 2,4 GHz **[46].**

- **Réseau maillé :** Le protocole ZigBee est conçu pour supporter des réseaux maillés, formant une structure complexe où les dispositifs se connectent entre eux sans ordre hiérarchique fixe. Ceci permet au signal de se propager de manière itérative jusqu'à sa destination, étendant considérablement la portée effective de ZigBee au-delà de sa limite initiale. Cette fonction est particulièrement avantageuse pour les dispositifs connectés éloignés de la centrale. En cas de défaillance d'un dispositif sur le chemin du signal, le réseau trouve un autre itinéraire vers le destinataire. Les dispositifs servant de points de relais pour étendre la portée des données sont appelés routeurs. En revanche, les terminaux, tels que les commutateurs ou télécommandes, assurent que des fonctions de base et ne relaient pas le signal d'autres appareils, ne contribuent donc pas directement au maillage. Un coordinateur, souvent une centrale domotique, est nécessaire pour initialiser et maintenir le réseau ZigBee, ainsi que pour stocker des informations clés **[47].**

### 3. 6 Avantages principaux :

Outre l'extension de portée et la communication stabilisée via le réseau maillé, ZigBee offre d'autres avantages notables pour la domotique **:**

- **Économie d'energie :** Le protocole est conçu pour une faible consommation énergétique, surpassant le WiFi et Bluetooth en efficacité, grâce à sa capacité à transmettre de petits volumes de données rapidement, réduisant ainsi l'énergie requise pour la communication**.**
- **Retour d'etat :** ZigBee, étant bidirectionnel, permet de connaître l'état d'un appareil connecté en temps réel, facilitant la gestion à distance de la maison intelligente**.**
- **Sécurité améliorée :** La sécurité est une priorité absolue pour la Connectivite Standards Alliance, l'entité régissant ZigBee, qui s'engage à sauvegarder la confidentialité des données des utilisateurs, faisant de ZigBee l'une des technologies les plus sécurisées pour la domotique **[48].**

### 3.7 Interprétation :

#### 3.7.1 Description du projet et de son système :

Le projet consiste à relier un Raspberry Pi avec un ESP32 via une connexion ZigBee pour transférer des données. L'architecture du système comprend plusieurs étapes clés pour assurer un transfert de données efficace et fiable entre les dispositifs. Le Raspberry Pi agit comme le point de collecte des données en utilisant divers capteurs connectés à ses ports. Ces capteurs peuvent mesurer des paramètres environnementaux tels que la température et l'humidité. Les données recueillies par ces capteurs sont ensuite prétraitées par le Raspberry Pi. Le prétraitement peut

inclure des étapes telles que le filtrage des données pour éliminer les bruits ou les valeurs anormales, ainsi que l'agrégation des données pour réduire le volume de données à transmettre. Une fois le prétraitement des données terminé, le Raspberry Pi utilise un module ZigBee pour envoyer les données au module ZigBee connecté à l'ESP32. Le module ZigBee sur le Raspberry Pi convertit les données en un format adapté à la transmission sans fil. Ce processus de conversion est crucial pour garantir que les données peuvent être transmises efficacement et sans perte d'intégrité sur la liaison sans fil. Le module ZigBee sur le Raspberry Pi joue donc un rôle essentiel en tant qu'interface de communication entre le Raspberry Pi et l'ESP32. L'ESP32, de son côté, reçoit les données transmises via le module ZigBee. Une fois les données reçues, l'ESP32 procède à leur traitement. Ce traitement peut inclure la vérification de l'intégrité des données, leur décryptage si elles ont été cryptées, et leur stockage pour une utilisation ultérieure. L'ESP32 peut également inclure une interface utilisateur ou un autre système auquel il peut envoyer les données traitées pour un affichage en temps réel ou pour une analyse plus approfondie. Ce processus de réception et de traitement des données par l'ESP32 permet d'assurer que les données collectées par le Raspberry Pi sont non seulement transmises de manière fiable mais aussi traitées et présentées de manière utile**.**

En résumé, cette architecture permet de créer un système de collecte et de transfert de données efficace en utilisant un Raspberry Pi, un module ZigBee, et un ESP32. Le Raspberry Pi collecte et prétraite les données, le module ZigBee assure la transmission sans fil, et l'ESP32 reçoit et traite les données pour les rendre disponibles à des fins d'affichage ou d'analyse. Cette approche modulaire permet une flexibilité dans la configuration des capteurs et des traitements des données, tout en assurant une communication fiable entre les différents composants du système**.**

