Esther FABRE - GI05
Aness KEBIR - GI04
Manon DUPRE - GI04
Soulaymane KEBLI - GI01

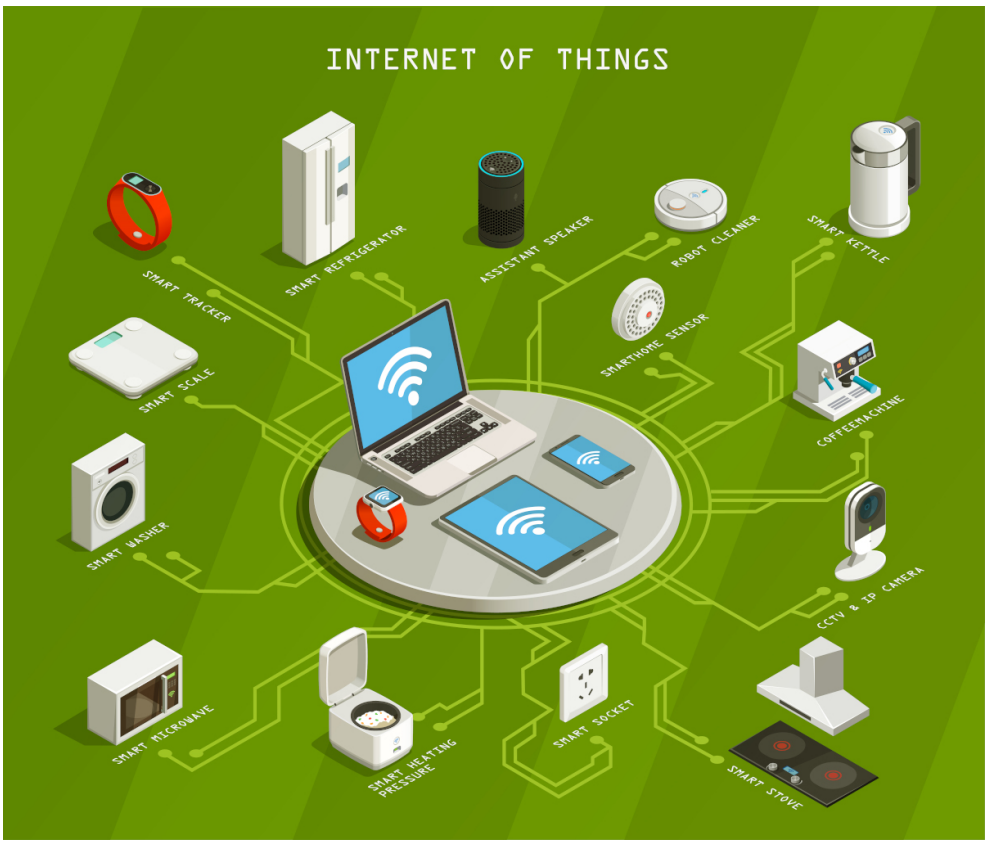
Université de Technologie de Compiègne

SR04 - Réseaux Informatique

Responsable

Mr. Abdelmadjid BOUABDALLAH

Objets connectés pour l'environnement



Remerciements

Nous tenons à exprimer notre profonde gratitude envers notre estimé professeur et encadrant Mr. Adelmadjid Bouabdallah pour sa guidance, son soutien inestimable et son engagement indéfectible tout au long de ce projet sur l'IoT et l'environnement.

Sa connaissance pour le sujet et son expertise ont été des piliers essentiels qui ont éclairé notre chemin tout au long de cette exploration complexe. Ses conseils éclairés, sa disponibilité constante pour discuter de nos idées et ses suggestions précieuses ont grandement enrichi notre compréhension du domaine de l'IoT et de ses implications environnementales.

Sa capacité à encourager la créativité, tout en apportant des orientations constructives, a été d'une valeur inestimable pour le développement de nos compétences et de notre compréhension approfondie de ce sujet vaste. Sa patience et sa volonté de nous guider à travers les défis techniques ont été des atouts majeurs qui ont contribué au succès de notre expérimentation.

De plus, nous sommes reconnaissants pour sa disponibilité et sa flexibilité, répondant à nos questions et préoccupations avec une attention et une expertise inégalées. Ses commentaires perspicaces sur nos travaux ont été essentiels pour améliorer la qualité de notre projet et pour nous encourager à viser l'excellence.

Nous tenons à lui exprimer notre profonde reconnaissance et nos remerciements les plus sincères pour avoir été un guide exceptionnel, et un professeur précieux tout au long de ce projet captivant sur l'IoT et l'environnement.

supervisé par
Mr. Adelmadjid BOUABDALLAH

Sommaire

Table des figures

Introduction

Dans un monde de plus en plus interconnecté, les objets connectés se sont imposés comme une révolution technologique majeure, transformant notre façon d'interagir avec notre environnement quotidien. Ces dispositifs sont des éléments physiques qui intègrent des composants électroniques, logiciels, capteurs et de connectivité réseau, leur permettant de collecter et d'échanger des données avec d'autres appareils via l'Internet des Objets (IoT). Ce document explore en profondeur le monde des objets connectés et de l'Internet des Objets, en se penchant tout d'abord sur leurs définitions et la structure de leur modèle en couches.

Nous nous intéresserons ensuite à leurs composants, plus particulièrement aux dispositifs finaux, protocoles de communication et au M2M. Dans un troisième temps, ce rapport aborde les applications variées de l'IoT, mettant en évidence les différences entre les applications web et mobiles, tout en explorant les fonctionnalités communes aux applications mobiles IoT pour les plateformes Android et iOS.

Au-delà de la théorie, ce document présente également une expérimentation concrète sous la forme d'un projet. Ce projet offre un aperçu pratique de la mise en œuvre des concepts abordés dans les sections précédentes. Nous examinerons en détail l'objectif de cette expérimentation, son protocole, son architecture ainsi que son analyse. Ce projet offre un aperçu concret des défis et des opportunités rencontrés lors de l'application des connaissances théoriques sur l'IoT dans un contexte réel.

En explorant les fondements théoriques et en les appliquant à travers une expérimentation pratique, ce document offre une certaine vision du monde complexe et aujourd'hui incontournable des objets connectés et de l'Internet des Objets. Comprendre les rouages nous permet non seulement d'appréhender le présent, mais aussi de façonner l'avenir, en exploitant intelligemment les technologies qui continueront à façonner notre monde connecté de demain.

1 Partie Étude

1.1 Définitions

1.1.1 Objets Connectés & IoT

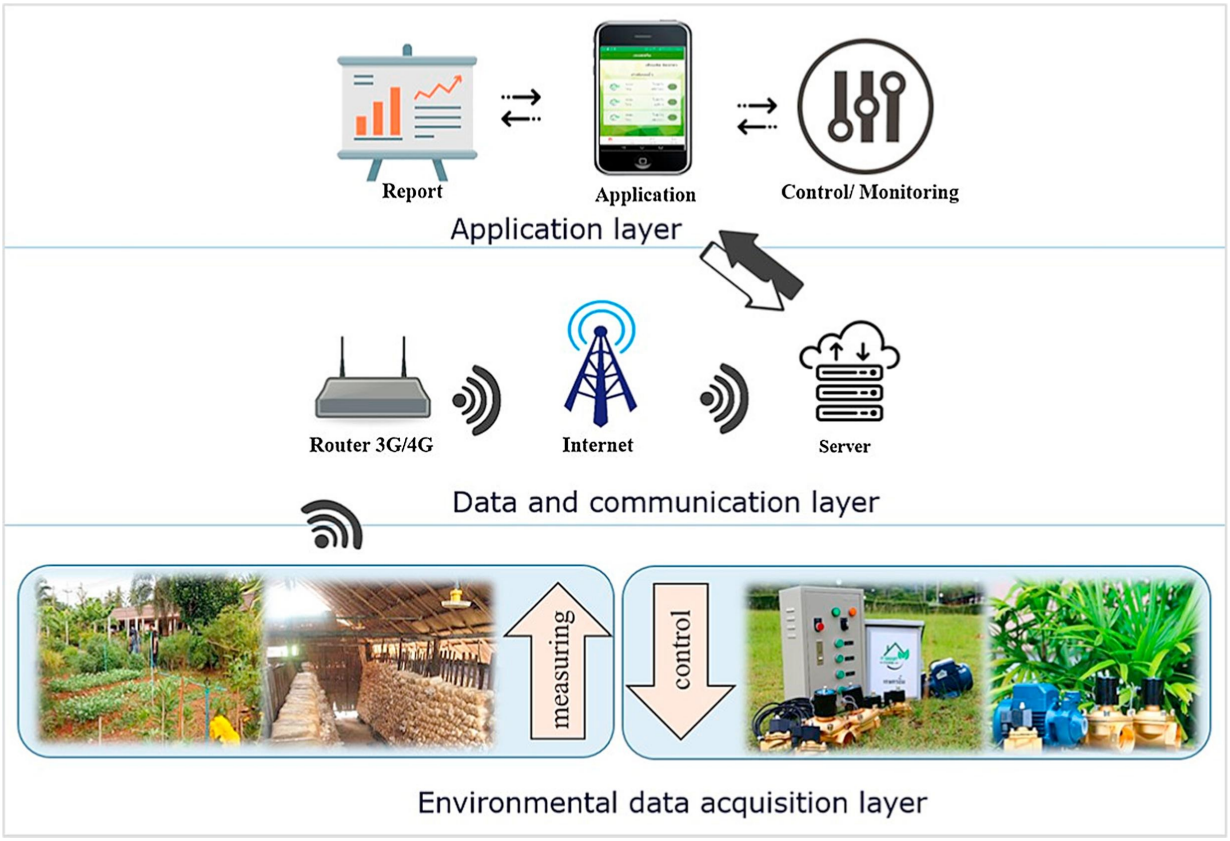
Un objet connecté est un dispositif physique capable de se connecter à d'autres dispositifs afin de collecter (à l'aide de capteurs), envoyer ou recevoir des données. Ensemble, ils constituent un réseau local ou dispersé qui agrège et traite les données obtenues afin de répondre à une variété de problématiques : création de villes intelligentes, transport, agriculture, santé, industrie, production/distribution d'énergie et gestion des ressources énergétiques. Le traitement de l'information capturé en temps réel dans les réseaux IoT confère une autonomie et une réactivité accrues à ces systèmes. Par conséquent, celles-ci peuvent optimiser leurs opérations, anticiper les besoins ou les problèmes ou prendre des décisions sans intervention humaine.

L'IoT, Internet of Things, désigne un réseau d'objets connectés dont la communication s'effectue à travers Internet. Il s'agit du type d'objets connectés privilégiés en raison de l'interconnectivité permise par l'intégration dans un écosystème mondialisé. En effet, l'utilisation d'Internet permet une collecte, une analyse et une utilisation à une échelle transcendant les limites des réseaux locaux tout en profitant de la robustesse d'Internet. L'écosystème complexe qu'est l'IoT est devenu incontournable ces dernières années. Les informations sont ainsi partagées et utilisées de manière intelligente pour améliorer notre qualité de vie, notamment pour simplifier nos tâches quotidiennes et optimiser les processus industriels.
En 2020, le nombre d'appareils connectés à l'intérieur du réseau IoT était estimé à 25 milliards. Il s'agit d'une tendance croissante, non seulement en ce qui concerne l'amélioration des performances industrielles, mais également à travers la véritable révolution dans la façon dont les appareils se fondent dans la vie quotidienne des individus, changeant la manière dont une personne interagit et perçoit le monde.

1.1.2 M2M & IoT

Le terme M2M, abréviation de "Machine-to-Machine" (en français, "Machine à Machine"), fait référence à la communication directe entre des machines, dispositifs, ou objets, sans intervention humaine. Son objectif est d'automatiser les processus de décision et de communication. Nous pouvons prendre l'exemple d'un réseau OT où deux objets communiques via le protocole Modbus : un capteur de mouvement à l'entrée d'un périmètre et un bras motorisé. Si le capteur détecte le moindre mouvement (c'est-à-dire une personne qui rentre dans le périmètre), il indique automatiquement au bras motorisé de s'arrêter sur le champs, afin d'éviter tout accident. Il s'agit d'une communication point par point, qui n'utilise pas internet.

L'architecture fermée du M2M et l'architecture ouverte de l'IoT, bien que différentes, se complétent de manière intéressante. Le M2M offre un noyau d'appareils électroniques formant un réseau soudé et relativement autonome, ce qui est idéal pour des tâches spécifiques et localisées comme nous avons vu. En revanche, l'IoT sert de passerelle pour le partage de donnée et permet d'étendre la portée de ce noyau à l'extérieur. En fin de compte, cette combinaison permet d'obtenir des systèmes plus robustes et polyvalents pour des possibilités d'applications plus larges.



[1]

FIGURE 1 – Exemple de réseau IoT

1. Muangprathub, J., Boonnam, N., Kajornkasirat, S., Lekbangpong, N., Wanichsombat, A., & Nillaor, P. (2019). IoT and agriculture data analysis for smart farm. Computers and Electronics in Agriculture, 156, 467 474. https ://doi.org/10.1016/j.compag.2018.12.011

1.2 L'IoT dans la vie quotidienne

L'Internet des Objets (IoT) s'affirme comme une force transformative influente, apportant des avantages concrets à divers secteurs grâce à une connectivité intelligente et à la collecte de données. Cette révolution numérique redéfinit nos approches dans de nombreux domaines tels que l'industrie, la grande distribution, la sécurité, la santé, les villes intelligentes, la domotique, l'énergie ou encore l'agriculture. En explorant les ramifications de l'IoT, il devient évident que cette convergence technologique offre des gains d'efficacité opérationnelle et des solutions innovantes aux défis contemporains, marquant ainsi le début d'une ère numérique transformée.

1.2.1 Industrie manufacturière (IoT industriel)

Dans le domaine de l'industrie manufacturière, l'Internet des Objets (IoT) a révolutionné les opérations en permettant une surveillance en temps réel des équipements. Cette approche représente la quatrième révolution industrielle, succédant aux révolutions liées à la machine à vapeur, à l'électricité, au pétrole, à la mécanique, à la chimie et aux technologies de l'information. On parle alors d'industrie 4.0. Cette connectivité intelligente facilite l'optimisation des processus de production, la mise en œuvre de la maintenance prédictive et la gestion intelligente de la chaîne d'approvisionnement. En conséquence, l'efficacité opérationnelle s'améliore considérablement, réduisant les temps d'arrêt non planifiés et augmentant la productivité globale.

