INTEGRATION AND INTEROPERABILITY OF CONNECTED OBJECTS OF E-HEALTH OBJECTS IOT

Abdelfetteh Lachtar

République Tunisienne
Ministère de l'Enseignement Supérieur, de la Recherche Scientifique

Université de Sfax
École Nationale d'Ingénieurs de Sfax

Ecole Doctorale
Sciences et Technologies

Thèse de *DOCTORAT*
Nom du Doctorat
N° d'ordre : 2019– 40nn

THESE

Présentée à

L'École Nationale d'Ingénieurs de Sfax

En vue de l'obtention du

DOCTORAT

Dans la discipline
Ingénierie des Systèmes Informatiques (ISI)

Par

Abdelfetteh LACHTAR

(Ingénieur informatique)

INTEGRATION ET INTEROPERABILITE DES OBJETS CONNECTES DE L'INTERNET DES OBJETS DE L'E-SANTE

Soutenu le 11 Juillet 2020, devant le jury composé de :

M.	**Mohamed ABID** (professeur ENIS)	Président
MM.	**Leila SAIDANE** (professeur ENSI)	Rapporteur
M.	**Mohamed Adel ALIMI** (professeur ENIS)	Rapporteur
M.	**Mounir SAMET** (professeur ENIS)	Examinateur
M.	**Abdennaceur KACHOURI** (professeur ENIS)	Directeur de Thèse
M	**Thierry VAL** (professeur IRIT-UT2J)	Co-Directeur de Thèse

INTEGRATION ET INTEROPERABILITE DES OBJETS CONNECTES DE L'INTERNET DES OBJETS DE L'E-SANTE

Abdelfetteh LACHTAR

الخلاصة: مع الزيادة الكبيرة في أنظمة M-Health وأنظمة المدن الذكية ، أثبتت الحاجة إلى استيعاب أجهزة الاستشعار والمحركات ، من أجل التشغيل الآلي الفعال ، أنها تشكل مطلبًا حاسمًا للاتصال من آلة إلى آلة (M2M). تتمثل العناصر الرئيسية لنظام M-Health الناجح في استهلاك الطاقة والحفاظ على قابلية التشغيل البيني. وفي هذا السياق ، يمكن إعداد العمل الحالي ، حيث يتم تنفيذ نظام مخصص للمسنين يرصد ويراقب باستخدام عصا المشي المتصلة. يتكون نظامنا من عقدة مرسل مرسلة على قصب والتي تنقل البيانات المتعلقة بالموقع وحالة كبار السن ، إلى محطة أساسية عبر تقنية LoRa ، ثم يستخدم الأخير بروتوكول نقل الرسائل في قائمة انتظار الرسائل (MQTT) للتفاعل مع البيئة عندما يحدث السقوط. تم إجراء العديد من التجارب لتقييم المنطقة التي تغطيها شبكة LoRa واستهلاك الطاقة لنظامنا. تشير النتائج إلى أن متوسط المساحة المغطاة هو حوالي 6 كم 2 وأن استهلاك الطاقة لنظامنا أقل بعشر مرات على الأقل من نظام النقل القائم على GPRS.

Résumé : Vu le développement rapide des systèmes E-santé et de la ville intelligente, la nécessité de prendre en charge les capteurs et les actionneurs, pour une automatisation efficace, s'avère être une exigence essentielle pour la maintenance de la communication machine à machine (M2M). Les éléments clés d'un système E-santé performant sont la consommation d'énergie et l'interopérabilité. C'est dans ce contexte que l'on pourrait définir notre thèse, un système dédié aux personnes âgées, agissant et surveillant à l'aide de leur canne connectée qui est mis en œuvre. Notre système consiste en un nœud émetteur positionné sur la canne qui transmet les données relatives aux déplacements et à l'état des personnes âgées à une station de base via la technologie LoRa. Cette dernière utilise ensuite le protocole MQTT (Message Queuing Telemetry Transport) pour interagir avec l'environnement quand une chute est survenue. Plusieurs expériences ont été menées pour évaluer la zone couverte par notre réseau LoRa et la consommation d'énergie de notre système. Les résultats indiquent que la superficie moyenne couverte est d'environ 6 km2 et que la consommation électrique de notre système est au moins dix fois inférieure à celle d'un système de transmission basé sur le GSM.