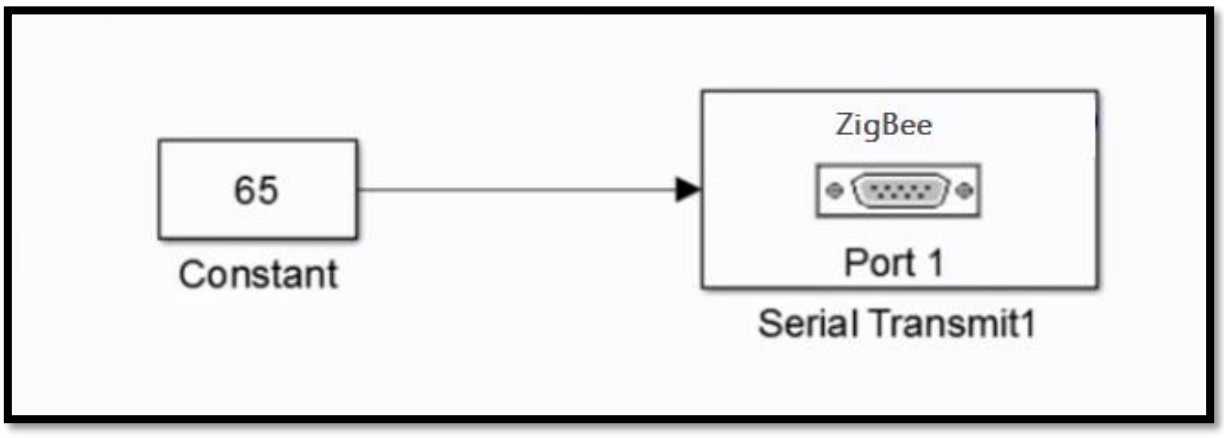



**Figure 3.7 :** Transfert de données du module fixe (65) vers le module ZigBee**.**

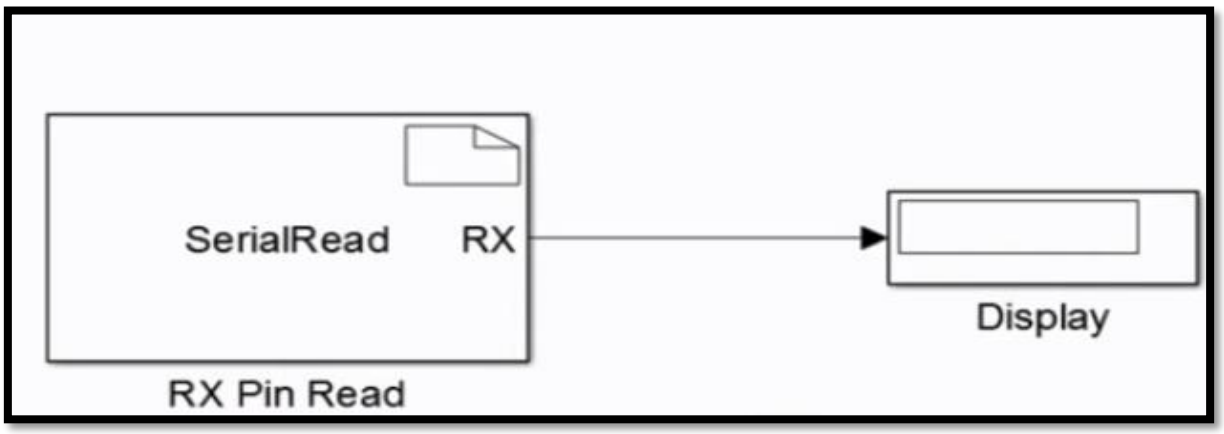



**Figure 3.8 :** Recevoir des données via une lecture série à l'aide du bloc "SerialRead"**.**

### 3.7.2 Processus de communication entre le module ZigBee et Raspberry Pi :

Le processus de communication entre un module ZigBee et un Raspberry Pi via l'émission et la réception de données peut être illustré à l'aide des diagrammes Simulink que vous avez fournis. La figure **3.8** représente la réception de données via une lecture série. Dans ce modèle, un bloc "SerialRead" est utilisé pour lire les données provenant d'un capteur ou d'un autre dispositif connecté au module ZigBee. Le bloc "SerialRead" est configuré pour lire les données reçues sur le port de réception série (RX). Ces données sont ensuite transmises à un bloc d'affichage qui permet de visualiser les informations reçues en temps réel. Cette étape est essentielle pour la surveillance continue des données et assure que les informations transmises par le ZigBee sont correctement reçues et interprétées par le Raspberry Pi. La figure **3.7** montre l'émission de données à partir d'une constante vers le module ZigBee. Ici, un bloc "Constant" est utilisé pour générer une valeur fixe (dans cet exemple, 65). Cette valeur est ensuite envoyée au bloc "Serial Transmit1", qui est configuré pour transmettre des données sur le port série (Port 1) associé au module ZigBee. Le module ZigBee prend cette valeur et la transmet sans fil à un autre dispositif compatible avec ZigBee, tel que le ESP32 ou un autre module ZigBee connecté à un capteur. Cette étape est cruciale pour envoyer des commandes ou des données spécifiques recueillies par le Raspberry Pi vers d'autres dispositifs au sein du réseau ZigBee. En intégrant ces deux processus – la réception et l'émission de données – on obtient une communication bidirectionnelle efficace entre le Raspberry Pi et les modules ZigBee. Le Raspberry Pi peut recevoir des données de différents capteurs via ZigBee, les traiter, et afficher les résultats en temps réel. Simultanément, il peut envoyer des commandes ou des données collectées à d'autres dispositifs, créant ainsi un réseau interconnecté capable de surveiller et de contrôler divers aspects d'un environnement. Cette communication bidirectionnelle est essentielle pour les applications où la surveillance et le contrôle à distance sont nécessaires, telles que les systèmes

de maison intelligente, les réseaux de capteurs environnementaux, ou les applications industrielles où les données en temps réel et le contrôle précis sont critiques**.**