1.2.2 Santé connectée

L'IoT a également apporté des changements significatifs dans le secteur de la santé en permettant le suivi en temps réel des données de santé des patients. Cela se traduit par des avancées majeures telles que la télémédecine, l'utilisation de dispositifs portables pour surveiller l'activité physique et la gestion des maladies chroniques. Ces applications contribuent à la prévention des maladies, à la réduction des coûts de soins de santé et à une approche plus proactive de la gestion de la santé individuelle.

A titre d'exemple, des systèmes de surveillance du taux de glucose tels que le FreeStyle Libre de la société Abbott, permettent aux personnes atteintes de diabète de connaître leur glycémie sans avoir à effectuer de prélèvements sanguins aux bouts des doigts. En scannant le capteur qu'ils portent sur le bras avec un lecteur adapté, ils ont accès à un l'ensemble de leur profil glycémique (valeurs, tendances, variabilité glycémique, historique...)

1.2.3 Des domaines d'application en faveur de l'environnement

1.2.3.1 Ville intelligente

Les villes intelligentes tirent pleinement parti de l'IoT pour améliorer la qualité de vie des citoyens et limiter les dépenses énergétiques. Des systèmes de gestion du trafic optimisés à l'éclairage public intelligent, en passant par la collecte des déchets basée sur la demande, l'IoT favorise une gestion urbaine plus efficiente. En intégrant des technologies connectées, les villes peuvent surveiller l'environnement, gérer le trafic et les déchets de façon plus efficace, renforcer la sécurité publique et optimiser l'utilisation des ressources énergétiques, contribuant ainsi à créer des espaces urbains durables et résilients.

1.2.3.2 Domotique

La domotique représente une intégration intelligente de la technologie dans nos habitations. Cette convergence permet une connectivité fluide entre divers dispositifs, tels que les thermostats, les éclairages, les serrures, les caméras de sécurité et les appareils électroménagers, créant ainsi une maison connectée. Les utilisateurs peuvent aisément contrôler et automatiser ces éléments via des applications sur leurs smartphones, offrant un confort accru et une personnalisation de l'environnement domestique.

La sécurité est également renforcée grâce à des systèmes d'alarme connectés et à une surveillance vidéo accessible à distance. En parallèle, la domotique contribue à une gestion énergétique plus efficiente, permettant la programmation intelligente des appareils et favorisant des économies d'énergie significatives. En évoluant avec les avancées de l'IoT, la maison connectée promet un habitat toujours plus intelligent, adapté aux besoins individuels et résolument orienté vers le bien-être de ses occupants.

1.2.3.3 Énergie intelligente

Dans le secteur de l'énergie, l'IoT contribue à la création de réseaux électriques intelligents. Ces réseaux permettent une gestion plus efficace de la consommation d'énergie, l'intégration harmonieuse des énergies renouvelables et la surveillance en temps réel des équipements énergétiques. En favorisant une utilisation plus intelligente des ressources énergétiques, l'IoT contribue à réduire les coûts et à promouvoir une transition vers des sources d'énergie plus durables. Ces systèmes peuvent notamment avoir un impact très important sur la consommation efficace de ressources, afin de détecter et diminuer les impacts de pertes au cours de l'acheminement desdites ressources.

Système de détection de fuite dans les pompes à essence

Dans leur étude, Sandhra C et Roopa M ont conçu un système efficace pour la détection de fuite dans les pompes à essence avec pour objectif de le déployer dans une ville intelligente. En l'occurrence, il s'agit d'éviter les fuites de Benzène, un liquide sans couleur et hautement inflammable, dont les vapeurs toxiques peuvent se propager dans l'air.

Le système, composé d'une carte Arduino pour les calculs, d'un capteur de gaz, et d'un module GSM pour une communication avec les serveurs de traitement côté cloud, est capable de détecter une augmentation de la concentration de Benzène dans l'air, de déclencher un son d'alarme et de passer une LED de vert à rouge pour signaler un danger aux usagers. De plus, le module GSM envoie un SMS d'alerte aux autorités compétentes pour permettre un suivi en temps réel et entamer les procédures de vérification et réparation le plus tôt possible. Ce type de système est très intéressant à déployer dans des contextes industriels, mais également dans des environnements publics comme des stations essences.

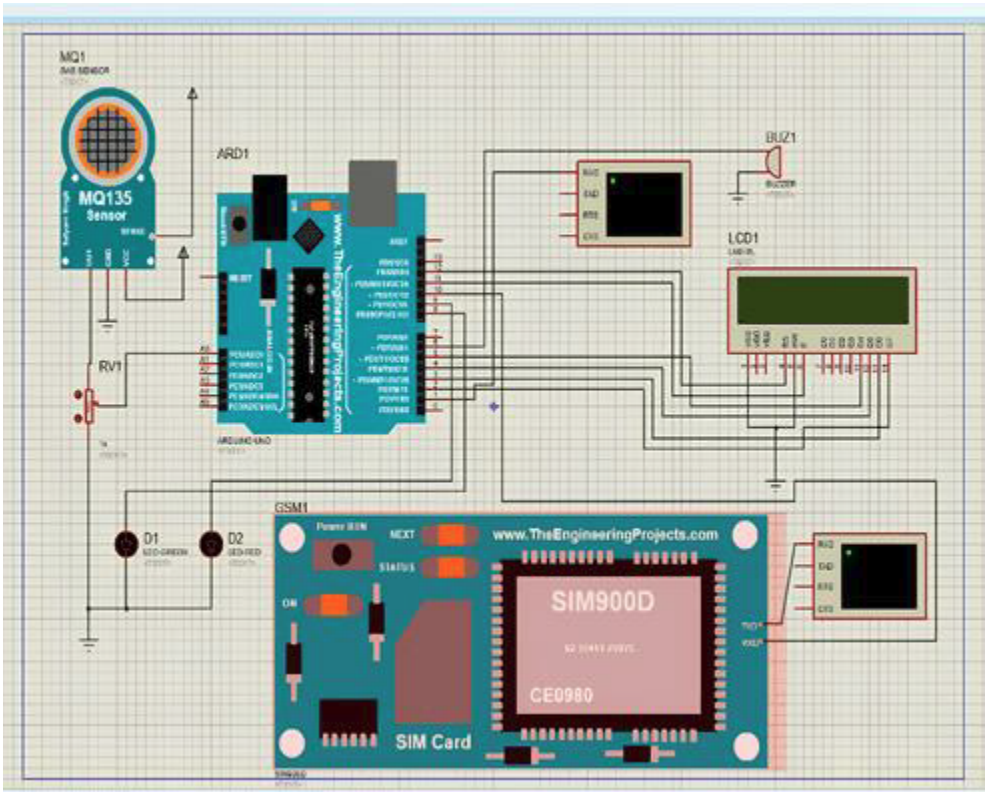


FIGURE 2 – Diagramme de circuit du système de détection des fuites de Benzène

1.2.3.4 Agriculture intelligente

L'IoT a transformé l'agriculture en permettant une gestion plus précise et efficiente des ressources agricoles. Grâce à des capteurs intelligents, les agriculteurs peuvent optimiser l'irrigation en fonction des besoins réels des cultures, surveiller les conditions du sol, surveiller les troupeaux et automatiser diverses tâches agricoles. Ces avancées favorisent une agriculture durable, améliorent les rendements et réduisent l'impact environnemental de l'activité agricole. Cette révolution technologique met alors en lumière de nouvelles manières de produire.

Les Fermes verticales

Dans leur étude, Monica D et Deepali G décrivent les caractéristiques d'une IoT verte, notamment dans un contexte de production en fermes verticales pour réduire la surface de production en raison de notre mode de vie toujours plus urbanisé.

Il existe trois types de fermes verticales, chacune ayant ses avantages et inconvénients. Les fermes aéroponiques diffusent leur solution d'eau et de nutriments dans l'air sous forme de brume, et les plantes placées au-dessus de la cuve récupèrent les particules via leurs racines qui descendent dans la cuve. Les fermes hydroponiques laissent la solution couler du haut vers le bas de la ferme, alimentant des racks de plantes au passage. Enfin, les fermes aquaponiques reprennent la structure des fermes hydroponiques, en ajoutant un écosystème aquatique, souvent des poissons, dans un réservoir au bas de la ferme. Ainsi, les plantes produisent des nitrates bénéfiques pour les poissons, et les poissons augmentent la quantité de nitrates et d'ammonium dans la solution, bénéficiant à leur tour les plantes.

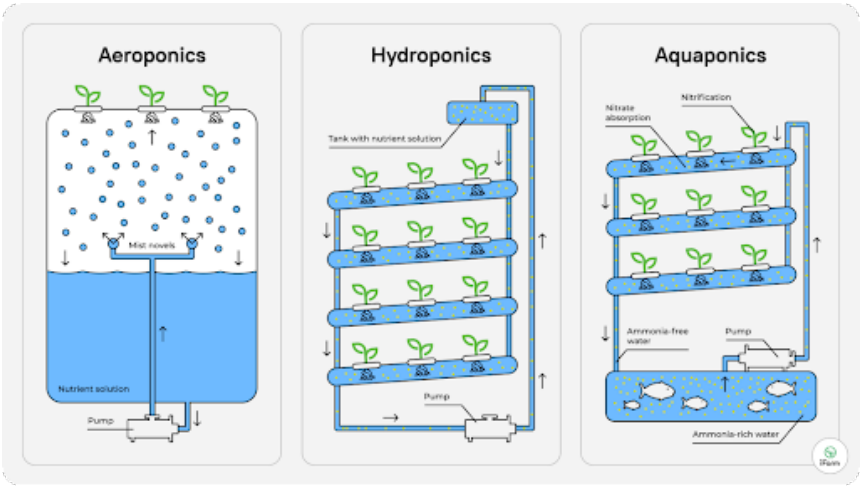


FIGURE 3 – Types de fermes verticales

Ce type de ferme combinée à de la détection et gestion automatique via un système IoT permet de contrôler automatiquement la distribution d'eau, la lumière via des LEDs, le tout actionné automatiquement en fonction de la quantité d'ions H2 ou de la conductivité électrique des plantes. Les agriculteurs peuvent donc se concentrer sur des productions plus manuelles pendant que ces fermes automatisées leur relaient les informations de croissance automatiquement, et les alertent en cas d'intervention nécessaire.

FIGURE 4 – Ferme urbaine verticale

En somme, l'Internet des Objets (IoT) émerge comme une force transformative, redéfinissant la manière dont nous interagissons avec le monde qui nous entoure. Des avantages significatifs se dessinent dans des secteurs clés tels que l'industrie, la santé, les villes intelligentes, la domotique, l'énergie et l'agriculture. Grâce à sa connectivité intelligente et à la collecte de données, l'IoT offre des solutions novatrices, améliorant l'efficacité opérationnelle, la qualité de vie et la durabilité environnementale. Cette révolution technologique témoigne du potentiel immense de l'IoT à façonner un avenir où la connectivité intelligente joue un rôle central dans notre quotidien, ouvrant la voie à des avancées continues et à des solutions adaptatives pour les défis contemporains dont notamment la préservation de l'environnement.

1.3 Topologie IoT

L'IoT repose sur une architecture en quatre couches servant de cadre conceptuel qui propose une manière de structurer les différents composants et le traitement d'un environnement IoT. Chacune des quatre couches est un environnement dans lequel il est possible de choisir entre plusieurs solutions et protocoles de communication, comportant leurs propres avantages et compromis, avec toutefois ce soucis omniprésente de compatibilité étendue et d'interopérabilité. Les quatre couches réunies garantissent une circulation fluide depuis la source des données jusqu'à le traitement final des données.
A noter que tout comme le modèle OSI, il ne s'agit que de directives générales, et non des règles incontestables. Par exemple, certains réseaux nommés "edge/fog computing" appliquent du traitement avant même le routage des données vers la couche de traitement.

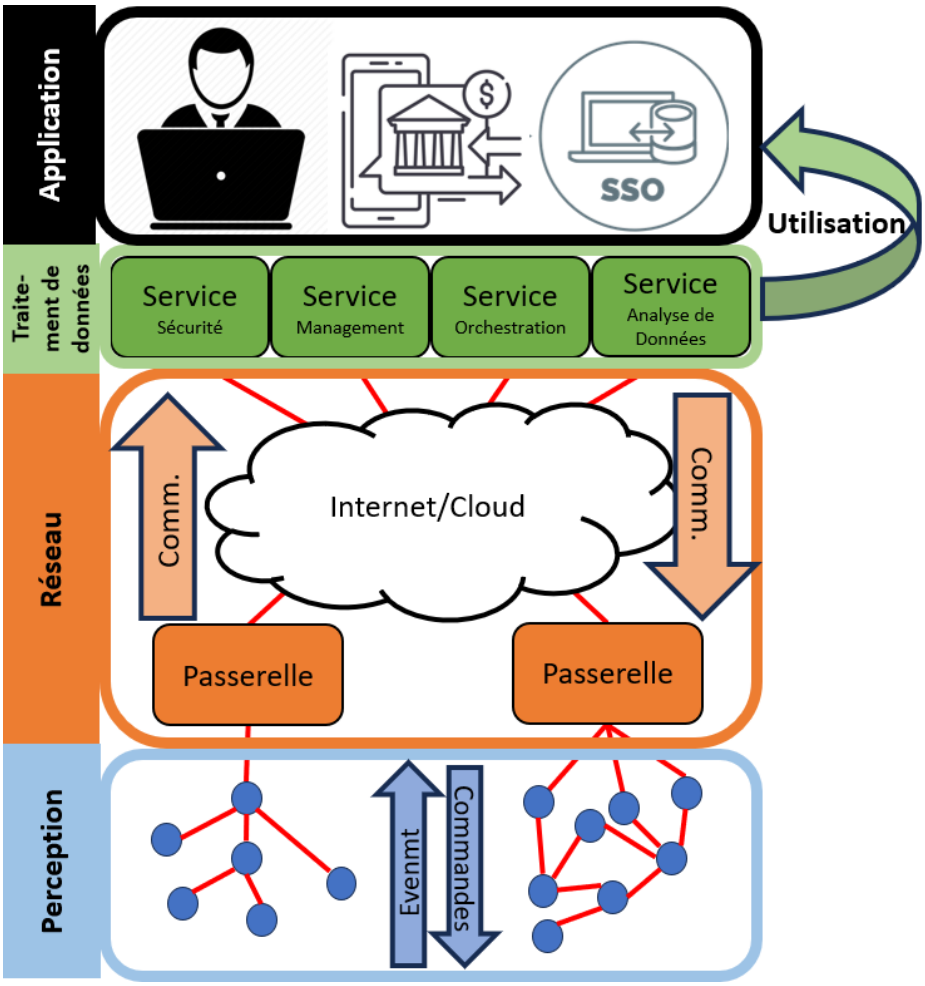


FIGURE 5 – Le modèle en 4 couches de l'IoT

Ce modèle s'articule en quatre couches :

- **La couche perception :** Première strate de l'architecture IoT, elle sert de point d'entrée dans la collecte de données, une sorte de mine où chaque dispositif, appelé nœud, collecte des données grâce à un capteur pour un usage ultérieur qui ne les intéresse relativement pas. Une fois les informations recueillies et éventuellement légèrement traitées, elles sont transmises à la couche réseau.