Abstract: With the increasing surge of M-Health and smart city systems, the need to accommodate sensors and actuators, for an effective automation to take place, proves to constitute a critical requirement for Machine-to-Machine (M2M) communication to be maintained. The key elements for a successful M-Health system are power consumption and maintaining interoperability .It is in this context that the present work could be set, whereby a system dedicated to the elderly tacking and monitoring using their connected walking stick is implemented. Our system consists of a transmitter node positioned on the cane that transmits data related to the position and the state of the elderly, to a base station via LoRa technology, then the latter uses Message Queuing Telemetry Transport (MQTT) protocol to interact with the environment when a fall has occurred. Several experiments have been conducted to evaluate the area covered by our LoRa network and the power consumption of our system. The results indicate that the average covered area is around 6 km2 and the power consumption of our system is at least ten times lower than for a GPRS-based transmission system.

المفاتيح: إنترنت الأشياء ، التشغيل المتداخل ، M- الصحة ، M2M، MQTT ، لورا

Mots clés: IoT, interopérabilité, E-santé, M2M, MQTT, LoRa

Key-words: IoT, Interoperability, M-Health, M2M, MQTT, LoRa

Remerciements

Ce travail de thèse a été développé dans l'équipe Microélectronique et Electronique Médicale (MEEM) dirigé par Monsieur le Professeur Mounir SAMET, au sein du Laboratoire d'Electronique et des technologies de l'Information (LETI) de l'Université de Sfax et au sein du l'Institut de Recherche en Informatique de Toulouse (IRIT), équipe IRT dirigé par Monsieur le Professeur Thierry Val.

Je tiens à exprimer tout d'abord ma profonde reconnaissance à mon directeur de thèse Monsieur Abdennaceur KACHOURI, Professeur à l'ENIS, qui a toujours su me guider avec un grand professionnalisme. Son expertise, sa rigueur scientifique et ses conseils pertinents m'ont permis d'avancer dans la bonne direction. Je le remercie également pour sa disponibilité tout au long de cette période. Ainsi que mon Co-directeur de thèse Monsieur Thierry VAL, professeur à l'IRIT rattaché à l'université de Toulouse 2 pour son aide efficace avec ses précieux conseils. Ses encouragements et sa bonne humeur contagieuse m'ont beaucoup aidée aux moments de doute.

Je tiens à exprimer ma gratitude et mes remerciements à Madame Leila SAIDANE, Professeur à l'ENSI, et à Monsieur Adel ALIMI Professeur à l'ENIS pour avoir accepté de rapporter mon travail.

Je souhaite exprimer mes remerciements les plus respectueux aux membres du Jury qui ont accepté d'évaluer mon travail de thèse.

Je tiens également à remercier le colonel-major Houssin GHARBI qui m'a donné la chance de soutenir cette thèse tout en offrant du confort et les moyens nécessaire pour avancer. Mes remercîments s'adresse aussi au colonel-major Bechir SALAH, colonel-major Abdelkarim TLILI, colonel Mohamed Amine BEN ABDALLAH et Colonel Sadok BELLILI pour leurs encouragement.

Je tiens à remercier toutes les personnes que j'ai pu côtoyer dans les laboratoires LETI et IRIT qui m'ont permis de réaliser ces travaux dans une ambiance très sympathique et motivante.

Dédicaces

A mon père Taher.

Aucune dédicace ne saurait exprimer l'amour, l'estime, le dévouement et le respect que j'ai toujours eu pour toi. Rien au monde ne vaut les efforts fournis pour mon éducation et mon bien être.
Ce travail est le fruit de tes sacrifices que tu as consentis pour mon éducation et ma formation.

A ma mère Noura.

Symbole de la bonté par excellence, la source de tendresse et l'exemple du dévouement qui n'a pas cessé de m'encourager et de prier pour moi.
Ta prière et ta bénédiction m'ont été d'un grand secours pour mener à bien mes études.
Aucune dédicace ne saurait être assez éloquente pour exprimer ce que tu mérites pour tous les sacrifices que tu n'as cessé de me donner.

A ma chère sœur Marwa.

En témoignage de l'attachement, de l'amour et de l'affection que je porte pour toi.
Tu es toujours dans mon cœur. Je te remercie pour ton aide sans égal et ton affection si sincère.
Je vous dédie ce travail avec tous mes vœux de bonheur, de santé et de réussite.