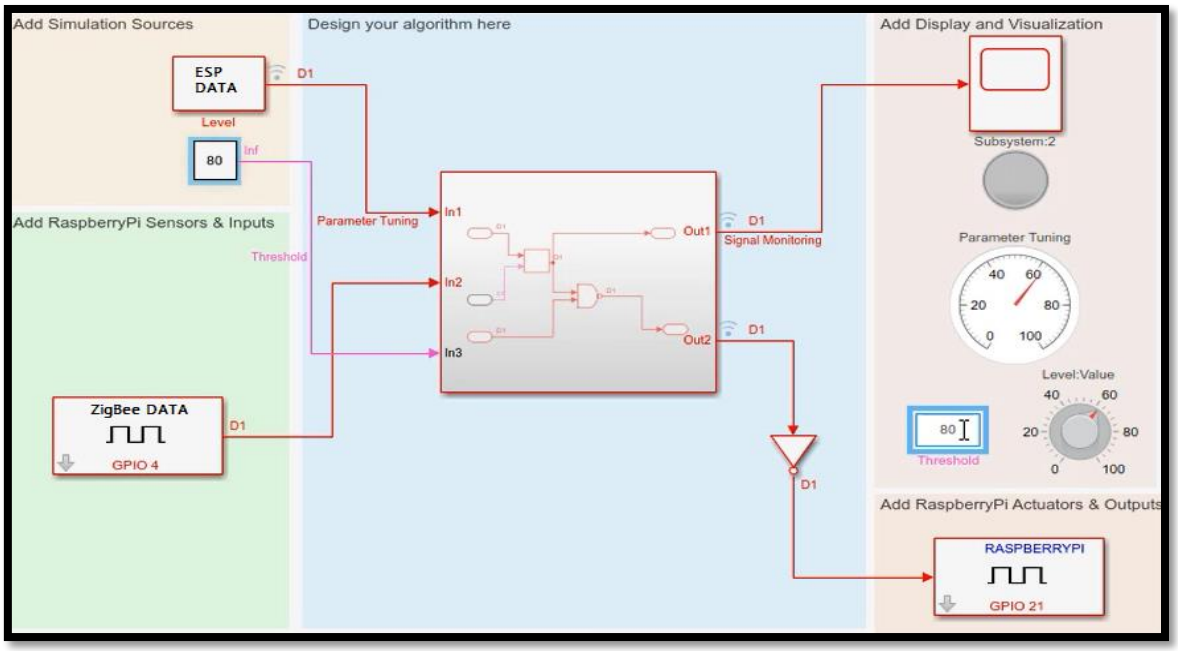



**Figure 3.9 :** Diagramme de flux de données entre Raspberry Pi et ESP32 via ZigBee**.**

### 3.7.3 Une solution de surveillance environnementale avancée :

Le projet représenté sur la figure **3.9** onsiste à intégrer des capteurs de température et d'oxygène avec un Raspberry Pi et un ESP32 en utilisant la technologie de transfert de données ZigBee. L'architecture du système commence par deux capteurs : un capteur d'oxygène et un capteur de température, chacun connecté à un module ZigBee pour la transmission des données. Ces capteurs collectent des données environnementales importantes, qui sont ensuite envoyées sans fil via ZigBee. Les données des deux capteurs sont reçues par un module ZigBee connecté à l'ESP32. L'ESP32 joue un rôle central dans la réception des données transmises, dans leur traitement pour vérifier leur intégrité et dans leur stockage pour une analyse ultérieure. Après le traitement initial par l'ESP32, les données sont envoyées au Raspberry Pi pour un traitement ultérieur. Le Raspberry Pi effectue des opérations de traitement de données plus complexes, telles que le filtrage et l'agrégation des données, pour fournir des informations précises et utilisables. Une fois les données traitées, elles peuvent être affichées sur l'interface utilisateur ou envoyées vers un autre système pour une utilisation plus avancée. Cette interface permet aux utilisateurs de visualiser les données en temps réel et de surveiller les conditions environnementales mesurées par des capteurs. L'intégration de ces composants dans une architecture cohérente garantit une communication de données transparente et fiable, depuis la collecte par les capteurs jusqu'à l'affichage et l'analyse par l'utilisateur final. Cette solution

modulaire offre flexibilité et extensibilité, permettant d'ajouter facilement des capteurs ou d'autres modules de traitement en fonction des besoins spécifiques de l'application.

Le diagramme de l'œil fournis montre le schéma de signaux en phase et en quadrature transmission par Zigbee, ce qui permet d'évaluer la qualité du signal et la performance du système de communication. Un diagramme de l'œil est un outil essentiel pour visualiser les distorsions temporelles et les interférences dans les systèmes de transmission numérique, comme illustré dans la figure suivante **:**