- **La couche réseau :** Les données collectées dans la couche de perception sont ensuite encapsulées puis routées de la passerelle jusqu'à un serveur de traitement (à l'autre bout de l'internet, voire dans le cloud). Réciproquement, des directives des couches supérieures parviennent à la couche perception à travers la couche réseau.
  En reprenant l'image de la mine, cette couche correspond à tout le réseau de convoyeurs au sein des mines permettant d'acheminer les richesses vers l'entrée de la mine (la passerelle), puis l'acheminement des diamants vers Kinshasa et les émeraudes vers une autre ville pour un traitement ultérieur à plusieurs kilomètres des mines, avec en parallèle un réseau téléphonique permettant aux fonctionnaires dans les villes de diriger les mineurs.

- **La couche traitement de données :** Les données sont arrivées à destination, c'est-à-dire sur le serveur de traitement ou plus généralement dans le Cloud. Cette irruption d'information doit être stockée, traitée et analysée, ce qui s'effectue dans le cadre de la couche de Traitement., tâches remplient par cette 3ème couche à travers des modules et services réutilisables. Ses responsabilités ne s'arrêtent pas là, car cette couche est pourvue d'une forme d'autonomie qui lui permet de prendre des décisions en conséquence des résultats des analyses. Enfin, c'est ici que la gestion et l'organisation des clusters de nœuds s'opèrent.
  On peut la comparer au quartier général d'une industrie minière qui non seulement récupère les minéraux, les nettoie, vérifie leur authenticité et les enregistre, mais aussi produit un grand nombre de statistiques et prend des décisions en fonction des résultats.

- **La couche application :** La dernière couche est l'interface qui relie l'utilisateur (humain ou machine) à toute la machinerie IoT latentes des autres couches. Cela se fait à travers des interfaces permettant la visualisation des données, l'interaction avec les dispositifs IoT, des analyses plus poussées, une prise de décision et d'action sur des instances en dehors du réseau IoT, etc.
  Cette couche est assimilable à un magasin de bijoux, où tout le processus de collecte, de traitement des pierres précieuses et d'analyse aboutit à une valeur marchande constamment en évolution en fonction des caprices des clients et du marché.

1.4 La couche Perception

1.4.1 Enjeux

A première vue, l'enjeux de la couche perception semble évident : collecter des données avec des nœuds, et éventuellement appliquer les commandes des couches supérieures.

Mais les choses se gâtent rapidement : de part leur nombre exponentiellement croissant, les nœuds sont organisés en clusters, soit des groupes de nœuds voisins qui peuvent communiquer directement entre eux. On parle de "Mesh topology" (réseau émaillé) ou de "Ad Hoc mode". Chaque cluster peut lui-même communiquer avec d'autres clusters, dans une sorte de Mesh de cluster. Ou le cluster peut directement et exclusivement se connecter à la passerelle (et donc le cloud) dans une topologie en étoile aussi appelée "Infrastructure mode". Cette double échelle nœud/cluster remplit plusieurs objectifs d'un point de vue logistique : configurations et maintenance simplifiées, efficacité énergétique (éteindre tout un cluster au lieu d'éteindre chaque nœud un à un) et amélioration de la fiabilité du réseau (redondance, load balancing, etc.). De plus, une communication directe entre les nœuds d'un même cluster permet une coordination et une collaboration fluides entre les clusters (par exemple, la synchronisation de la couleur de la lumière dans un système d'éclairage) ou une prise de décision immédiate (par exemple, une communication entre un capteur de température et un capteur d'humidité pour déterminer si l'irrigation est nécessaire). Ce sont des possibilités indispensables pour répondre aux exigences de "scalabilité" (capacité à faire grandir et évoluer un réseau sans perturber son fonctionnement ni sa gestion) et de la résistance à la panne par la même occasion, sans quoi un chaotique torrent impétueux de données se déferlerait sur les couches supérieures.

Le soucis du nombre de plus en plus astronomique des capteurs pèsent aussi sur des questions d'ordre énergétique et logistique : comment minimiser la consommation énergétique de chaque capteur ? Et plus généralement, comment accompagner le capteur tout au long de son cycle de vie sans nuire à l'activité réseau ?

Des considérations en terme de sécurité nous préoccupe également, nous ne souhaitions pas que les données récoltaient soient modifiée en cours d'acheminement, ce qui potentiellement pourrait entraîner des dégâts ; nous pouvons prendre l'exemple d'un réseau de capteurs malicieusement manipulés de sorte qu'ils signalent un incendie imaginaire. Un problème sous-jacent figure dans l'ajout frauduleux de capteurs dans un réseau, problème traité en grande partie dans les couches supérieures, mais exige une identité propre pour chaque capteur.

De retour à l'échelle du simple nœud, il est essentiel de considération sa puissance de calcul. Est-il capable de déchiffrer et retourner des messages ? De quelle taille au maximum ? Peut-il éventuellement les déchiffrer, et lui même produire une clé pour chiffrer ses informations ? Nous verrons par la suite que le header de HTTP, trop lourd et complexe, peut poser un problème rédhibitoire aux capteurs de faible puissance, contrairement à d'autres protocoles plus légers. La question de la distance influence aussi grandement sur le choix du matériel et des protocoles. Un réseau de nœud qui couvre de vastes étendues de terrain n'opterait pas pour un protocole Bluetooth.

Enfin, un défi majeur de cette couche reste dans l'interopérabilité : comment concilier des technologies et du matériel hétérogènes provenant de fabriquant différents, quelques

fois même conçu pour un domaine et un usage ultérieur spécifique ? En effet, toutes les problématiques évoquées précédemment doivent être étudié sous le prisme du problème d'interopérabilité : que ce soit dans les réseaux de nœuds en étoile ou émaillés, quelque soit la distance les séparant et la puissance de calcul, comment faire en sorte que chaque nœud puisse être compris et puisse dialoguer avec le reste du réseau ? Cela passe par une uniformisation du format des données recueillis.

1.4.2 Équipement

Un "end device", ou dispositif final, dans l'Internet des objets (IoT) est un composant matériel électronique ou un objet physique qui est capable de collecter, de transmettre et/ou d'agir sur des données dans le cadre d'une application IoT spécifique. Ces dispositifs sont souvent équipés de capteurs pour recueillir des informations sur leur environnement, de capacités de communication pour transmettre ces données à d'autres composants du réseau IoT, et parfois d'actionneurs pour effectuer des actions en réponse aux données collectées. Les "end devices" sont les points d'extrémité du réseau IoT, où la collecte de données et les interactions avec le monde réel ont lieu, contribuant ainsi à la création de systèmes intelligents et connectés. Les dispositifs IoT peuvent aller des smartphones aux lecteurs RFID, en passant par les dispositifs portables, les tablettes, les gadgets, pour n'en citer que quelques-uns.

Les dispositifs IoT peuvent être classés en deux catégories :

- **Sensors :** nœuds qui traduisent une grandeur physique en un signal numérisé ou qui détectent un changement dans l'environnement. Par exemple, un capteur d'humidité du sol.
- **Actuators :** nœuds qui agissent sur le système afin de changer son état en exécutant une action. Par exemple, un système d'irrigation automatique d'un champ.

Une seconde distinction, plus matérielle, peut être opérée : les dispositifs IoT bas de gamme, les dispositifs IoT milieu de gamme, les dispositifs IoT haut de gamme.

- **Dispositifs IoT de Basse Gamme (Low-End IoT Devices) :**
  Ces dispositifs sont contraints en termes de ressources, tels que la RAM et le flash de stockage. Ils ne peuvent pas exécuter des systèmes d'exploitation traditionnels comme Linux ou Windows 10 IoT Core. Ils sont principalement conçus pour des applications de base de détection et d'actionnement. Ces dispositifs sont généralement programmés à l'aide de micrologiciels de bas niveau ou d'un système d'exploitation (OS) de réseau de capteurs sans fil (WSN).
  Exemple : OpenMote-B et Atmel SAMR21 Xplained-Pro.

- **Dispositifs IoT de Milieu de Gamme (Middle-End IoT Devices) :**
  Ces dispositifs ont des ressources moins contraintes par rapport aux dispositifs IoT haut de gamme. Ils offrent davantage de fonctionnalités avec des capacités de traitement supérieures par rapport aux dispositifs IoT de basse gamme. Ils peuvent prendre en charge des fonctionnalités telles que la reconnaissance d'image à l'aide

d'algorithmes de vision par ordinateur de bas niveau. Ces dispositifs peuvent avoir plusieurs technologies de communication.
Exemple : Arduino Yun, Netduino, etc.

- **Dispositifs IoT Haut de Gamme (High-End IoT Devices) :**
  Ce sont généralement des ordinateurs monocartes (SBC) avec des ressources suffisantes pour exécuter des systèmes d'exploitation traditionnels comme Linux ou Windows 10 IoT Core. Ils disposent de capacités de traitement puissantes, d'une grande RAM et d'une capacité de stockage élevée, ainsi que d'une unité de traitement graphique éventuelle. Ces dispositifs sont dotés de connectivité à bord, y compris des interfaces FastEthernet/GigaEthernet, des puces Wi-Fi/Bluetooth, des interfaces HDMI, et plusieurs ports USB 2.0. Ils sont souvent utilisés comme passerelles IoT en raison de leurs ressources élevées.
  Exemple : Raspberry Pi.

1.4.3 Protocoles

Un protocole de la couche perception remplit un but : une communication standardisée au sein d'un cluster et entre clusters, c'est-à-dire un langage commun permettant à chaque nœud de communiquer avec d'autres nœuds. Nous nous concentrons donc ici exclusivement sur des topologies en maille (ad hoc mode), et des échanges machine-2-machine (peer2peer). Les réseaux en étoile où un nœud émet et reçoit directement à la passerelle seront traités dans la couche supérieure puisque le protocole des noeuds vers la passerelle et de la passerelle vers internet sont généralement identiques (MQTT, HTTP, CoAP, etc.). Chaque protocole possède des caractéristiques différentes en thermes de débit, de puissance de calcul requis ou de portée.

Features/Technology	NFC	RFID	Bluetooth	ZigBee	6LoWPAN
Coverage Area	PAN	PAN	PAN	LAN	LAN
Topology	P2P	P2P	Star	Mesh/Star/Tree	Mesh/Star
Power consumption	Very Low	Very Low	Low	Very Low	Very Low
Speed	400 Kbps	400 Kbps	0,7 - 1 Mbps	250Kbps	250Kbps
Range	< 10 cm	< 3 m	5 - 30 m	10 - 300m	800 m

[2]

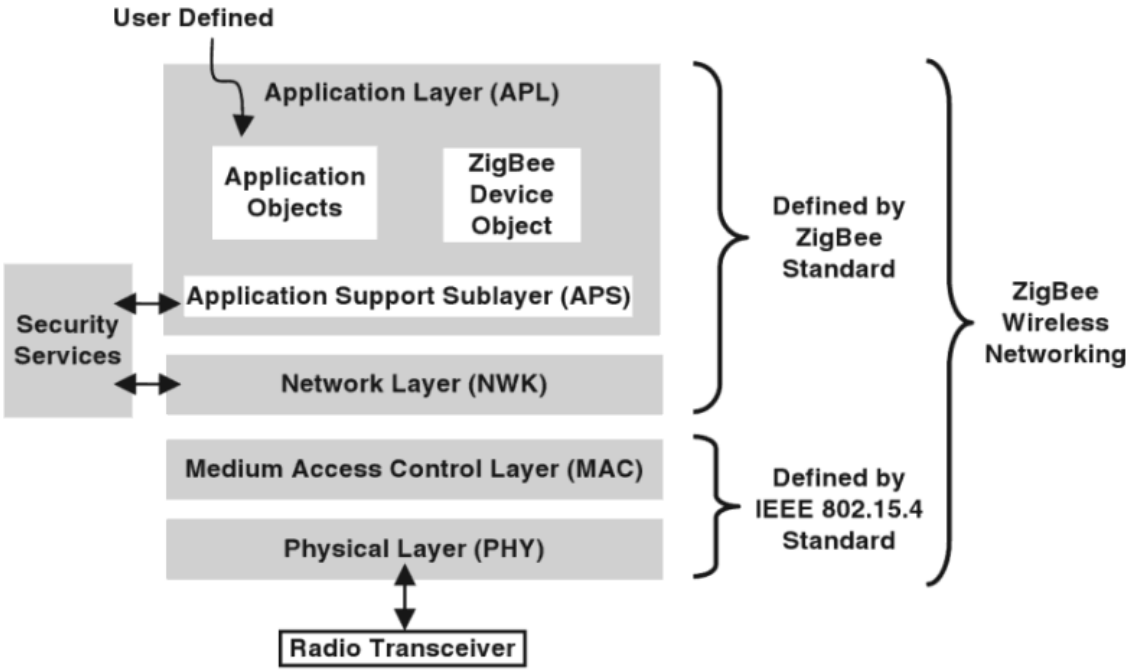
FIGURE 6 – Protocoles de communication ad hoc mode

On remarque que nul protocole n'excède les 1 km de portée, 6LoWPAN s'en reproche le plus mais utilise IPv6 pour toutes ses communications ce qui s'avérait difficile à implémenter dans un réseau hétérogène de petits capteurs de mesure éparpillées. La seule option viable dans le cas où nous voudrions étendre un maillage de capteurs couvrant une surface respectable tout en limitant la consommation d'énergie est le protocole ZigBee, que nous allons approfondir.