A ma chère sœur Maha

Ma chère petite sœur présente dans tous mes moments d'examens par son soutien moral et ses belles surprises sucrées.
Je te souhaite un avenir plein de joie, de bonheur, de réussite et de sérénité. Je t'exprime à travers ce travail mes sentiments de fraternité et d'amour.

A tous ceux qui m'aiment.

A tous ceux qui ne cessent de m'encourager.

A tous ceux qui ont confiance en moi.

Table des matières

Table des figures

Liste des tableaux

Glossaire

AMQP : Advanced Message Queuing Protocol

CCSA: Canadian Cable Systems Alliance

CDMA: Code Division Multiple Access

CERA: Code Expanded Random Access

CoAP : Constrained Application Protocol

COP: Contention Only Period

CR: Cognitive Radio

CSMA: Carrier Sense Multiple Access

CTS: Clear to Send

DBTMA: Dual Busy Tone Multiple Access

DSS : Data Distribution Service

EHPAD : Etablissement d'Hébergement pour Personnes Agées Dépendantes

ETSI: European Telecommunications Standards Institute

FDMA: Frequency Division Multiple Access

FI PPP: Future Internet Public Private Partnership

FPRP: Five Phase Reservation Protocol

GSM: Global System for Mobile Communications

GSMA: Global System Mobile Association

HTTP: Hypertext Transfer Protocol

H2H: Human to Human

IEEE: Institute of Electrical and Electronics Engineers

IETF: Internet Engineering Task Force

IOT : Internet Of Things

IPv6 : Internet Protocol version 6

LTE: Long Term Evolution

LTE-A: Long Term Evolution Advanced

MAC : Medium Access Control

MACA: Multiple Access with Collision Avoidance

MQTT: Message Queuing Telemetry Transport

MTC: Machine Type Communication

M2M: Machine to Machine

NAMA: Node Activation Multiple Access

NP: Notification Period

OMA: Open Mobile Alliance

OMG : Object Management Group

OPEX: operational expenditure

PAN : Prsonal Area Network

PCF: Point Coordination Function

PRACH: Physical Random Access Channel

QOS : Quality Of Service

RACH: Dynamic Random Access Channel

RB: Resource Blocks

RFG : Request For Gateway

RFID: Radio Frequency Identification

ROLL: Routing Over Low-Power and Lossy

RTS: Request to Send

SCADA: Supervisory Control And Data Acquisition

SDO : Standard Development organization

SMQTT : Secure MQTT

TDMA: Time Division Multiple Access

TIA: Telecommunications Industry Association

TISPAN: Telecoms & Internet Converged Services & Protocols for Advanced Networks

TOP: Transmission Only Period

UICC: Universal Integrated Circuit Card

WFA: World Fellowship Activities

WGSN: WLAN-Based GPRS Environment Support Node

WSAN: Wireless Sensors and Actuators Networks

WSN: Wireless Sensors Network

xSDL: XML Schema Definition Language

XMPP: Extensible Messaging and Presence Protocol

3GPP : 3rd Generation Partnership Project

6LowPAN : IPv6 Low power Wireless Personal Area Networks

Introduction générale

Selon l'Organisation Mondiale de la Santé [1], entre 28 et 35% des personnes âgées de 65 ans et plus tombent chaque année et ces valeurs augmentent de 32 à 42% pour les personnes de plus de 70 ans. En fait, les chutes augmentent de façon exponentielle avec les changements biologiques liés à l'âge, ce qui entraîne une forte incidence de chutes et de blessures liées aux chutes dans les sociétés vieillissantes. Si aucune mesure préventive n'est prise dans les meilleurs délais, le nombre de blessures causées par des chutes sera 100% plus élevé en 2030. Par conséquent, les aides à la mobilité et l'assistance personnelle sont fortement souhaitées pour assurer un certain degré d'indépendance. Les dispositifs d'assistance possibles incluent les cannes qui ont un grand nombre de personnes âgées en raison de leur simplicité et de l'aide à la marche qu'elles fournissent.

L'Internet des objets [2], avec ses avancées technologiques, pourrait être le moyen d'assurer de meilleures conditions de vie aux personnes âgées et de surveiller leur santé par le développement d'environnements intelligents innovants [3]. Ces technologies peuvent également offrir plus de sécurité aux personnes âgées en fournissant des mécanismes d'intervention d'urgence [4], des solutions de détection des chutes [5] et des systèmes de surveillance vidéo [6]. En outre, ils apportent un soutien dans la vie quotidienne, surveillent les activités de la vie quotidienne, produisent des rappels [7], permettant aux personnes âgées de communiquer avec leur famille et le personnel médical. L'un des éléments critiques d'un système de surveillance active pour les personnes âgées est la consommation d'énergie et l'interopérabilité.