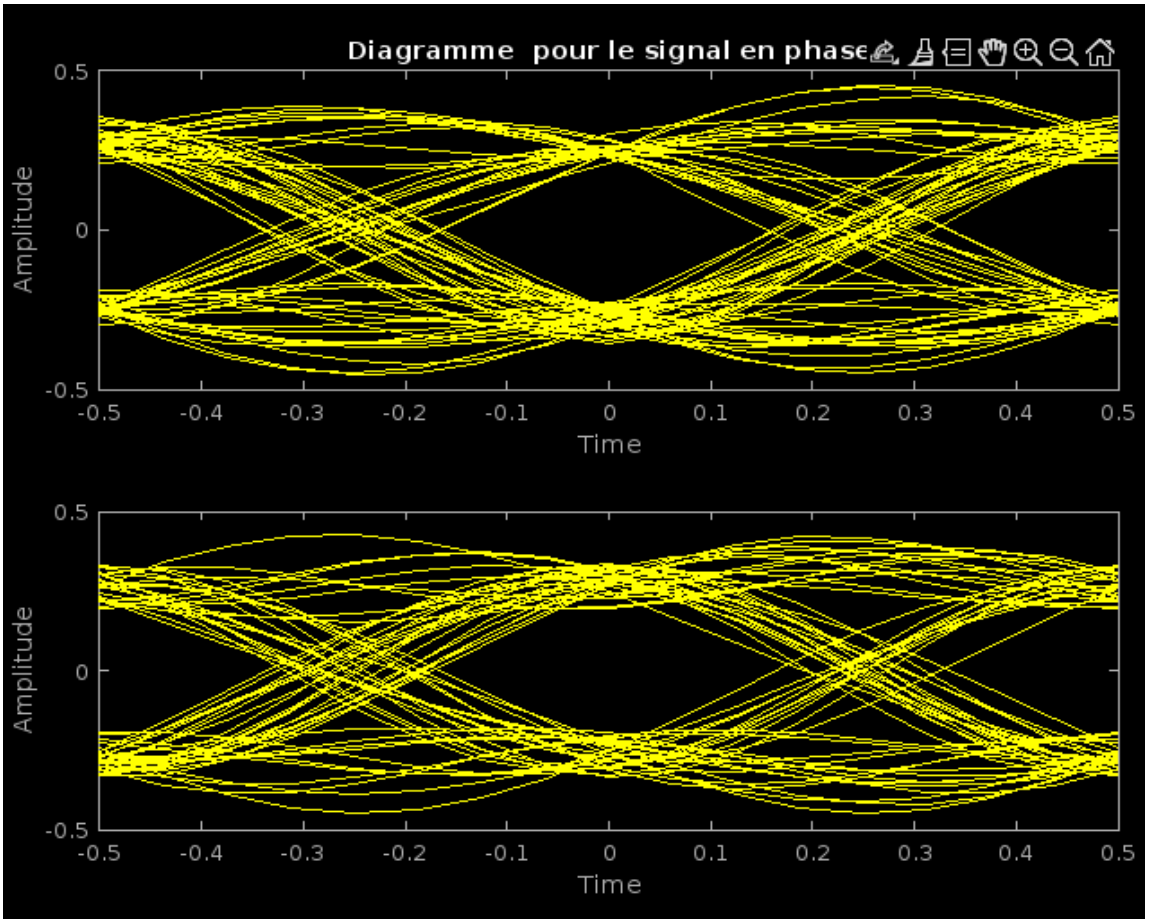



**Figure 3.10 :** Diagramme l 'oeil des signaux phasiques envoyés par ESP32**.**

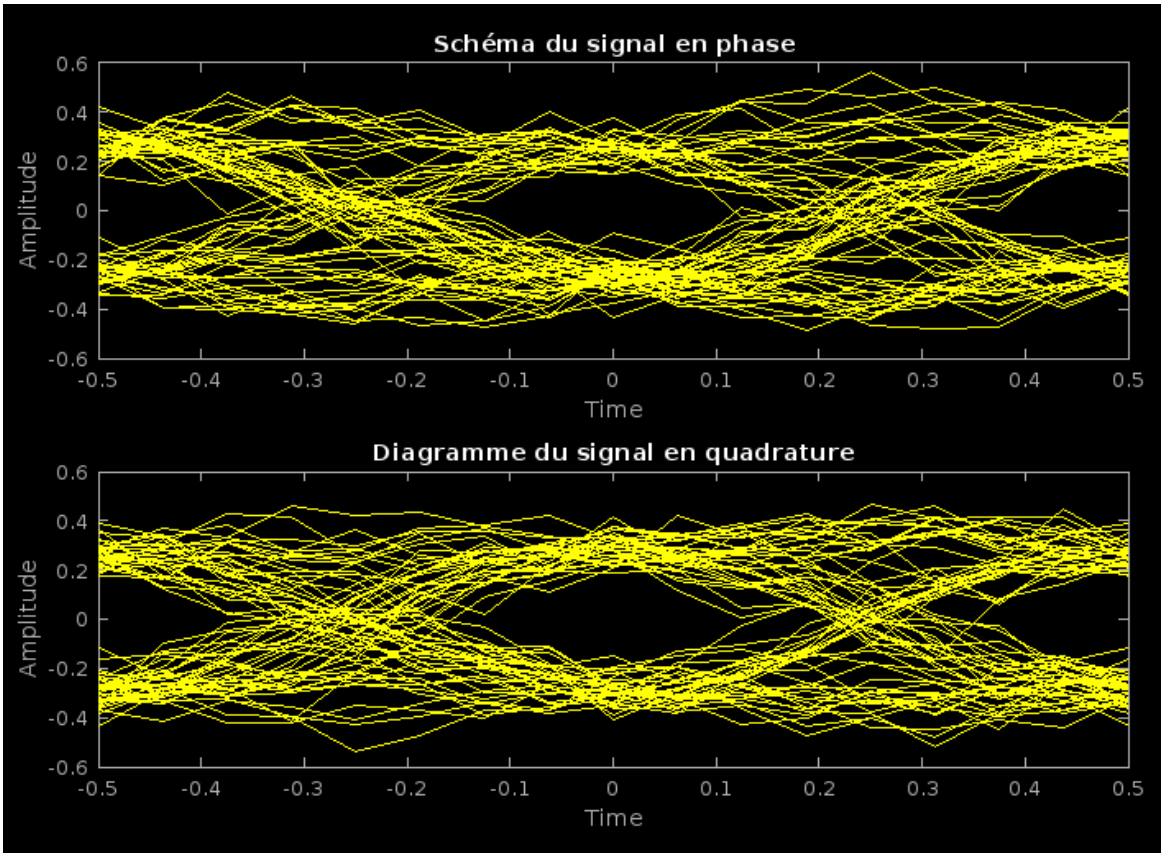


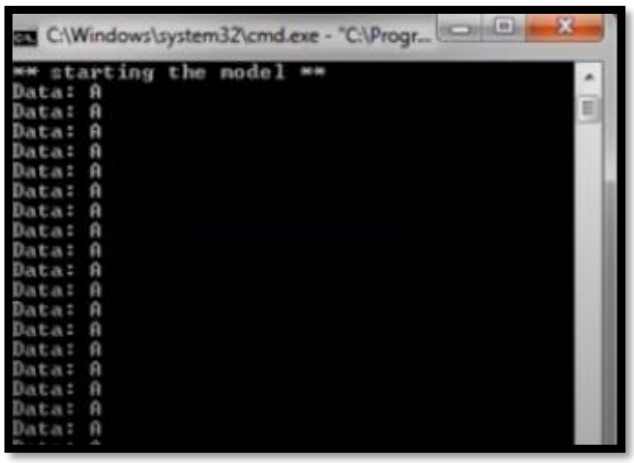

**Figure 3.11 :** Diagramme l'oeil schématique des signaux audio transmis par Zigbee**.**

Dans la partie de transmission des données par ESP32 figure **3.10** on remarque que les diagrammes présentent une structure claire et bien définie, ce qui est un indicateur positif. Les ouvertures des yeux sont bien visibles et ne montrent pas de signes significatifs de fermeture, ce qui suggère que les signaux reçus ont une bonne intégrité et que les niveaux de bruit et de distorsion sont faibles. La symétrie et la régularité des trajectoires des signaux dans les diagrammes en phase et en quadrature sont également des indicateurs que le système fonctionne de manière optimale et que la transmission est stable**.**