Les avantages de ZigBee en terme de coût énergétique, d'interopérabilité et de distance lui ont valu une adoption massive pour tout projet IoT exigeant un échange entre noeuds. Le protocole ne s'embarrasse pas des couches 1 et 2 du modèle OSI, il délègue en effet le

2. Cvitić, I., Vujić, M., & Husnjak, S. (2016). Classification of security risks in the IoT environment. Dans Annals of DAAAM for . . . & proceedings of the . . . International DAAAM Symposium .. (p. 0731 0740). https ://doi.org/10.2507/26th.daaam.proceedings.102

soucis des connexions physiques et au niveau MAC au standard IEEE 802.15.4, bien plus souple par rapport au WiFi IEEE 802.11, et donc plus facilement configurable quelque soit le matériel du nœud. C'est au détriment de la performance, n'excédant pas les 250 Kbps, mais amplement suffisant pour de simples transmissions de mesures de grandeur ou de partage de commandes. Tout équipement ZigBee opère sur la bande de fréquence 2.4GHz (ou très rarement 868 ou 915 MHz) conformément aux spécificités physique de IEEE 802.15.4. Le standard exige aussi un accès au support de communication de type CSMA/CA.



[3]

FIGURE 7 – Réseau ZigBee du point de vue du modèle OSI

IEEE 802.15.4 (couche PHY et MAC du modèle OSI) distingue 2 types de machines :

- **Full Function Device (FFD) :** nœuds plus performants capable d'endosser n'importe quel rôle décrit dans le standard IEEE 802.15.4 (dispose de fonctionnalités de stockage, de communication avec d'autres dispositifs FFD ou RFD et de routage).
- **Reduced Function Device (RFD) :** nœuds rudimentaires uniquement capable de communiquer avec un FFD.

ZigBee affine cette distinction au niveau des couches supérieures avec une séparation en trois groupes de dispositifs :

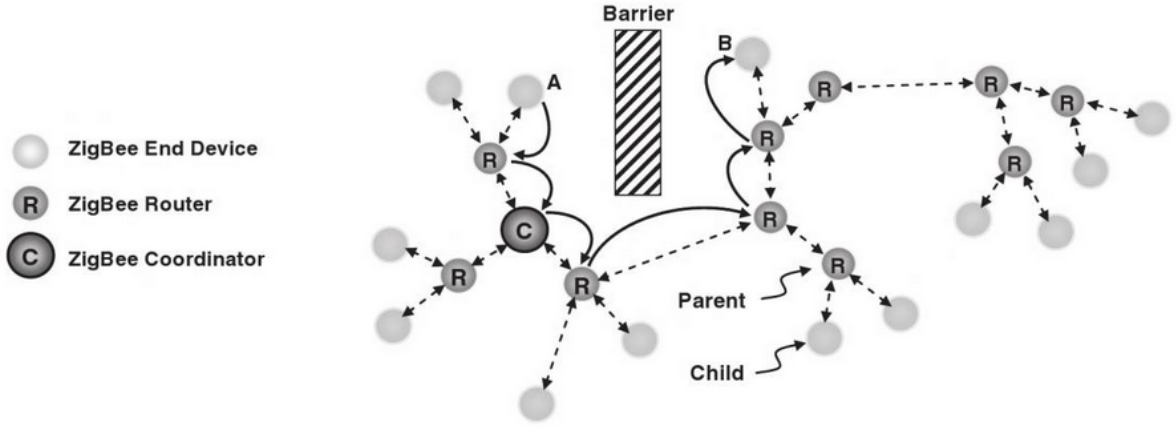
- **Le coordinateur :** unique dispositif FFD au sein du réseau qui gère l'accès au médium de communication, maintiens l'éventuel synchronisation des nœuds, initialise et sauvegarde les paramètres du réseau (fréquence, id du réseau, clés de sécurité, etc.). Il est constamment en écoute, en attente de requêtes. De plus, il assure le rôle de routage entre le réseau maillé et internet (fonction passerelle/gateway). Généralement dans un réseau maillé, tout FFD qui assume le rôle de coordinateur en premier devient automatique le coordinateur du réseau.
  C'est lui qui alloue une adresse différente à chaque nœud du réseau, parmi un pool

3. Farahani, S. (2011). ZigBee wireless networks and transceivers. newnes.

d'adresses IEEE de 64 bits. De plus, afin d'accélérer les communications, le coordinateur attribue également une adresse locale sur 16 bits pour chaque noeud du réseau également. Des réseaux qui peuvent contenir des milliers de end-devices, couvrant ainsi de très vastes surfaces tout en assurant la fiabilité.

- **Le router :** FFD agissant comme sorte de re-transmetteur intelligents qui relaye les données entre les dispositifs. Ils sont essentiels dans les topologies Mesh car ceux sont eux qui permettent le multi-hop et donc à deux end-devices éloignés de communiquer. Ce ne sont pas de simples switches ou hubs toutefois, car ils sont responsables de découvrir les routes et de les maintenir dans une table de routage.

- **Le end-device :** un nœud RFD, le type de dispositif le moins puissant en terme de calcul, avec le moins de mémoire et le moins coûteux en énergie.



4

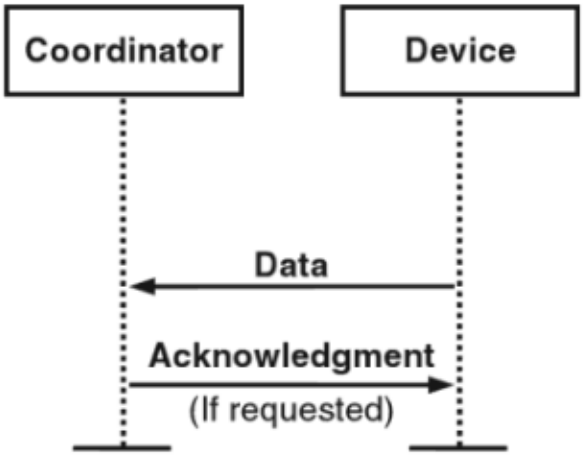
FIGURE 8 – Multi-hop dans un réseau ZigBee en ad hoc mode

La stratégie générale de ZigBee, à travers de cette organisation en 3 est d'étendre le réseau avec un maximum de end-devices, capteurs et actionneurs, trop faible ou éloigné pour traiter les données recueillis et avoir une conscience globale du réseau, en tirant parti de la capacité à relayer les données par l'intermédiaire de nœuds coopératifs proches. Contrairement aux end-devices, le coordinateur nécessite des aménagements énergétiques résilients (une alimentation électrique au lieu de simple batterie).
Lorsqu'un end-device ou un router souhaite intégrer le réseau, il doit le signaler au coordinateur, qui peut accepter ou rejeter la requête d'association.
Au contraire, lorsqu'un end-device tombe en panne, et que le chemin optimal jusqu'alors utilisé pour router les données n'existe plus, le réseau peut sélectionner une route alternative. Le réseau maillé chaotique retrouve alors une structure logique en arbre, pour assurer un routage fluide, comme dans la figure ci-dessus. On parle de "self-healing", ce qui offre au réseau Zigbee résilience et une forme d'autonomie.

Il y a trois types de transfert de données (rappelons qu'entre les deux interlocuteurs, il peut y avoir plusieurs routers qui relaient les différents messages dont on fait abstraction dans les shémas) :

4. Farahani, S. (2011). ZigBee wireless networks and transceivers. newnes.

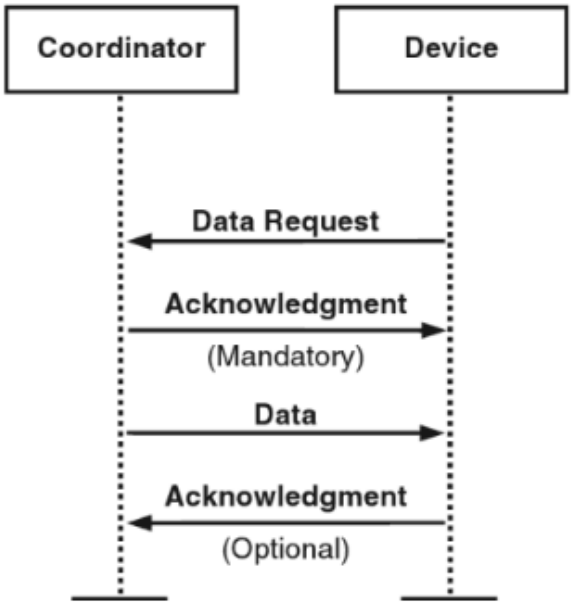
- **transfert de données entre end-devices par multi-hop**
- **transfert de données vers le coordinateur**



[5]

FIGURE 9 – Echange d'un end-device vers le coordinateur

- **transfert de données du coordinateur vers un end-device**



[6]

FIGURE 10 – Echange du coordinateur vers un end-device

5. Farahani, S. (2011). ZigBee wireless networks and transceivers. newnes.
6. Farahani, S. (2011). ZigBee wireless networks and transceivers. newnes.

1.5 La couche Réseau

1.5.1 Enjeux

La couche réseau réponds au besoin de routage des données du réseau de nœuds et de clusters vers le cloud et les servers webs (et vice versa). Cela suppose tout d'abord une forme d'adressage, presque exclusivement assurée par IPv4 et IPv6.
Les passerelles, ces dispositifs qui font le lien entre réseau de capteurs et internet, doivent être en mesure de dialoguer avec tous types de nœuds quelque soit le fabriquant, en particulier dans le cadre de réseaux en étoile. Un défi d'interopérabilité qui accompagne un autre défi spécifique à cette couche : la QoS. En effet, des priorités doivent être définies de sorte qu'une bande passante adéquate soient assurées aux applications nécessitant des réponses en temps réels (nous pouvons penser au système de surveillance).
Toujours dans ce soucis de performance, le load-balancing (équilibrage de la charge) est indispensable afin de gérer les grandes quantités de données et de pallier aux problèmes de panne. Il apporte également un réponse douce aux évolutions des besoins sporadiques et à l'adaptabilité à l'échelle.
La question de la fiabilité se pose également à l'échelle des paquets : comment détecter les erreurs tout d'abord mais surtout comment se prémunir des acteurs malveillants qui voudraient consulter, modifier ou juguler l'envoi paquet (exigences de confidentialité, d'intégrité et de disponibilité ?).

1.5.2 Équipement

La couche réseau assure la connectivité à internet du réseau de capteurs. L'intermédiaire permettant un tel processus s'appelle la passerelle. Il s'agit en somme d'un dispositif de traduction de protocole, un pont entre le protocole au sein du réseau de capteur (Zigbee, Bluetooth, etc) et le protocole utilisé dans le cloud (HTTP, MQTT, CoAP).
En plus de ces facultés de communication multiples, elles disposent de fonctions de calculs locales pour réduire la charge sur les servers de la couche supérieure ou pour pallier la faible puissance de calcul de la couche inférieure (notamment pour la sécurité).
Selon la spécificité du matériel et ses configurations, la passerelle peut faire parti intégrante du réseau de capteurs en étant soi-même capable de communiquer les autres passerelle du réseau avec le protocole du réseau maillé (dans le cas contraire, une communication entre les passerelles d'une même architecture devra s'effectuer à travers le cloud).

1.5.3 Protocoles

Les protocoles de communication jouent un rôle fondamental dans l'IoT en facilitant la connectivité et en garantissant que le réseau IoT de la couche de perception puisse échanger des données de manière fiable et sécurisée avec l'extérieur (internet ou le cloud). Le choix du protocole dépend des besoins spécifiques de l'application, de la portée de communication, de la consommation d'énergie et d'autres facteurs. Ils sont tous implémentés dans la couche Application du modèle OSI, c'est-à-dire qu'ils présupposent l'utilisation de protocoles de couches inférieures, généralement TCP/IP.

Voici quelques-uns des protocoles couramment utilisés dans l'IoT :

1. **MQTT (Message Queuing Telemetry Transport) :** Protocole de communication léger basé sur le modèle de publication/abonnement. Efficace pour les communications asynchrones entre dispositifs. Nous revenons plus en détail sur le protocole

dans la partie expérimentation.

2. **CoAP (Constrained Application Protocol) :** Protocole conçu pour les dispositifs avec des ressources limitées. Fonctionne sur le modèle de requête/réponse, adapté pour les environnements à bande passante et énergie limitées, couvrant de longues distantes. Cela est possible car le protocole repose sur UDP. La sécurité est assuré par une version de TLS adaptée au mode non connectée de UDP : DTLS (datagram TLS).
3. **HTTP (Hypertext Transfer Protocol) :** Largement utilisé sur le Web, également utilisé dans l'IoT pour des cas spécifiques. Souvent utilisé en combinaison avec des protocoles de passerelle plus légers.
4. **DDS (Data Distribution Service) :** Standard de l'OMG facilitant la communication en temps réel dans des systèmes distribués. Communément utilisé dans des applications industrielles et médicales.
5. **AMQP (Advanced Message Queuing Protocol) :** Protocole de messagerie pour la transmission de messages entre dispositifs. Assure une communication asynchrone et prend en charge la fiabilité.
6. **Thread :** Protocole de communication sans fil basé sur IPv6, conçu pour les réseaux d'objets connectés dans la maison intelligente. Optimisé pour une faible consommation d'énergie et une connectivité à faible coût.
7. **LoRaWAN (Long Range Wide Area Network) :** Protocole sans fil pour les réseaux longue portée et basse consommation d'énergie. Souvent utilisé dans le suivi d'actifs et les réseaux de capteurs.
8. **Sigfox :** Protocole bas débit, longue portée et faible consommation d'énergie. Adapté pour les dispositifs IoT qui transmettent de petites quantités de données de manière sporadique.

1.6 La couche traitement de données

La couche traitement de donnée est quelques fois appelée la "couche service", car cette couche peut être comprise comme un enchevêtrement de services réutilisables et flexibles répondant à des exigences variées, mais avec ce souci constant de faire le pond entre le monde physique et le monde digital. Certaines exigences sont spécifiques au problème ce pourquoi le réseau IoT a été conçu, mais nous retrouvons certains enjeux qui émergent quelque soit le projet.