L'universitaire et l'industrie ont mis l'accent sur l'importance du défi de l'interopérabilité dans l'Internet des objets. L'industrie tente de résoudre les problèmes d'interopérabilité IoT par la normalisation [8]. Plusieurs efforts ont été déployés pour établir des normes d'interopérabilité entre les appareils, les réseaux, les services et les formats de données IoT appartenant à différents fournisseurs. L'Union européenne a également récemment financé plusieurs projets de recherche dans le cadre du programme H2020, axés sur la fédération de plates-formes IoT. Cependant, il faudra peut-être beaucoup de temps avant que les normes correspondantes soient entièrement approuvées et acceptées. Pour résoudre ce problème, des

chercheurs du monde universitaire et de l'industrie ont élaboré une liste de solutions novatrices d'interopérabilité et d'hétérogénéité dans différents systèmes IoT.

La différence essentielle entre "Internet" et "Internet des objets (IoT)" [9] réside dans le fait que, dans l'IoT, "un peu moins de tout" est disponible sur un périphérique ou un périphérique réseau : moins de mémoire, moins de puissance de traitement, moins de bande passante, etc. bien sûr, moins d'énergie disponible. Cela est dû au fait que les objets sont alimentés par batterie et que maximiser leur durée de vie est une priorité, ou parce que leur nombre est énorme (on estime qu'il y aura 50 milliards d'appareils connectés d'ici 2020 [10]). Cette volonté de "faire plus avec moins" conduit à des contraintes qui limitent l'applicabilité des réseaux cellulaires traditionnels, ainsi que des technologies, telles que le WiFi, en raison des demandes d'énergie et d'évolutivité. LoRa cible les déploiements où les périphériques finaux ont une puissance limitée (par exemple, une alimentation par batterie), où les périphériques finaux ne doivent pas transmettre plus de quelques octets à la fois [11] et où le terminal peut initier un trafic de données (par exemple lorsque le terminal est un capteur) ou une entité externe souhaitant communiquer avec le terminal (par exemple lorsque le terminal est un actionneur). La nature longue portée et faible consommation de LoRa faisant de cette dernière un candidat attrayant pour la technologie de détection intelligente dans les infrastructures civiles (telles que la surveillance de la santé, la mesure intelligente, la surveillance de l'environnement, etc.) uniquement dans les applications industrielles.

La communication de machine à machine (M2M) représente un potentiel IoT prometteur où des milliards d'objets du quotidien et des environnements environnants deviennent interconnectés et gérés à l'aide de toute une gamme d'appareils, de réseaux de communication et de serveurs basés sur le Cloud [12]. À cet égard, la communication M2M, également appelée communication de type machine (MTC), semble être en mesure de maintenir l'échange d'informations entre machines et des machines sans aucune interaction humaine ni interférence. Il s'avère être applicable dans de nombreux domaines des applications IoT [13], y compris les soins de santé, l'automatisation industrielle et agricole, les systèmes de transport et les réseaux électriques. MQTT est un protocole de connectivité machine à machine (M2M) pour IoT, conçu comme un protocole de messagerie publication / abonnement basé sur le protocole TCP / IP extrêmement léger. La messagerie pub-sub est une forme de communication centrée sur les données, largement utilisée dans les réseaux d'entreprise, principalement en raison de son évolutivité et de sa prise en charge des topologies d'applications dynamiques. L'adoption du paradigme pub/sub dans les réseaux de capteurs permet de simplifier leur intégration avec d'autres applications distribuées. L'approche de

communication centrée sur les données est basée sur le contenu des données plutôt que sur les adresses des destinataires et semble plus efficace et appropriée pour les réseaux de capteurs sans fil (WSN) [14]. MQTT a été conçu comme un middleware de communication approprié pour dissimuler la complexité des protocoles réseau de bas niveau et pour faciliter le développement et l'interopérabilité des applications [15].