Ces diagrammes confirment que le système de communication ZigBee et Raspberry Pi, en termes de transmission et de réception des signaux, est performant et proche de l'idéal. Ils permettent de vérifier que les données transmises sont reçues avec une bonne fidélité, ce qui est crucial pour des applications nécessitant une transmission de données fiable et précise.

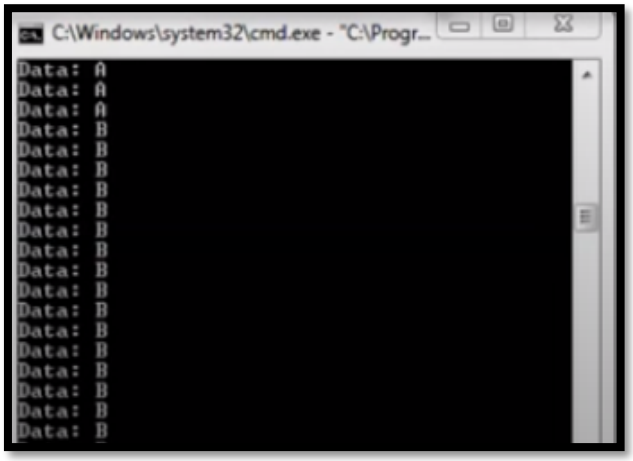
En résumé, les diagrammes de l'œil fournis sont acceptables et confirment que le système est capable de transmettre des signaux de haute qualité, proche de l'idéal théorique**.**

### 3.7.4 Confirmation de l'envoi et de la récupération des données des capteurs :

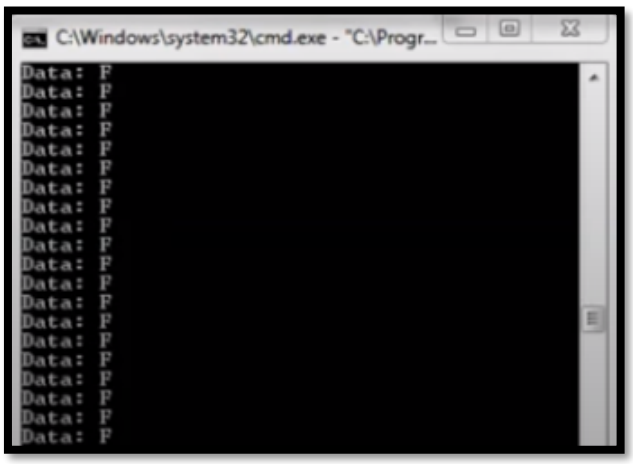



**(a)**

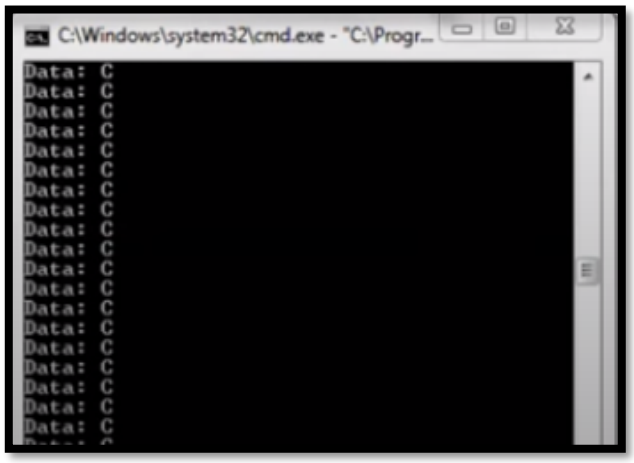

**(b)**




**(c)**




**(d)**




**(e)**

**Figure 3.12 (a), (b), (c), (d), (e) :** Les données reçues des 4 capteurs**.**

### 3.8 Explication et interprétation :

Les captures d'écran montrent les résultats de la transmission de données de capteurs via un système utilisant ESP32 et Raspberry Pi. Voici une explication détaillée des différents types de données affichées et de leur interprétation **:**