En effet, en plus des services de collecte, d'agrégation, de normalisation, de corrélation et d'analyse (statistique) des données, certains modules "méta" offrent la possibilité de gérer et configurer les services classiques : la création de services, l'orchestration des services à travers du scheduling ou la gestion de l'exécution des services.

C'est dans cette strate que les contrôles de sécurité sont implémentées, avec des modules de gestion de l'identité et de AAA (authentication, authorization, accountability) que ce soit pour les utilisateurs configurant les différents services de la couche traitement de données que les passerelles, capteurs et flux des couches inférieures. De plus en plus, la sécurité des réseaux IoT se renforce d'un système analogue au PKI avec un système de clé agrémenté d'algorithmes de réputation (afin de détecter et rejeter les nœuds malicieux).

La couche traitement de donnée interface donc avec la réalité physique des capteurs, mais cela s'étends à plus que la sécurité. On retrouve également des services de mise à jour de firmware des équipements physiques et réseaux, la surveillance de leur état de santé ou le dépannage.

1.7 La couche application

La couche application interface non seulement avec les utilisateurs, mais aussi avec des systèmes d'entreprise existants en dehors du projet IoT ou à des services proposées par d'autres société (virements, le SSO, etc.). Ce souci de compatibilité nécessite un travaille d'harmonisation de plusieurs composants différents.
Notamment des composants spécifiquement conçus pour interagir au sein du projet IoT, du code fait maison qui doit répondre aux exigences habituelles de projets de programmation : maintenabilité, modularité, standardisation, etc... afin d'assurer le rajout de nouvelles fonctionnalités et des mises à jour régulières sans impact sur le code existant.
De plus, cette couche intègre également des éléments essentiels tels que la gestion des données, la sécurité, l'analyse et l'interopérabilité [7] pour garantir un fonctionnement fluide et sécurisé du système IoT.
Enfin, il faut accommoder l'utilisateur avec une interface ergonomique qui lui permet en plus d'une navigation intuitive une personnalisation en fonction de ses besoins et préférences.

Les enjeux associés à cette couche d'application sont multiples. La sécurité demeure l'un des défis majeurs, exigeant la mise en place de protocoles robustes pour protéger les données sensibles transitant entre les appareils connectés et les serveurs. Une évolutivité adéquate est également nécessaire pour que les applications IoT puissent s'adapter à de nouveaux appareils ou à une augmentation du nombre d'utilisateurs, sans compromettre leurs performances. L'interopérabilité entre les divers dispositifs de différents fabricants constitue un autre défi crucial pour assurer une communication transparente entre les appareils et les plateformes IoT.

7. Possibilité de communication entre deux ou plusieurs systèmes, appareils ou éléments informatiques

2 L'IoT, des bénéfices évidents accompagnés d'enjeux à surmonter

De par la multiplicité des technologies, protocoles et interconnexions de données qu'il favorise, l'IoT a révolutionné divers secteurs : la santé avec des dispositifs médicaux connectés pour le suivi à distance, l'industrie avec l'automatisation et la maintenance prédictive, les villes intelligentes grâce à la surveillance des infrastructures, et l'agriculture avec des systèmes de gestion précise des ressources. Ces avancées ne se limitent pas seulement à l'amélioration de l'efficacité et de la qualité de vie, mais contribuent également à des pratiques plus durables et respectueuses de l'environnement, telles que la réduction des émissions de carbone, la gestion efficace des ressources et le soutien à une agriculture durable. L'IoT joue ainsi un rôle central dans la création d'un avenir interconnecté, efficient et plus ou moins écologiquement responsable. Cependant, au-delà de ses avantages indéniables, l'IoT doit également relever des défis et contraintes majeurs pour garantir un déploiement efficace et éthique de ses technologies.

2.1 Des problématiques de sécurité

Une des contraintes principales qu'affronte le déploiement de l'écosystème IoT est liée à sa sécurité. En effet, la confidentialité et la sécurité des données tant au sein du réseau qu'à l'extérieur sont cruciales pour rendre le réseau fonctionnel et utile, tout en préservant l'intégrité des personnes et entreprises utilisants des objets connectés.

En raison des contraintes énergétiques des réseaux IoT, il est souvent compliqué de déployer des mécanismes de chiffrement sur les réseaux en raison de la puissance de calcul demandée par les divers algorithmes de chiffrement. Le réseau peut donc être vulnérable à des attaques d'usurpation d'identité, ainsi que de captations illicites de données, via des attaques de type Man-in-the-Middle. De plus, rendre le réseau IoT accessible sur Internet peut rendre vulnérable les actionneurs du réseau à divers acteurs malveillants : dans le cas d'une maison connectée à réseau complexe, un attaquant pourrait, à titre d'exemple, rendre le contrôle de certains équipements, et demander une rançon à son propriétaire pour qu'il en récupère l'accès.

De plus, ce type de réseau de machines peut contribuer à l'insu de son propriétaire à des attaques d'échelles bien plus importantes, comme des attaques DDoS (Distributed Denial of Service). À partir du moment où le réseau est infecté par un acteur malveillant, ce dernier peut prendre contrôle des machines et les rajouter à un "botnet", un réseau de machines zombies dont il a le contrôle complet. Une fois le contrôle acquis, l'acteur peut ensuite demander à l'ensemble de son réseau d'effectuer de grandes quantités de requêtes diverses sur une machine ou un ensemble de machines spécifique, afin de perturber les services d'une entreprise ou d'un état. Dans ce cas, le réseau IoT lui-même est vulnérable. Le manque de sécurité cryptographique mentionné plus tôt est une vulnérabilité importante étudiée depuis des années.

2.2 De nombreuses normes de communication

L'interopérabilité entre les dispositifs et les plateformes représente un défi essentiel dans le domaine de l'IoT, mais il est souvent confronté à la réalité d'une multiplicité de normes de communication. Les standards et protocoles universels, tels que MQTT, CoAP,

ou encore le protocole HTTP, jouent un rôle crucial en permettant aux dispositifs de communiquer indépendamment de leurs spécifications techniques. Toutefois, la diversité des normes adoptées par différents acteurs peut générer des défis d'interopérabilité, nécessitant une approche concertée pour trouver des solutions.

Malgré les défis, l'émergence de consortiums et d'alliances visant à établir des normes communes témoigne des efforts de l'industrie pour favoriser l'interopérabilité. Ces initiatives facilitent l'adoption de standards partagés, encourageant ainsi la collaboration entre les fabricants et contribuant à unifier les pratiques. Les architectures modulaires et évolutives offrent une perspective positive en permettant l'intégration aisée de nouveaux dispositifs et la mise à jour des plateformes existantes sans perturber l'ensemble du système. Les technologies de middleware, agissant comme des interfaces entre les dispositifs et les plateformes, jouent un rôle crucial en facilitant la communication entre des systèmes hétérogènes.

Bien que certains défis subsistent, l'interopérabilité entre les dispositifs et les plateformes reste un objectif prioritaire, stimulant l'innovation et la coopération au sein de l'écosystème IoT. Ces efforts combinés visent à surmonter les obstacles des normes de communication éparpillées pour construire un environnement favorable à l'épanouissement continu de l'Internet des objets.

2.3 Une scalabilité importante

La scalabilité des réseaux IoT représente à la fois un défi majeur et une nécessité cruciale pour accompagner l'expansion rapide et massive des appareils connectés. La croissance exponentielle du nombre d'objets connectés nécessite une infrastructure réseau capable de s'adapter et de répondre à cette demande croissante sans compromettre les performances.

Pour assurer cette scalabilité, plusieurs aspects doivent être pris en compte. La gestion efficace des adresses IP, notamment avec l'adoption de l'IPv6 permettant un nombre colossal d'adresses uniques, est essentielle pour accompagner le déploiement massif des appareils IoT. De plus, l'utilisation de technologies telles que le Edge Computing, qui décentralise le traitement des données en les rapprochant des appareils, allège la charge sur les réseaux centraux et réduit la latence, contribuant ainsi à une meilleure scalabilité. Par ailleurs, l'adoption de protocoles de communication et de standards interopérables favorise l'extension harmonieuse des réseaux en permettant la connectivité entre des dispositifs provenant de divers fabricants.

Enfin, l'évolution continue des infrastructures réseau, notamment avec l'avènement de la 5G et des technologies de communication à haut débit, offre des solutions pour soutenir la croissance future des réseaux IoT en offrant une bande passante plus large et une connectivité plus fiable. La scalabilité des réseaux IoT est donc un enjeu crucial pour accompagner l'essor de cette technologie, nécessitant une approche proactive et évolutive pour garantir un déploiement réussi et pérenne à grande échelle.

2.4 La difficulté d'un stockage performant et respectueux de l'environnement

2.4.1 La performance des solutions de stockage

La gestion efficace de la connectivité et des énormes quantités de données générées par les réseaux IoT est un autre défi majeur de cette technologie. La connectivité doit être gérée de manière à garantir une disponibilité constante et fiable pour tous les appareils connectés, qu'ils soient situés dans des environnements urbains denses ou des zones reculées. Cela implique la mise en place de réseaux robustes et flexibles, capables de s'adapter aux variations de charge et de trafic, tout en assurant une faible latence et une haute disponibilité. Parallèlement, la gestion des données massives engendrées par ces réseaux nécessite des stratégies de collecte, de stockage, d'analyse et d'utilisation efficaces. Les technologies de traitement distribué, telles que le Big Data et le Cloud Computing, jouent un rôle crucial dans cette gestion, permettant de stocker et d'analyser ces volumes massifs de données de manière efficiente.

De plus, l'adoption de techniques d'apprentissage automatique (Machine Learning) et d'intelligence artificielle pour analyser ces données en temps réel et en extraire des informations pertinentes représente un aspect clé pour exploiter tout le potentiel des réseaux IoT. La sécurisation des données tout au long de leur cycle de vie, de la collecte à l'analyse, demeure également un élément essentiel de la gestion de ces données massives, garantissant la confidentialité, l'intégrité et la disponibilité des informations sensibles.

En somme, la gestion de la connectivité et des données massives dans les réseaux IoT exige une approche complète et intégrée, combinant des technologies de pointe, des stratégies de traitement efficaces et des mesures de sécurité rigoureuses pour garantir un fonctionnement fluide et sécurisé de ces réseaux complexes. Cependant, au-delà des défis opérationnels, l'Internet des objets (IoT) pose également des enjeux importants sur le plan environnemental.

2.4.2 L'empreinte environnementale des datacenters

La croissance exponentielle des dispositifs connectés et la génération massive de données associée ont des implications directes sur la consommation d'énergie et les ressources. Les centres de données, qui jouent un rôle central dans le stockage et le traitement des données IoT, requièrent d'importantes quantités d'électricité pour maintenir leurs opérations. Cette demande accrue en énergie contribue à l'empreinte carbone globale des infrastructures informatiques, exacerbant les préoccupations liées au changement climatique. Aujourd'hui, les datacenters sont parmis les principaux pollueurs mondiaux. La plupart sont alimentés en énergies fossiles comme le gaz ou le charbon. C'est notamment le cas de deux tiers des infrastructures chinoises.

L'utilisation généralisée de technologies de traitement distribué, telles que le Big Data et le Cloud Computing, bien que cruciale pour répondre aux besoins de stockage massif, intensifie également la pression environnementale. Les centres de données nécessitent une climatisation constante et une grande quantité d'eau pour prévenir la surchauffe des serveurs, ajoutant ainsi une couche supplémentaire de consommation énergétique. En l'année 2020, la consommation énergétique des datacenters était estimée à 650 térawattheures, dépassant ainsi la consommation totale de la France. Avec la croissance exponentielle des

besoins en stockage de données, ce chiffre pourrait être multiplié par 5 d'ici 2030. De plus, la fabrication, la maintenance et l'élimination des équipements électroniques utilisés dans ces centres contribuent à la production de déchets électroniques, présentant des défis supplémentaires en matière de gestion des déchets et de recyclage.

Pour atténuer les impacts environnementaux des datacenters, il est impératif d'explorer ces solutions éco-responsables, comprenant l'optimisation énergétique, l'utilisation d'énergies renouvelables, et le déploiement de technologies de stockage plus efficientes sur le plan énergétique. Ainsi, des géants de la Tech se tournent vers des solutions innovantes visant à minimiser leur empreinte écologique. Parmi les approches adoptées, on retrouve l'utilisation de méthodes de refroidissement par évaporation, ainsi que la mise en œuvre de contrôles intelligents de température et d'éclairage pour optimiser la consommation énergétique. Certains acteurs de l'industrie réutilisent également le surplus de chaleur généré pour chauffer des habitations, contribuant ainsi à une utilisation plus efficace de l'énergie produite.

Dans la quête d'un stockage plus durable, plusieurs solutions émergent. Le stockage sur bande, moins énergivore que le stockage sur disque, se distingue par un coût financier total considérablement réduit pour la conservation de grandes quantités de données. En effet, le coût financier total de la conservation d'1 pétaoctet de données sur bande pendant 5 ans est 3,5 fois moins élevé qu'un stockage sur disque. La consolidation des données sur un seul serveur représente également une stratégie efficace pour réduire la consommation d'énergie liée au stockage. Sans surprise, l'une des solutions cruciales reste l'utilisation d'énergies renouvelables, que ce soit pour des datacenters sur site ou dans le cloud Des études suggèrent que la transition vers des sources d'énergie plus durables pourrait permettre à l'industrie numérique de réduire significativement ses émissions de gaz à effet de serre.

Il est ainsi recommandé aux utilisateurs d'évaluer les mesures prises par leurs fournisseurs de solutions cloud pour réduire l'impact environnemental du stockage de données. Des indicateurs tels que les normes ISO 50001, ISO 14001, PUE, WUE et le taux d'énergies renouvelables peuvent servir de critères pour évaluer l'engagement environnemental d'une entreprise. Pour atténuer les impacts environnementaux des datacenters, il est impératif d'explorer ces solutions éco-responsables, comprenant l'optimisation énergétique, l'utilisation d'énergies renouvelables et le déploiement de technologies

2.5 Une expansion (trop) rapide du marché des objets connectés

L'essor rapide de l'Internet des Objets (IdO) a engendré des préoccupations significatives quant à son impact environnemental négatif. Selon une étude conjointe menée par l'Arcep et l'ADEME sur l'évaluation de l'impact environnemental du numérique en France, bien que les équipements IdO représentent actuellement moins de 7% de l'empreinte des terminaux, leur potentiel de développement massif pourrait considérablement modifier les effets environnementaux associés. L'ADEME souligne que la fabrication des objets connectés concentre la majeure partie des émissions de gaz à effet de serre (GES), représentant 73% du bilan carbone de leur cycle de vie complet. Cette phase inclut des aspects tels que l'assemblage, le transport et l'extraction de matières premières. Cette constatation met en lumière le poids écologique substantiel lié à la production même de ces dispositifs.