En outre, la "nature autonome des machines" dans les communications M2M crée des problèmes de communication potentiels, par exemple dans cette technologie, des milliards de périphériques communiquent pour un certain nombre d'opérations, entraînant une congestion et une surcharge dans les réseaux et générant différents types de trafic de données. Certains des défis importants dans les communications M2M comprennent l'efficacité énergétique [16], la fiabilité, la sécurité, l'ultra-évolutivité, l'hétérogénéité [17] et la qualité de service (QoS).

Dans un premier temps, nous considérons les problèmes de la couche MAC liés aux communications M2M. La couche MAC est principalement responsable de l'accès au canal pour des nœuds dans un réseau qui utilise un support partagé. La contribution apportée est la conception d'un protocole MAC hybride, qui consiste en une période de contention et une période de transmission, il est conçu pour des réseaux M2M hétérogènes. Dans ce protocole, les différents dispositifs avec des priorités prédéfinies (probabilités hiérarchiques concurrentes) Contestent d'abord les opportunités de transmission suite au mécanisme d'accès multiple (CSMA). Seuls les périphériques réussis seront affectés un intervalle de temps pour la transmission suite au mécanisme basé sur la réservation (TDMA).

Puis, nous nous intéressant au système de surveillance de la personne âgée utilisant sa canne de marche spécialement conçu pour aider à transmettre des données relatives à l'état des personnes âgées (suivi GPS, détection des chutes, nombre de pas) à la station de base BS via la technologie LoRa (longue distance, faible consommation). La BS représente une passerelle M2M, car elle permet la communication via MQTT avec un autre objet connecté dans un environnement de ville intelligente. La deuxième contribution est la mise en œuvre d'un nouveau système d'E-santé en utilisant une canne de marche connectée. Ainsi, La troisième contribution de ce travail est le maintien de l'interopérabilité efficace entre la canne et d'autres objets connectés, dans un environnement de ville intelligente, via MQTT.

En plus de cette introduction, ce manuscrit est organisé en trois chapitres et une conclusion générale.

Dans le chapitre 1 nous donnons une définition générale de l'internet des objets ainsi que son architecture et ses applications. Nous évoquons ensuite la notion des communications M2M

en présentant ses caractéristiques et ses standards. Puis, nous abordons les principales approches du terme interopérabilité.

Dans le chapitre 2, après avoir évoqué les inconvénients des protocoles MAC étudiés pour un contexte des réseaux M2M, nous avons proposé un protocole MAC hybride CSMA/TDMA qui combine les avantages des protocoles MAC à base de contention et les protocoles MAC sans contention. Nous avons présenté son fonctionnement avec une période de contention et une période de transmission. Les relations entre les différents paramètres sont également dérivées. De plus, nous avons présenté un exemple précis de son fonctionnement. Finalement, un problème d'optimisation est formulé pour déterminer les paramètres de contention optimaux afin de maximiser le débit globale.

Dans le chapitre 3, nous présentons le système de surveillance de la personne âgée utilisant leur canne de marche spécialement conçu pour aider à transmettre des données relatives à l'état des personnes âgées (suivi GPS, détection des chutes, nombre de pas) à la station de base via la technologie LoRa (longue distance, faible consommation). De plus nous présentons les performances de notre système en termes de communication et de faisabilité.

Finalement, dans la conclusion générale, nous résumons nos travaux effectués et les résultats obtenus tout en abordant des perspectives pour des travaux futurs.

Chapitre 1 : Internet des objets et interopérabilité entre les objets connectés

1.1. Introduction

Le nombre d'appareils intégrés dans les réseaux M2M n'a cessé d'augmenter ces dernières années. Traditionnellement, de tels dispositifs ont travaillé localement de façon indépendante et ont fourni des services aux utilisateurs. Le progrès dans les technologies de communication radio ont permis même la connectivité mobile pour les appareils connectés sur internet. Ces tendances sont maintenant visibles par le nombre croissant d'application qui dépendent des services exposés à partir d'équipements physiques, tels que des capteurs, des actionneurs, des étiquettes RFID, des machines, des véhicules et des dispositifs industriels embarqués. De tels systèmes de service sont appelés services Machine to Machine, qui peuvent également être appelés Internet des objets ou bien Cyber-Physical Systems [18]. Souvent, ces systèmes incluent des capacités pour les mesures à distance et le contrôle à distance des dispositifs embarqués. Les mesures à distance consistent à détecter des phénomènes physiques, à stocker, à envoyer, à recevoir et à traiter des informations mesurées. Le contrôle à distance des appareils comprend le contrôle d'accès, l'exclusion mutuelle, l'envoi, la réception et le traitement des commandes de contrôle. Le facteur de base de ces fonctionnalités est la connectivité M2M, où différents types d'appareils intégrés sont connectés à Internet. La valeur ajoutée est créée par les services M2M activés qui sont basés sur l'utilisation intelligente des informations mesurées, ainsi que sur le raisonnement et l'exécution des actions de contrôle à distance avec les équipements M2M.