- **Figure 3.12 (a) :** Cette figure montre que les données envoyées sont principalement constituées de la lettre "**A**"**.** Le message "starting the model" au début indique que le modèle a été démarré, et la transmission des données a commencé. Les données "**A**" peuvent provenir du capteur d'oxygène**.**
- **Figure 3.12 (b) :** Semblable à la première, cette capture d'écran montre une série de données "A" envoyées et affichées. Le message "stopping the model" à la fin indique que le modèle a été arrêté après avoir envoyé plusieurs données "**A**"**.**
- **Figure 3.12 (c) :** Les données "**A**" et "**B**" alternent, ce qui suggère une communication entre deux états différents du capteur d'oxygène. Cette alternance pourrait indiquer des variations

dans les mesures ou les états du capteur**.**

- **Figure 3.12 (d) :** Les données envoyées sont "**F**", probablement provenant du capteur de température. La transmission répétée de "F" indique que ce capteur envoie des données de manière continue et stable**.**
- **Figure 3.12 (e) :** Ici, les données transmises sont "**C**". Cela pourrait également provenir du capteur de température, représentant peut-être une autre condition ou mesure**.**

### 3.9 Analyse des données de capteurs transmises par ZigBee :

Les données affichées montrent une transmission régulière et continue de différentes valeurs provenant de capteurs connectés à un ESP32 ou un Raspberry Pi. Les lettres "A" et "B" sont probablement liées aux données du capteur d'oxygène, tandis que les lettres "C" et "F" représentent les données du capteur de température. Les caractères « :" peuvent être utilisés comme délimiteurs ou pour représenter des états inactifs**.**

### 3.10 Points de coupure :

Les points de coupure dans la transmission de données peuvent être dus à plusieurs facteurs, tels que des interférences dans le signal, des interruptions dans la communication sans fil, ou des problèmes de traitement au niveau des microcontrôleurs. Il est essentiel de vérifier la stabilité de la connexion sans fil et de s'assurer que le traitement des données est optimisé pour éviter de telles coupures**.**

### 3.11 Interprétation générale :

Les captures d'écran fournies montrent un système de communication fonctionnant correctement avec des capteurs d'oxygène et de température, envoyant des données via ESP32 et Raspberry Pi. Les différents caractères affichés représentent les valeurs mesurées par les capteurs, et la stabilité de cette transmission est cruciale pour le bon fonctionnement du système global**.**

Le diagramme de dispersion que vous avez fourni illustré la constellation d'un signal modulé en quadrature. Ce type de diagramme est couramment utilisé pour évaluer la qualité de la modulation et la performance du système de communication, comme illustré dans la figure suivante **:**

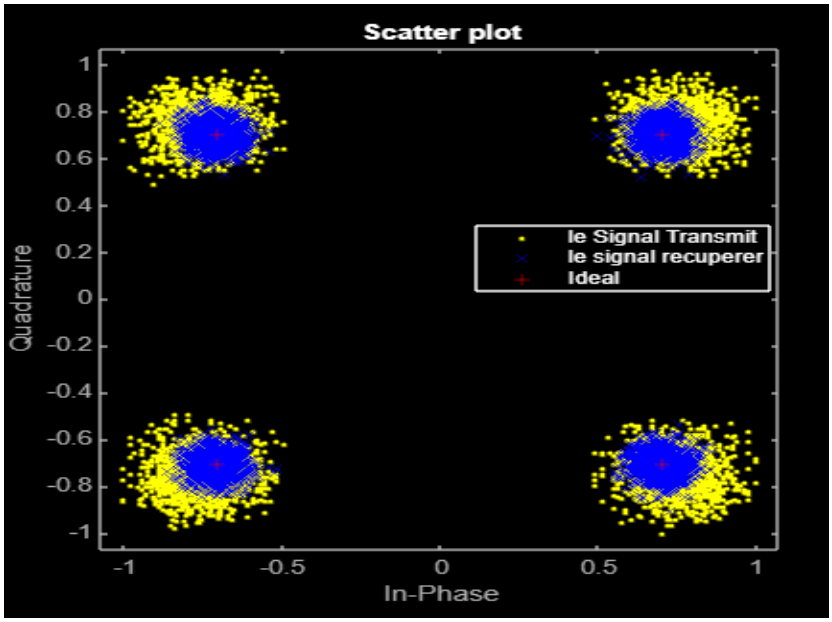



**Figure 3.13 :** Nuage de points de phase et signal quadratique**.**

- **1. Points jaunes (Signal Transmit) :** Les points jaunes représentent les symboles du signal transmis. Ils sont concentrés autour des quatre coins du diagramme (-1, -1), (-1, 1), (1, -1), et (1, 1). Cela indique une modulation en quadrature avec quatre états de phase distincts**.**
- **2. Points bleus (Signal Récupéré) :** Les points bleus représentent les codes de signal récupérés après la transmission. On voit que les points bleus sont également concentrés autour des quatre coins, mais ils sont moins dispersés que les points jaunes. Cette diffusion indique du bruit et une distorsion dans le canal de communication, mais la concentration autour des coins indique que le système de communication récupère les symboles avec précision.
- **3. Croix rouges (Ideal) :** Les croix rouges indiquent les positions idéales des symboles en l'absence de bruit ou de distorsion. Comparées aux points bleus et jaunes, on peut voir que les symboles récupérés (bleus) et transmis (jaunes) sont proches des positions idéales, ce qui indique que le système de communication fonctionne bien et que les erreurs de symboles sont minimales**.**