Aujourd'hui, une tendance omniprésente pousse les consommateurs à acquérir des objets connectés, souvent caractérisés par une durée de vie limitée. Cette réalité s'inscrit dans un contexte où certaines marques adoptent des pratiques d'exclusivité, contraignant les utilisateurs à multiplier leurs acquisitions pour garantir une compatibilité entre différents dispositifs. Un exemple concret de cette situation peut être observé dans le secteur des assistants vocaux, où la concurrence entre les fournisseurs crée des obstacles significatifs à l'interopérabilité. Ces entraves incitent les consommateurs à s'engager exclusivement avec une seule plateforme et limitent la possibilité d'utiliser différents assistants vocaux sur un même dispositif intelligent. Des entreprises, comme Apple, adoptent également une stratégie d'écosystème fermé, où l'acquisition d'objets de la marque devient le seul moyen pour les utilisateurs d'exploiter pleinement leurs fonctionnalités, créant ainsi des barrières supplémentaires à l'interopérabilité et favorisant la fidélisation au sein de leur écosystème exclusif. Ces tendance sont soulignées par Mme Margrethe Vestager, comissaire européenne à la concurrence de 2014 à 2023, qui a noté la caractérisation de ce marché par des barrières élevées à l'entrée, un nombre limité d'acteurs verticalement intégrés, et des préoccupations concernant l'accès aux données, l'interopérabilité et les pratiques d'exclusivité.

FIGURE 11 – Ecosystème Apple

Par ailleurs, la prolifération d'objets connectés souvent perçus comme des gadgets soulève des interrogations sur la réelle utilité de certains de ces dispositifs. Les industries semblent parfois créer des besoins artificiels pour stimuler la demande et accroître leurs ventes. Un cas illustratif est celui des montres connectées, où de nombreux utilisateurs optent pour ces dispositifs sans exploiter pleinement leurs fonctionnalités liées à la santé, répliquant des services déjà accessibles via leur smartphone. Cette culture de la surconsommation d'objets connectés, combinée à des fonctionnalités superflues, soulève des préoccupations quant à la durabilité, à l'impact environnemental et à la véritable utilité de ces innovations technologiques dans la vie quotidienne.

Au-delà de la phase de fabrication, l'utilisation quotidienne des objets connectés contribue également de manière significative à leur impact environnemental. La connectivité sans fil, nécessaire au fonctionnement de ces dispositifs, exige une quantité importante d'énergie. De plus, l'appariement de nombreux objets connectés avec d'autres appareils pour assurer leur fonctionnement (comme les écouteurs, enceintes, montres, casques de réalité virtuelle...) entraîne une duplication de la consommation énergétique, illustrant le manque d'efficacité énergétique de ces équipements.

Le nombre massif d'objets connectés dans le monde, estimé à environ 15 milliards en 2018 et susceptible de dépasser les 45 milliards d'ici 2030 selon l'ADEME, aggrave ces inconvénients. Cette projection ferait des objets connectés la deuxième source de pollutions numériques dans le monde, juste après le réseau Internet et les data-centers. Une étude réalisée en 2020 pour un groupe parlementaire du Parlement européen classe déjà l'Internet des Objets au deuxième rang des causes d'impact environnemental les plus importantes, soulignant le poids significatif de certaines catégories, telles que les contrôles des bâtiments commerciaux et les compteurs intelligents, dans cette équation.

La croissance rapide du marché des objets connectés soulève donc des préoccupations sérieuses quant à son impact environnemental, soulignant la nécessité de solutions innovantes et durables pour atténuer ces répercussions négatives et promouvoir un développement plus responsable de cette technologie. Face à la prolifération d'objets connectés à la durée de vie limitée, aux fonctionnalités souvent superflues, et aux pratiques commerciales incitant à la surconsommation, il est impératif d'adopter une approche plus réfléchie. Les consommateurs doivent être encouragés à opter pour une consommation plus responsable, en privilégiant des objets connectés dont les caractéristiques répondent réellement à leurs besoins. Un examen critique de l'utilité réelle d'un dispositif avant l'achat contribuerait à éviter l'accumulation d'appareils redondants. De plus, en mettant particulièrement l'accent sur des dispositifs de gestion et de minimisation de la consommation énergétique, les consommateurs peuvent jouer un rôle crucial dans la transition vers une utilisation plus durable et éco-responsable des objets connectés, tout en exploitant pleinement leur potentiel positif pour l'environnement.

3 Expérimentation - Projet

3.1 Introduction

La pollution lumineuse mondiale est un problématique à fort enjeu économique et environnementale. Nous avons jugé pertinent de réaliser une expérimentation liée à celle-ci. Afin de tenir informés la population de sa consommation de lumière, nous avons utilisé un capteur de détection de mouvement appelé capteur PIR pour automatiser le déclenchement des éclairages en rendant compte de cette activité dans une page web.

Ce projet a pour vocation de manipuler les concepts présentés dans la partie théorique de notre rapport. Chaque aspect du projet sera présenté de manière exhaustive, en allant de la justification de la sélection des composants à la mise en œuvre concrète, en passant par les résultats obtenus. Les objectifs spécifiques comprennent la description de l'architecture matérielle et logicielle, les détails de la configuration, les résultats des tests, ainsi que des réflexions sur les limites du projet et les améliorations possibles. En fournissant ces informations, le rapport offre une vision approfondie de la conception et de l'implémentation du système, tout en soulignant son importance potentielle dans le domaine de l'IoT.

3.2 Matériel nécessaire

Pour la mise en œuvre d'un réseau IoT, diverses technologies peuvent être exploitées, nous avons choisis de présenter certaines d'entre elles : l'Arduino, le Raspberry Pi et l'ESP. Dans la réalisation de notre projet, nous n'avons utilisé que l'ESP8266 mais envisageons des pistes d'amélioration nécessitant l'utilisation de ces autres technologies.

3.2.1 Arduino

3.2.1.1 Présentation générale

Un Arduino est une plateforme de prototypage électronique open-source qui permet aux personnes, même sans une expertise approfondie en électronique, de créer des projets interactifs. L'Arduino se compose d'une carte de circuit imprimé avec un microcontrôleur et d'un environnement de développement logiciel qui permet de programmer ce microcontrôleur.

Les cartes Arduino sont équipées de diverses entrées/sorties (E/S) numériques et analogiques, ce qui permet de connecter différents capteurs, actionneurs et autres composants électroniques. Ces cartes sont largement utilisées pour créer des projets DIY (Do It Yourself), des prototypes, des œuvres d'art interactive, des dispositifs automatisés, des robots, etc.

L'environnement de développement Arduino comprend un langage de programmation simplifié basé sur Wiring, ainsi qu'une interface utilisateur conviviale. Les utilisateurs peuvent écrire du code pour contrôler le comportement de leur projet, puis télécharger ce code sur la carte Arduino via un câble USB. Cela permet à la carte de fonctionner de manière autonome selon le programme chargé.

L'open-source est un élément clé d'Arduino, ce qui signifie que les schémas matériels, les logiciels et la plupart des composants associés sont disponibles pour que quiconque puisse les utiliser et les modifier.

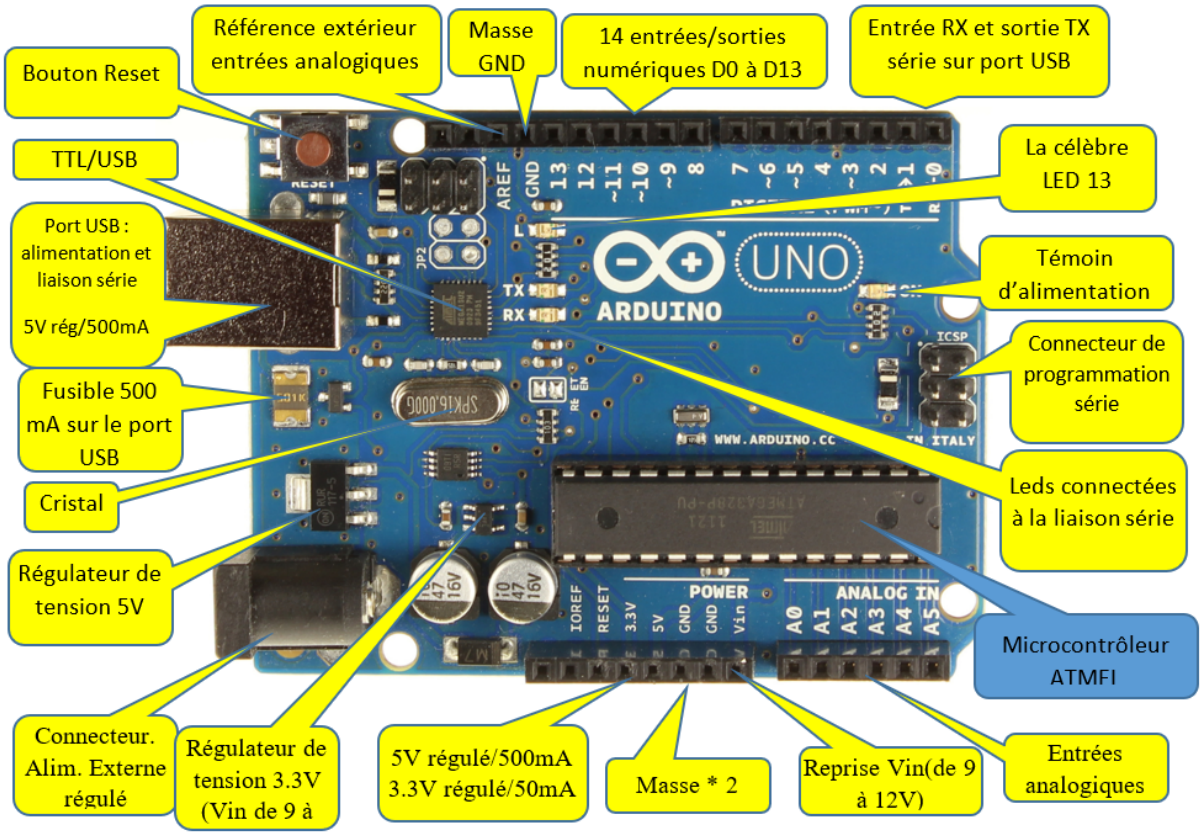


FIGURE 12 – Schéma descriptif de la carte Arduino

3.2.1.2 Arduino et L'IoT

Arduino est également largement utilisé dans le domaine de l'Internet des objets (IoT). L'IoT implique la connexion d'objets physiques à Internet pour collecter et échanger des données. Les cartes Arduino, avec leur facilité d'utilisation et leur polyvalence, peuvent être intégrées dans des projets IoT pour créer des prototypes et des solutions personnalisées.

Voici quelques façons dont Arduino est utilisé dans le contexte de l'IoT :

- **Collecte de données :** Arduino peut être équipé de capteurs divers tels que des capteurs de température, d'humidité, de mouvement, etc. Ces capteurs peuvent collecter des données environnementales qui peuvent ensuite être transmises à un serveur ou stockées localement.
- **Communication sans fil :** Arduino peut être couplé avec des modules de communication sans fil tels que Wi-Fi, Bluetooth, Zigbee, LoRa, etc., pour permettre la transmission des données vers des serveurs, d'autres appareils ou des plateformes IoT.
- **Contrôle à distance :** En utilisant des modules de communication, Arduino peut être contrôlé à distance. Cela permet de prendre des mesures ou de modifier le comportement d'un dispositif à distance via Internet.
- **Automatisation :** Les projets IoT basés sur Arduino peuvent être utilisés pour l'automatisation de tâches domestiques, industrielles ou agricoles. Par exemple, la gestion intelligente de l'énergie, l'irrigation automatisée basée sur les conditions météorologiques, etc.

- **Prototypage rapide :** Arduino facilite le prototypage rapide d'applications IoT en fournissant une plateforme matérielle et un environnement de développement convivial. Cela permet aux développeurs de tester rapidement des idées et de créer des prototypes fonctionnels.

Enfin, bien que l'Arduino soit idéal pour le prototypage, dans des déploiements IoT à plus grande échelle, on peut passer à des solutions matérielles et logicielles plus spécialisées en fonction des besoins spécifiques du projet. Arduino sert souvent de point de départ pour le développement d'applications IoT avant de migrer vers des solutions plus robustes.

3.2.2 Raspberry Pi

3.2.2.1 Présentation générale

Le Raspberry Pi est un micro-ordinateur monocarte, doté de composants matériels essentiels, développé par la Raspberry Pi Foundation. L'objectif principal du créateur de ce dispositif, Eben Upton, était de créer un outil très accessible pour permettre aux étudiants d'apprendre plus efficacement la programmation informatique et le développement.

Le Raspberry Pi se distingue alors par son format compact, son coût, à l'origine, abordable[8] et sa modularité. Il fonctionne comme un ordinateur de poche, embarquant un processeur, une mémoire vive (RAM) et des options de stockage. Sa polyvalence ainsi que sa conception ouverte favorisent l'expérimentation et le prototypage rapide, en faisant un choix de prédilection pour les projets liés à l'IoT.