Dans ce chapitre d'état de l'art, nous présentons les termes IOT et M2M, puis nous évoquons les différents protocoles MAC sans fils. Nous introduisons aussi l'interopérabilité dans l'IoT et ces facteurs qui font l'objet d'étude de cette thèse.

1.2. Internet des objets

L'Internet des objets est l'Internet du futur, elle représente une révolution de l'informatique et de la communication. Elle constitue un monde d'objets en réseaux, où tous est interconnecté et possède une représentation virtuelle [19]. Les objets du quotidien se transforment en objets intelligents capables de détecter, interpréter et réagir à l'environnement grâce à la combinaison de l'internet et des technologies émergentes telles que l'identification par radiofréquence, localisation en temps réel et les capteurs embarqués [20].

1.2.1. Architecture de l'IOT

La figure 1.1 montre une architecture de haut niveau des systèmes IOT, qui est composée de trois domaines [21] : le domaine de périphérique M2M, le domaine de réseau et le domaine d'application.

Dans le domaine des périphériques, le périphérique fournit une connectivité directe au domaine réseau via des réseaux d'accès, qui peuvent inclure des technologies PAN à portée limitée telles que Bluetooth, ZigBee, etc. ou via une passerelle qui agit comme un proxy réseau pour le domaine réseau.

Une telle passerelle doit être suffisamment flexible pour gérer efficacement les ressources disponibles [22], la QoS, la sécurité, ainsi que l'échange des données multimédia. Ces concepts de passerelle sont répandus dans les modèles ADSL domestiques et les points d'accès WiFi trouvés dans les cybercafés et les points d'accès sans fil. Comme les systèmes IOT intègrent des objets intelligents hétérogènes, la conception de la passerelle est assez différente car elle ne doit pas obliger chaque sous-réseau IOT à avoir sa propre passerelle. Ainsi, une architecture convergente vers une solution unique intégrant le trafic entrant des dispositifs intelligents hétérogènes devrait être conçue. De plus, comme les objets intelligents sont limités en ressources et en énergie, la passerelle doit être consciente du contexte de chaque processus géré. Elle devrait également utiliser des protocoles de routage intelligents et des techniques de mise en cache pour acheminer le trafic sur les chemins les moins contraints.

Le domaine de réseau [23] comprend différents réseaux d'accès, qui fournissent une connectivité à travers diverses technologies, telles que xSDL, Satellite, etc. vers des dispositifs et / ou des passerelles. Ils fournissent également une connectivité au réseau central qui inclut une connectivité hétérogène et multi-technologies, telle que 3GPP, TISPAN et LTE-A. Enfin, le domaine d'application inclut les applications IOT et les infrastructures serveur / cloud. Ces derniers doivent partager leurs contenus, éventuellement les sauvegarder sur d'autres appareils, programmes d'analyse et / ou personnes qui ont besoin de surveiller la réponse en temps réel. Ils incluent également des fonctionnalités de service, qui fournissent des fonctions partagées entre différentes applications via des abstractions de haut niveau ouvertes et des interfaces qui masquent les spécificités des réseaux sous-jacents.