## 3.12 Évaluation de la performance du système de communication ZigBee avec Raspberry Pi et ESP32 :

### 3.12.1 Analyse du diagramme de dispersion :

Le diagramme montre que le signal transmis et le signal récupéré sont bien alignés avec les positions idéales, ce qui suggère que le système de communication est efficace. La dispersion légère autour des positions idéales est attendue en raison du bruit et des interférences inhérentes à tout système de communication sans fil. Toutefois, cette dispersion est relativement faible, ce

qui indique une bonne performance du système. Le diagramme de dispersion démontre que le système de communication est capable de transmettre et de récupérer les symboles avec une haute-fidélité. Les symboles récupérés sont proches des symboles transmis et des positions idéales, ce qui confirme que le système est robuste contre le bruit et les distorsions. Par conséquent, on peut conclure que le système de communication ZigBee utilisé avec le Raspberry Pi et l'ESP32 est performant et fiable pour les applications envisagées**.**

### 3.13 Conclusion :

En conclusion, nous voyons clairement les grands avantages de la technologie ZigBee dans de nombreux domaines, depuis l'amélioration des communications entre les appareils intelligents dans les maisons jusqu'aux applications industrielles qui nécessitent des réseaux de communication fiables et à grande échelle. La poursuite de la recherche et du développement dans ce domaine entraînera sans aucun doute des améliorations supplémentaires et une fiabilité accrue des systèmes sans fil, renforçant ainsi notre capacité à créer des environnements connectés et plus intelligents à l'avenir**.**

# Conclusion générale

**Conclusion générale :**

Les technologies ZigBee et ESP32 ont été choisies pour leurs caractéristiques distinctes et complémentaires. ZigBee a une faible consommation d'énergie, ce qui le rend idéal pour les appareils alimentés par batterie. Sa capacité à former des réseaux maillés robustes permet une large couverture et une flexibilité accrue, ce qui est essentiel pour les environnements IoT complexes. Les avantages supplémentaires incluent la sécurité intégrée utilisant des clés de cryptage AES-128 et la compatibilité entre différents fabricants. En revanche, l'ESP32 offre une connectivité Wi-Fi et Bluetooth intégrée, ce qui en fait une option polyvalente pour les applications IoT. Sa puissance de traitement et sa capacité à gérer simultanément plusieurs capteurs et appareils permettent une communication efficace et fiable**.**

Les travaux présentés dans ces mémoires contribuent de manière significative à la littérature existante sur les systèmes IoT sous plusieurs aspects. L'intégration des technologies ZigBee et ESP32 avec le Raspberry Pi en tant que gestionnaire central offre une nouvelle approche de la gestion des réseaux IoT. Cette configuration permet de centraliser la collecte, le traitement et le stockage des données, tout en assurant une transmission sécurisée et fiable des données. Les simulations et tests effectués ont montré que cette architecture est valable pour des applications réelles. Par exemple, la création d'un système de surveillance environnementale utilisant des capteurs ZigBee pour collecter des données sur la qualité de l'air et la température a démontré une gestion efficace des informations en temps réel**.**

Les résultats de la simulation ont confirmé plusieurs points clés : les appareils ZigBee ont démontré une faible consommation d'énergie, ce qui prolonge la durée de vie de la batterie et réduit les coûts de maintenance. Les tests ont prouvé la robustesse du réseau maillé ZigBee, permettant à la communication de continuer même en cas de défaillance de certains nœuds. De plus, la configuration peut facilement être étendue pour inclure davantage de dispositifs et de capteurs, rendant le système adaptable à divers besoins et contextes**.**

Les perspectives d’avenir de ce travail sont nombreuses et variées. Les recherches futures pourraient viser à améliorer la compatibilité entre les différents protocoles IoT afin de faciliter une intégration plus transparente de divers appareils. Les résultats obtenus ouvrent la porte à de nouvelles applications, notamment dans les domaines de la santé, où les dispositifs IoT peuvent surveiller les signes vitaux des patients en temps réel, et dans l'industrie pour améliorer les processus de production et la maintenance prédictive. Compte tenu de l’importance de la sécurité dans les systèmes IoT, les recherches futures pourraient se concentrer sur le développement de protocoles de sécurité plus robustes pour protéger les données sensibles**.**

# Bibliographique

**[1] : Hidjeb Ali** « implémentation d'un protocole d'élection d'un serveur d'authentification dans l'internet des objets » Mémoire de fin de Cycle Master 2 Université Abderrahmane Mira de Bejaïa **2017.**

**[2] :** https://bscw.5g-ppp.eu/pub/bscw.cgi/d208247/IoT %20Rapport%20Abstract.pdf accédé le **29/06/2019.**

**[3] : Yacine CHALLAL** « Sécurité de l'Internet des Objets : vers une approche cognitive et systémique » Au vu d'obtenir le diplôme d'Habilitation à Diriger des Recherches **2012.**

**[4] : Rahimi, H, Zibaeenejad, A, & Safavi, A. A.** (2018, November). A Novel IoT Architecture based on 5G-IoT and Next Generation Technologies. In 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 81-88) **2018.**

**[5] : TALEB Omar, MANKOURI Abdelkrim** « Programmation de la sécurité Internet des Objet,Etude de cas module WIFI Electric imp » l'université de tlemcen **Mai 2016.**

**[6] :** https://www.fun-mooc.fr/c4x/MinesTelecom/04013/asset/S4-5_-Objets communicants.pdf accédé le **25/06/2019.**

**[7] : Saad EL JAOUHARI, Ahmed BOUABDALLAH, Jean-Marie BONNIN** Institut Mines-Telecom/TELECOM Bretagne **«** La sécurité des objets connectés »**.**

**[8] : Melle KARA Nadjah** « Conception d'un réseau de communication pour une maison intelligente en utilisant la technique d'internet des objets ». Mémoire de fin de cycle – université de Bejaia**.**