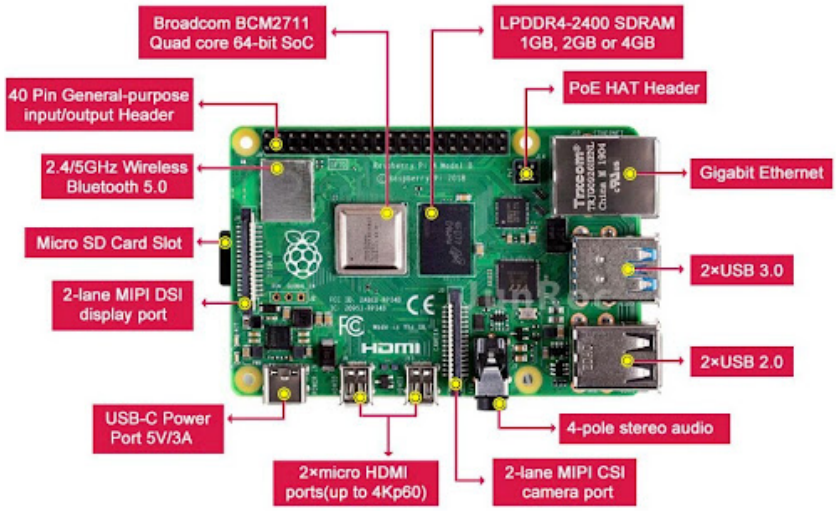


FIGURE 13 – Raspberry Pi 4 modèle B annoté de ses spécifications techniques

8. En raison des pénuries de composants, le prix des Raspberry Pi ont fortement augmenté depuis 2022.

Les composants d'un Raspberry Pi

La configuration exacte de ce dispositif peut varier en fonction du modèle spécifique choisi. En effet, la Raspberry Pi Foundation propose régulièrement de nouveaux modèles avec des fonctionnalités améliorées. Voici une liste des principaux composants d'un Raspberry Pi typique :

- **Micro-processeur ARM (CPU)** : Le Raspberry Pi intègre un processeur qui peut varier selon les modèles. Le Raspberry Pi 4 utilise, par exemple, un processeur Broadcom BCM2711, quad-core Cortex-A72 (ARM v8) 64-bit
- **Carte Graphique (GPU) :** Elle contribue à la polyvalence du Raspberry Pi en permettant des applications visuelles et multimédias.
- **Mémoire vive (RAM) :** La quantité de RAM peut varier selon le modèle. Par exemple, le Raspberry Pi 4 est disponible avec des options de 2 Go, 4 Go ou 8 Go de RAM.
- **Carte microSD :** Ce composant sert de support de stockage principal pour le système d'exploitation et les données. C'est sur la carte microSD que le Raspberry Pi démarre.
- **Ports USB :** Ils permettent de connecter des périphériques externes tels que claviers, souris, caméras, etc. Le nombre de ports USB peut varier en fonction du modèle.
- **Ports GPIO (General Purpose Input/Output) :** Ces ports permettent au Raspberry Pi d'interagir avec le monde extérieur en connectant des capteurs, des actionneurs et d'autres composants électroniques.
- **Connectivité avec et/ou sans fil :** Certains modèles du Raspberry Pi disposent d'un port Ethernet pour la connexion réseau filaire. De nombreux modèles intègrent également une connexion Wi-Fi et Bluetooth, offrant une connectivité sans fil.
- **Ports HDMI :** Ils permettent de connecter le Raspberry Pi à un écran externe, facilitant l'affichage du système d'exploitation et des applications. Le Rasberry Pi 4 dispose de ports micro-HDMI.
- **Connecteur d'alimentation :** Le Raspberry Pi est alimenté par un adaptateur secteur via un connecteur dédié. Pour le Raspberry Pi 4, c'est un port USB-C.
- **Sortie audio :** Certains modèles incluent une sortie audio pour la connexion à des haut-parleurs ou à un système audio.

Les systèmes d'exploitation d'un Raspberry Pi

Le Raspberry Pi est compatible avec plusieurs systèmes d'exploitation, mais l'un des plus populaires et largement utilisés est Raspbian, également connu sous le nom de Raspberry Pi OS. C'est le système d'exploitation officiel développé spécifiquement pour le Raspberry Pi par la Raspberry Pi Foundation. Il est basé sur la distribution Linux Debian et est optimisé pour tirer pleinement parti du matériel du Raspberry Pi. Il offre une interface utilisateur graphique (GUI) conviviale et est adapté aux débutants comme aux utilisateurs expérimentés.

Il est également possible d'installer d'autres systèmes d'exploitation comme Ubuntu Mate, Arch Linux ARM et d'autres distributions Linux spécialisées. De son côté, Microsoft propose une version allégée de Windows 10 appelée Windows 10 IoT Core, conçue spécifiquement pour les dispositifs IoT tels que le Raspberry Pi. Cependant, cette version

de Windows est moins couramment utilisée que les distributions Linux sur le Raspberry Pi.

L'installation du système d'exploitation se fait via la carte SD, sur laquelle il est généralement installé. Le processus d'installation implique de télécharger l'image du système d'exploitation, de la copier sur la carte microSD, puis d'insérer la carte dans le Raspberry Pi pour l'amorçage.

3.2.3 Raspberry Pi et l'IoT

Le Raspberry Pi joue un rôle significatif dans le domaine de l'Internet des Objets, offrant une plateforme polyvalente pour le développement de projets IoT. En plus de son prix abordable et de son faible volume, les fonctionnalités WI-FI et Bluetooth facilitent son intégration dans des réseaux IoT sans fil afin, notamment, de communiquer avec d'autres dispositifs et de collecter des données à distance. Les ports GPIO permettent, quant à eux, de connecter des capteurs, actionneurs et autres composants électroniques, ouvrant ainsi la voie à des interactions physiques avec l'environnement.

Ce micro-ordinateur peut également exécuter des systèmes d'exploitation spécialement conçus pour l'IoT, tels que Raspbian Lite qui offre une empreinte légère et une flexibilité accrue pour les projets centrés sur la connectivité et la collecte de données.De plus, le Raspberry Pi prend en charge plusieurs langages de programmation, ce qui facilité le développement d'applications pour l'IoT. Python est particulièrement utilisé sur ce dispositif de par sa simplicité et sa flexibilité.Finalement, la communauté Raspberry Pi est dynamique et offre un soutien considérable aux utilisateurs. En effet, de nombreuses ressources tels que des forums, tutoriels et projets open source, sont disponibles sur internet, facilitant ainsi l'apprentissage.

En résumé, le Raspberry Pi constitue une plateforme idéale pour les projets IoT en raison de sa facilité d'utilisation, de son coût abordable, de sa connectivité intégrée et de sa polyvalence dans l'interaction avec le monde physique.

3.2.4 ESP8266

L'ESP8266 correspond à un module Wi-Fi portable compacte utilisé pour ajouter une connectivité sans fil à un capteur. L'ESP32 est une version avancée de l'ESP8266 qui en plus du gain de performance intègre des fonctionnalités Bluetooth. Les deux permettent de transmettre les informations d'un capteur de la couche perception vers une passerelle, et donc d'intégrer le capteur à l'environnement IoT.

L'ESP8266 se compose de différents pins (ou broches), des réceptacles de courant électrique permettant de le connecter à un dispositif hôte selon les exigences du projet :

- **Pins GPIO (General Purpose Input/Output)** : polyvalents, ils peuvent être configurés soit comme entrées numériques, soit comme sorties afin d'interagir avec le hôte.
- **Pins TX et RX** : interface à travers lesquels l'ESP8266 émets et reçoit des données en communication série avec un ordinateur lors de la phase de programmation.
- **Pin A0** : utilisée pour lire des valeurs analogiques, il s'agit du point permettant de recueillir les données des capteurs, avec une résolution de 10 bits (valeurs de 0 à 1023, correspondant à la tension reçue en entrée, entre 0V et 1V).

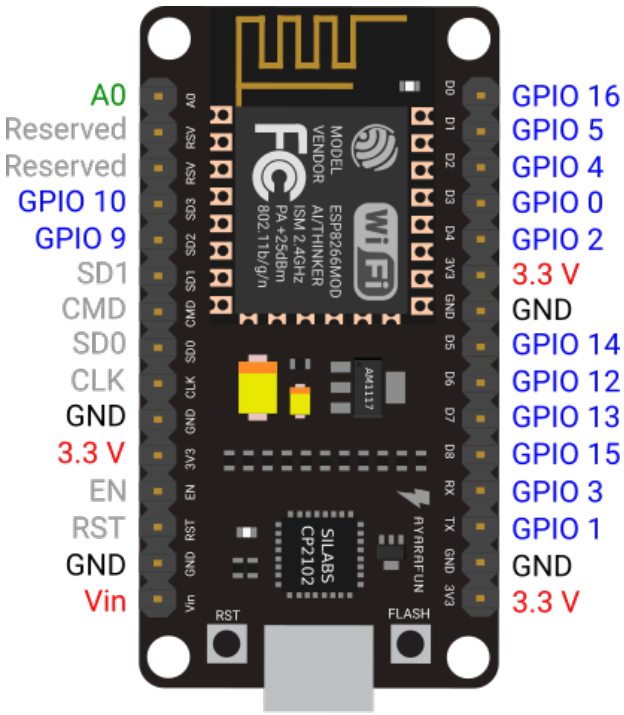


FIGURE 14 – ESP8266 et ses différentes broches

- **Pins SDx, CMD et CLK** : relatifs à la communication avec une carte SD. SDx s'occupent des transferts de données, tandis que CMD (Command) écrit des commandes à la carte SD et que CLK (Clock) synchronise la communication. Une telle connectivité peut répondre à des besoins de journalisation des données ou de mise à jour de l'ESP8266.
- **Pin EN (Enable)** : met en marche si mis en HIGH (HIGH par défaut).
- **Pin RST (Reset)** : réinitialise l'ESP8266 si mis en LOW (HIGH par défaut).
- **Pins 3.3V, GND (Ground) et Vin (Voltage Input)** : relatifs à l'alimentation de l'ESP8266.

3.3 Architecture

L'architecture du projet est très simple puisque nous n'utilisons qu'un seul capteur branché sur un esp8266 qui lui envoie via Wifi les données captées.

3.3.1 Fonctionnment capteur PIR :

Les détecteurs PIR détectent les mouvements en capturant le rayonnement infrarouge émis par les personnes ou les objets dans la zone souhaitée et en mesurant le changement de température.

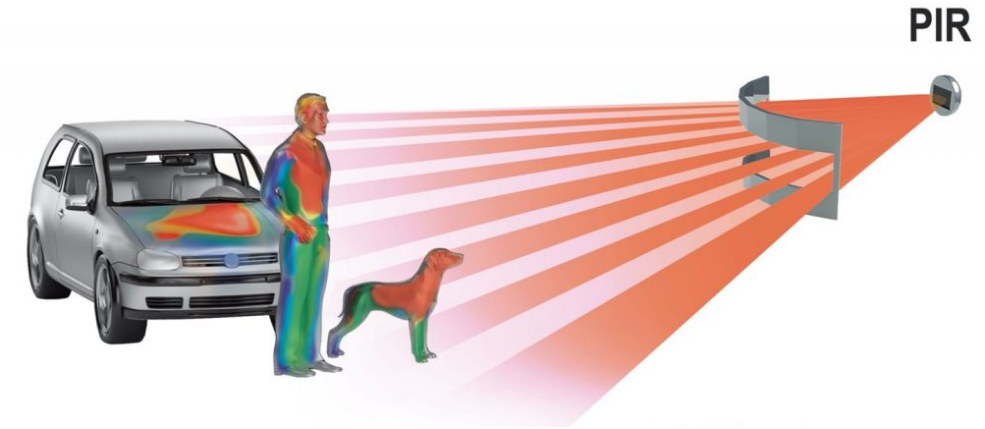


FIGURE 15 – Schéma du fonctionnement d'un capteur PIR

3.3.2 Étapes de câblage :

1. Connectez le fil VCC du capteur PIR à une broche 3.3V sur la carte ESP8266
2. Connectez le fil GND du capteur PIR à une broche GND sur la carte ESP8266
3. Connectez le fil OUT (signal de sortie) du capteur PIR à une broche numérique (par exemple, D1) sur la carte ESP8266

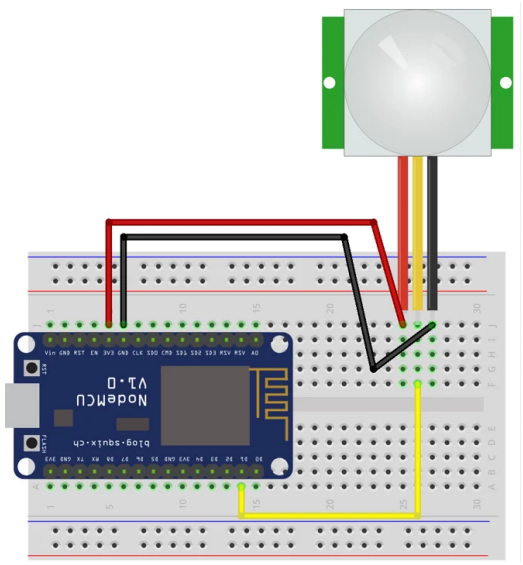


FIGURE 16 – Schéma des branchement PIR-ESP8266

3.4 Protocole

Dans ce projet, nous utilisons un serveur Web intégré à l'ESP8266 pour fournir une interface de visualisation de l'état d'un capteur PIR via une page HTML. Les requêtes HTTP sont utilisées pour obtenir l'état du capteur de manière asynchrone et mettre à jour dynamiquement la page sans avoir à recharger la page complète.

3.4.1 Client (Navigateur Web) demande la page :

Lorsque vous ouvrez la page web sur votre navigateur, une requête HTTP est envoyée à l'adresse IP du module ESP8266 sur le port 80 (car le serveur Web est configuré pour écouter sur ce port).

3.4.2 ESP8266 (Serveur Web) reçoit la demande :

Le serveur Web ESP8266 (qui est configuré pour répondre aux requêtes sur les chemins '/' et '/getPIRState') détecte la requête HTTP. En fonction du chemin de la requête, il appelle la fonction correspondante.

3.4.3 Traitement de la demande :

Si la requête est pour la racine ('/'), la fonction `handleRoot` est appelée. Cette fonction génère une réponse HTML en remplaçant %ETAT% par l'état actuel du capteur PIR (1 pour mouvement détecté, 0 sinon). Si la requête est pour '/getPIRState', la fonction `getPIRState` est appelée. Cette fonction renvoie simplement l'état actuel du capteur PIR en texte brut (1 ou 0).

3.4.4 Réponse au client :

Le serveur Web renvoie la réponse générée au client. Dans le cas de la page principale ('/'), il envoie la page HTML mise à jour avec l'état actuel du capteur PIR. Dans le cas de '/getPIRState', il envoie simplement l'état en texte brut.