**[9] : Nathalie Mitton** « INTERNET DES OBJETS, AUTO-ORGANISATION ET PASSAGE À L'ÉCHELLE » **8 Juin 2011.**

**[10] : TIZZAOUI YOUVA «** Internet des Objets (IoT) » Application : Industrie 4.0, Mémoire fin d'Études en vue de l'obtention du diplôme mastertélécommunication**.**

**[11] :** https://www.gsma.com/IoT /wp.../2014/08/cl**IoT** wp0714.pdf accédé le **29/06/2019.**

**[12] : Burhanuddin**, **M**. **A**., **Mohammed**, **A**. **A**. **J**., **Ismail**, **R**., & **Basiron**, **H.** «Internet of things architecture: Current challenges and future direction of research. International Journal of Applied Engineering Research, » 12(21), 11055-11061 **(2017).**

**[13] :** https://www.cigref.fr/wp/wp.../2016/12/CIGREF-Objets-Connectes-2016.pdf accédé le **29/06/2019.**

**[14] : Kathia Hart** « Taxonomie des consommateurs de bracelets intelligents capteurs d'activité physique basée sur l'adoption et l'utilisation des technologies » université de sherbrooke **Juin 2017.**

**[15] : ELISE MARGAIL** « innovation technologique, création esthétique et Discours d'accompagnement comme facteurs du Succès de l'appropriation des NTIC : Le cas des objets connectés » **Septembre 2014.**

**[16] : Imad Saleh** « Les enjeux et les défis de l'Internet des Objets (IoT ) » Laboratoire Paragraphe Université Paris **8. 2017.**

**[17] : Amri Toumia, Samuel Szoniecky** « Prétopologie et protection de la vie privée dans l'Internet des Objets » **2018.**

**[18] : Dechany, Maxime** « L'impact de l'internet des objets sur le futur de la logistique et du transport : cas du transport routier » HEC-Ecole de gestion de l'Université de Liège **: 2017-2018.**

**[19] :** https://www.cigref.fr/wp/wp.../2016/12/CIGREF-Objets-Connectes-2016.pdf accédé le **29/06/2019.**

**[20] : Internet of Things** « Privacy & Security in a Connected World » **JANUARY 2015.**

**[21] :** « Big data et objets connectés Faire de la France un champion de la révolution numérique » **2015.**

**[22] : Les Objets Connectés** « la nouvelle génération d'Internet Publié » **vendredi 13 septembre 2013.**

**[23] : Mohamed Tahar Hammi** « Sécurisation de l'Internet des objets » **28 January 2019.**

**[24] : Dorian Keuller** « Le secteur de la santé face à l'émergence de l'Internet des Objets **:** développement d'un outil d'aide à la décision » université catholique de louvain **2015.**

**[25] : Roman, Rodrigo, Pablo Najera, Javier Lopez** « Securing the internet of things » Computer 9 **(2011).**

**[26] : Panorama-internet**. **20/04/2019.**

**[27] : Achour Raouf, Makhloufi Naima** « Authentification dans L'IoT » mémoire de master recherche en informatique option réseaux et systèmes distribués, Université A.Mira, Bejaia juillet **2017.**

**[28] : MathWork,** shared document, definition of Zigbee and ESP Wifi.

**[29] : MathWorks :** Émetteur et Récepteur Zigbee, Canal AWGN**.**

**[30] : Horowitz, P, & Hill, W** « The Art of Electronics »**.** Cambridge University Press **(2015).**

**[31] : Proakis, J. G, & Salehi, M**. **McGraw-Hill** « Digital Communications » **(2007).**

**[32] : Sklar, B .Prentice Hall** « Digital Communications: Fundamentals and Applications » **(2001).**

**[33] : MathWorks** Documentation**.** « Unipolar to Bipolar Converter »

**[34] : Documentation MathWorks** « Modulateur et Démodulateur OQPSK, Générateur de Séquence PN, Convertisseurs de Signal »

**[35] : Proakis, J. G, & Salehi, M. McGraw-Hill** « Digital Communications » **(2007).**

**[36] : David A. Bell.** « Instrumentation et mesures électroniques » **2007.**

**[37] : Robert Boylestad** et **Louis Nashelsky** « Electronic Devices and Circuit Theory »**.**

**[38] : John G. Proakis. McGraw-Hill** « Digital Communications »5e édition,Education, page **371.**

**[39] : John G. Proakis** et **Dimitris G. Manolakis**,« Traitement numérique du signal : principes, algorithmes et applications » par 4e édition, Prentice Hall, page **200.**

**[40] : Benjamin S. Blanchard. Prentice Hall** « Systems Engineering and Analysis, 5e édition, page **135.**

**[41] : d'Andrew S. Tanenbaum, par Prentice Hall** « Computer Networks »**,** 5e édition, publiée, page **144.**

**[42] : David Harris. Sarah Harris** « Digital Design and Computer Architecture » 2e édition, page **346.**

**[43] : John G. Proakis** et **Dimitris G. Manolakis** « Traitement du signal numérique : principes, algorithmes et applications » 4e édition, page **201.**

**[44] : David Herres.** « Oscilloscopes : un manuel pour les étudiants, les ingénieurs et les scientifiques »

**[45] : Katsuhiko Ogata. Prentice Hall** « Modern Control Engineering », 5e édition,page **56.**

**[46] : Theodore S. Rappaport**, « Communications sans fil : principes et pratiques » 2e édition, page **567.**

**[47] : Shailesh Patil**, **Elsevier** « ZigBee Wireless Networks and Transceivers » page **89.**

**[48] : Drew Gislason**, **Newnes** « ZigBee Wireless Networking » page **12.**