3.4.5 JavaScript sur la page HTML côté client :

Le code JavaScript inclus dans la page HTML s'exécute côté client. Il utilise une requête asynchrone (AJAX) pour interroger périodiquement le serveur (/getPIRState) et mettre à jour dynamiquement le contenu de la page avec l'état actuel du capteur PIR.

3.4.6 Mise à jour dynamique de la page :

Le JavaScript met à jour la partie de la page où se trouve l'élément avec l'ID "etatPIR" en fonction de la réponse du serveur, indiquant s'il y a un mouvement détecté ou non.

En résumé, lorsque vous ouvrez la page web, le navigateur envoie des requêtes au serveur ESP8266, le serveur répond avec l'état actuel du capteur PIR, et le JavaScript sur la page met à jour dynamiquement le contenu pour refléter cet état. Ce processus se répète périodiquement en raison de l'intervalle défini par `setInterval(miseAJour, 1000);`.

3.5 Améliorations possibles

3.5.1 Raspberry PI

Intégrer un Raspberry Pi dans notre projet aurait pu apporter plusieurs avantages, offrant une plateforme plus puissante et polyvalente pour la gestion du capteur PIR et la mise en place d'un serveur web. En éliminant le besoin d'un ordinateur externe pour héberger la page web, cela peut rendre le système plus autonome et plus facile à gérer. De plus, cela aurait rendu notre projet plus scalable et extensible, permettant l'intégration de plusieurs capteurs et la gestion de données provenant de différentes sources.

Par ailleurs, la consommation d'énergie ainsi que l'encombrement peuvent être réduits, surtout avec les modèles récents, conçus pour être économes en énergie. Cela peut être particulièrement avantageux si notre projet nécessite un fonctionnement continu avec une consommation d'énergie minimale dans un espace restreint.

Sur le plan financier, les Raspberry Pi sont généralement plus abordables que la plupart des ordinateurs. Ainsi, cela permet de créer un système tout-en-un, où le traitement, la détection de mouvement et l'hébergement du serveur web sont tous pris en charge par la même carte. Cette intégration simplifie la gestion et la maintenance du système.

En termes de fiabilité, les Raspberry Pi sont conçus pour une utilisation continue et peuvent fonctionner de manière fiable pendant de longues périodes. Si la fiabilité est une considération importante pour votre projet, un Raspberry Pi pourrait être un choix plus robuste qu'un ordinateur.

La flexibilité et l'extensibilité des Raspberry Pi sont également des points forts. Ces cartes peuvent être étendues avec des modules complémentaires (HATs), offrant ainsi la possibilité d'ajouter des fonctionnalités supplémentaires en fonction des besoins spécifiques du projet.

3.5.2 Protocole MQTT

Le protocole MQTT (Message Queuing Telemetry Transport) est un protocole de communication légère et asynchrone conçu pour les dispositifs connectés à l'Internet des objets (IoT). Il repose sur le principe de la publication/abonnement, où les dispositifs peuvent publier des messages sur des "sujets" spécifiques et s'abonner à ces sujets pour recevoir les messages pertinents. MQTT est efficace, simple et adapté aux environnements avec des ressources limitées, favorisant une communication bidirectionnelle fiable entre les dispositifs IoT et les serveurs.

Un broker MQTT (Message Queuing Telemetry Transport) est un serveur intermédiaire qui facilite la communication entre les dispositifs connectés dans un réseau IoT utilisant le protocole MQTT. Le broker joue un rôle essentiel en tant que centre de distribution des messages, permettant aux dispositifs de publier et de souscrire à des informations.

Un sujet (topic) en MQTT est une chaîne de caractères utilisée pour identifier la destination d'un message. Les dispositifs publient des messages sur des sujets et s'abonnent à des sujets spécifiques pour recevoir les messages pertinents. Les sujets sont hiérarchiques, permettant une structuration logique dans l'organisation des messages.

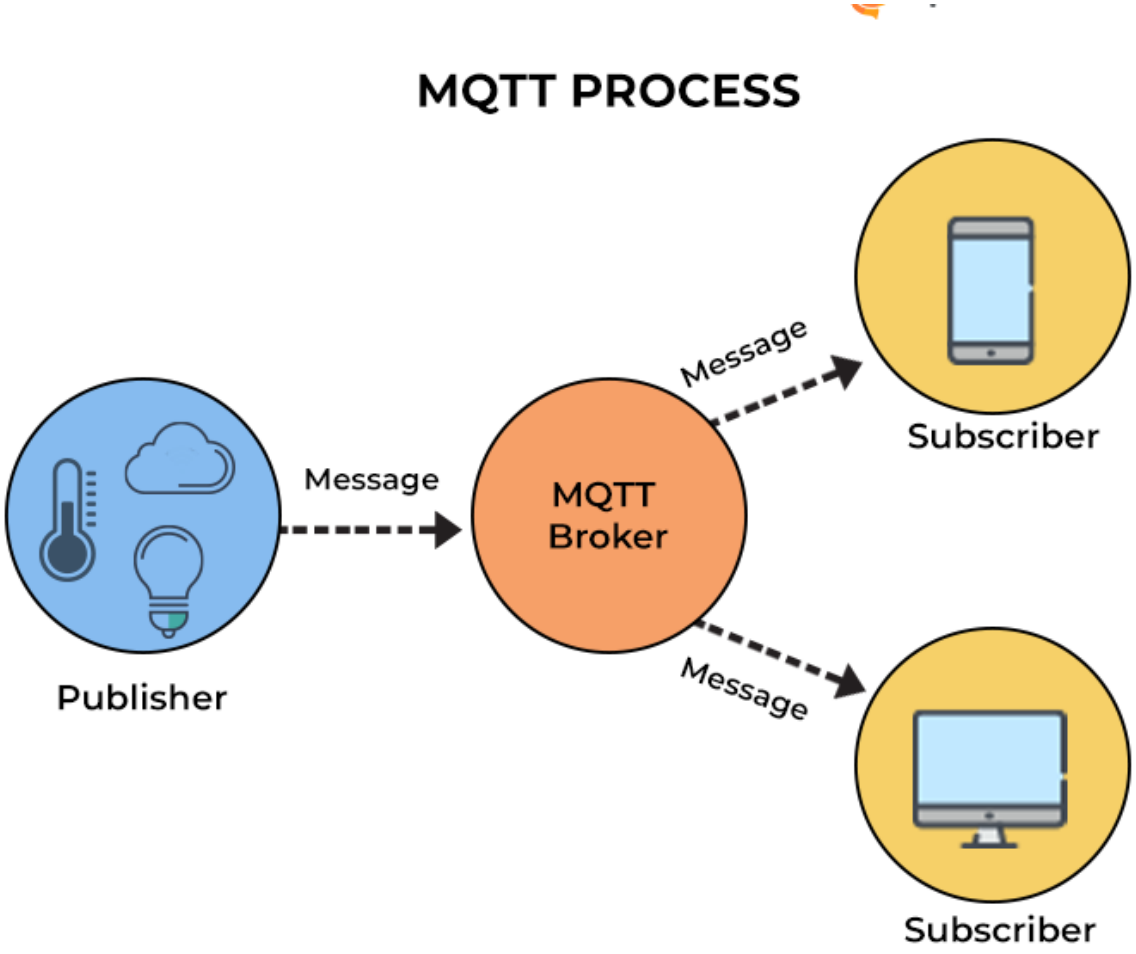


FIGURE 17 – Schéma simplifié du protocole MQTT

3.5.3 Raspberry Pi et protocole MQTT

La combinaison de ces deux technologies présentent une optimisation intéressante de notre projet. L'ESP8266, agissant en tant que capteur PIR, pourrait être configuré en tant que publieur (publisher) dans le contexte de MQTT. Lorsque le capteur détecte un mouvement, l'ESP8266 publie un message sur un sujet MQTT spécifique, contenant l'information sur l'état du capteur (par exemple, "motion detected").

Le Raspberry Pi, agissant comme un serveur central, pourrait être configuré en tant qu'abonné (subscriber) dans le contexte de MQTT. Le Raspberry Pi s'abonne au sujet spécifique sur lequel l'ESP8266 publie les informations sur l'état du capteur PIR. Lorsqu'un mouvement est détecté et que l'ESP8266 publie un message, le Raspberry Pi reçoit automatiquement cette information en tant qu'abonné MQTT.

Conclusion

Ce projet sur l'Internet des Objets (IoT) et son impact sur l'environnement a été une exploration approfondie des vastes implications technologiques de l'IoT dans divers domaines, allant de la santé à l'industrie, en mettant l'accent sur les opportunités et les défis qu'il présente pour la préservation de notre environnement.

Nous avons commencé par une analyse approfondie de l'IoT, plongeant dans ses fondements, ses mécanismes de fonctionnement et ses différentes couches. Comprendre la structure et la dynamique sous-jacentes de l'IoT nous a permis d'apprécier pleinement son potentiel et ses implications dans notre société moderne.

En explorant les applications concrètes de l'IoT, nous avons souligné plusieurs exemples marquants de son utilisation quotidienne, démontrant comment cette technologie peut être un catalyseur majeur pour des changements positifs en matière d'environnement. Des applications dans le domaine de la santé, où les dispositifs IoT peuvent surveiller et améliorer la qualité de vie, à l'industrie, où ils peuvent optimiser les processus pour réduire les déchets et les émissions, nous avons illustré comment chaque secteur peut bénéficier de manière significative de cette technologie émergente.

La phase d'expérimentation de ce projet a été particulièrement instructive. En codant un capteur PIR pour automatiser les éclairages et en rendant compte de cette activité via une page web, nous avons concrètement expérimenté la puissance de l'IoT dans la création de solutions pratiques et efficaces pour minimiser la consommation d'énergie. Cette expérience a été un exemple vivant de la façon dont la connectivité intelligente peut réduire le gaspillage énergétique en adaptant les ressources à la demande réelle.

En conclusion, ce projet a mis en lumière le rôle crucial que joue l'IoT dans la préservation de notre environnement. Tout en offrant des solutions novatrices pour améliorer notre quotidien, cette technologie présente également des défis, notamment en termes de sécurité et de gestion des données. Néanmoins, en utilisant judicieusement et de manière responsable l'IoT, nous pouvons façonner un avenir plus durable, où la technologie agit comme un moteur de progrès tout en préservant notre précieux écosystème.

3.6 Bibliographie

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things : A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys and Tutorials, 17(4), 2347 2376. https ://doi.org/10.1109/comst.2015.2444095

Cvitić, I., Vujić, M., & Husnjak, S. (2016). Classification of security risks in the IoT environment. Dans Annals of DAAAM for . . . & proceedings of the . . . International DAAAM Symposium .. (p. 0731 0740). https ://doi.org/10.2507/26th.daaam.proceedings.102

Elhadi, S., Marzak, A., Sael, N., & Merzouk, S. (2018). Comparative study of IoT protocols. Social Science Research Network. https ://doi.org/10.2139/ssrn.3186315

Farahani, S. (2011). ZigBee wireless networks and transceivers. newnes.

Muangprathub, J., Boonnam, N., Kajornkasirat, S., Lekbangpong, N., Wanichsombat, A., & Nillaor, P. (2019). IoT and agriculture data analysis for smart farm. Computers and Electronics in Agriculture, 156, 467 474. https ://doi.org/10.1016/j.compag.2018.12.011

Naik, N. (2017). Choice of effective messaging protocols for IoT systems : MQTT, CoAP, AMQP and HTTP. https ://doi.org/10.1109/syseng.2017.8088251

Ramya, C. M., Shanmugaraj, M., & Prabakaran, R. (2011). Study on ZigBee technology. https ://doi.org/10.1109/icectech.2011.5942102

Safaric, S., & Malarić, K. (2006). ZigBee Wireless Standard. Proceedings Elmar .. https ://doi.org/10.1109/elmar.2006.329562

Tightiz, L., & Yang, H. (2020). A comprehensive review on IoT protocols' features in smart grid communication. Energies, 13(11), 2762. https ://doi.org/10.3390/en13112762

Construire une passerelle IoT Raspberry Pi ? Avantages, tutoriel, lacunes et alternative. (s. d.). Consulté 13 décembre 2023, à l'adresse https ://dusuniot.com/fr/blog/is-raspberry-pi-an-iot-gateway/

Dominique. (2017, janvier 31). Le guide pour bien démarrer sur Raspberry. Le Blog Gotronic. https ://www.gotronic.fr/blog/guides/raspberry/

[Dossier] L'Internet des objets est-il soutenable ? - Labo. (s. d.). Consulté 13 décembre 2023, à l'adresse https ://labo.societenumerique.gouv.fr/fr/articles/dossier-linternet-des-objets-est-il-soutenable/

Dutta, M., & Gupta, D. (2023). Green IoT for Sustainable Smart Vertical Farming : A Comprehensive Analysis. 2023 IEEE 2nd International Conference on Industrial Electronics : Developments & Applications (ICIDeA), 175-180. https ://doi.org/10.1109/ICIDeA59866.2023.1029

Farooq, M. S., Riaz, S., Abid, A., Abid, K., & Naeem, M. A. (2019). A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. IEEE Access, 7, 156237-156271. https ://doi.org/10.1109/ACCESS.2019.2949703

Green IoT for Sustainable Smart Vertical Farming : A Comprehensive Analysis | IEEE Conference Publication | IEEE Xplore. (s. d.). Consulté 13 décembre 2023, à l'adresse https ://ieeexplore.ieee.org/document/10295191

Installation de Raspbian avec NOOBS | Projets de codage pour les enfants et les adolescents. (s. d.). Consulté 13 décembre 2023, à l'adresse https ://projects.raspberrypi.org/fr-FR/projects/noobs-install IoT-Enabled Smart Benzene Gas Detection System in Petrol Pumps for Smart City Applications | IEEE Conference Publication | IEEE Xplore. (s. d.). Consulté 13 décembre 2023, à l'adresse https ://ieeexplore.ieee.org/document/10331133

Raspberry Pi France | Tutoriels pour Raspberry Pi et actualités. (2023, octobre 23). Raspberry Pi France. https ://www.raspberrypi-france.fr/

What are vertical farming systems ? Here's all you need to know. (s. d.). Consulté 13 décembre 2023, à l'adresse https ://ifarm.fi/blog/vertical-farming-systems