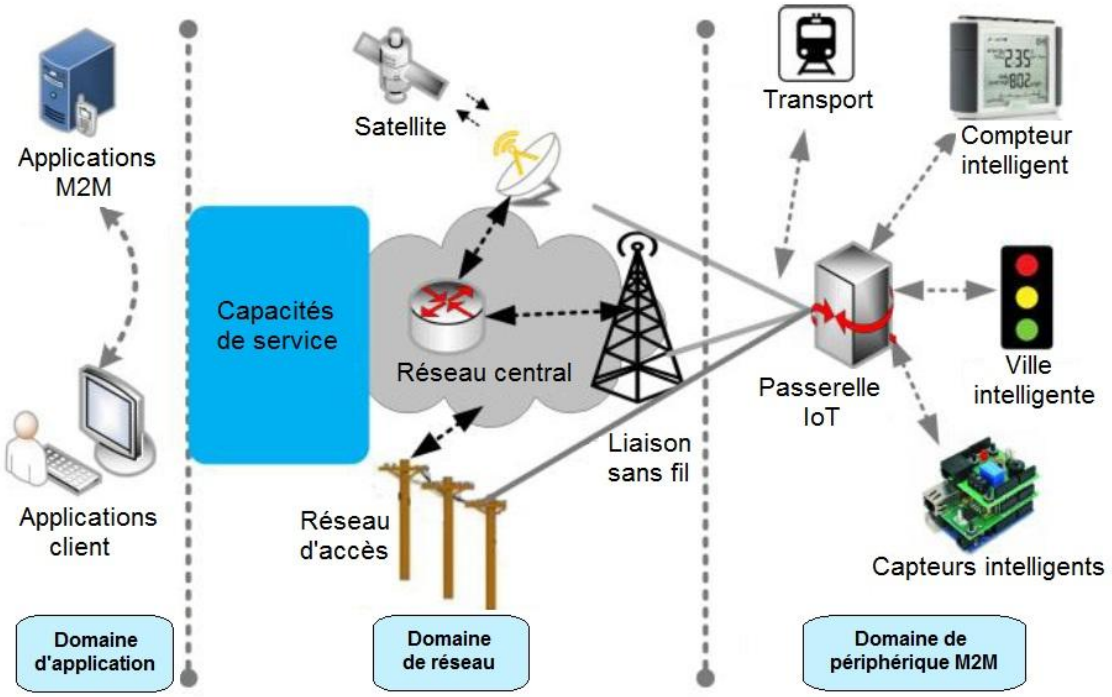


Figure 1.1 *Architecture globale de l'IOT [21]*

1.2.2. Les capteurs et les actionneurs

Les capteurs sont des petits appareils disposant de capacités de mesures, voire d'actions, sur leur environnement. La température, le taux d'humidité, la luminosité ambiante, la détection de présences ou de mouvements via un accéléromètre, présence de gaz, de polluants ou encore la géolocalisation font partie des informations les plus couramment collectées sur ce type de matériel. Selon les capteurs, ou grâce à l'ajout de cartes additionnelles, la pression atmosphérique, le niveau de radiation ou la pression acoustique (événements sonores) peuvent aussi être quantifiés. Les spécificités innovantes de ces capteurs résident dans leur taille et leur coût réduit, tout en étant dotés des capacités de traitements de l'information, et des possibilités de transmission sans fil. [24][25]

La nature de l'objet "intelligent" a de particulier qu'il dispose de possibilités de calcul et de transmission des données. L'échange d'informations, voire l'interaction entre différents objets est envisageable, et ce même sans intervention des utilisateurs. L'objet va "capter", mesurer une caractéristique physique de son environnement, éventuellement lui appliquer un traitement informatisé, et fournir le résultat aux autres (utilisateur, ordinateur, etc.).

Si les capteurs disposent d'éléments pour évaluer une caractéristique physique de leur environnement, certains d'entre eux peuvent également agir sur cet environnement : on parle alors d'actionneurs [26] (I. Akyikdiz les appelle ici "actors"). Ces effecteurs sont souvent plus puissants en termes de capacités mémoires, de traitement, voire en réserve d'énergie. Ils sont aussi moins

nombreux que les capteurs, car pour des raisons pratiques, il est cohérent de disposer d'un grand nombre de points de mesures tandis qu'il vaut mieux restreindre le nombre de points d'actions, et éviter les ordres et contre-ordres incohérents. Toutefois, cette approche tend à être modifiée par l'évolution des WSAN lorsque ceux-ci s'intègrent dans l'Internet des objets [27]. Dans ce cadre, leur usage diffère [28] pour s'orienter vers le service, et la multiplicité des capteurs s'amenuise (dans une vision domotique, on n'utilisera qu'un nombre réduit de capteurs de température, un capteur par pièce par exemple).

1.2.3. Le réseau des capteurs sans fil

Afin de satisfaire les besoins de communication entre eux, les capteurs sont équipés de dispositifs sans fil pour l'émission et la réception de données. Cela ne suffit cependant pas pour rendre un ensemble de capteurs accessibles, ou au moins interopérables. Pour cela, les capteurs doivent aussi s'organiser. Ce qui caractérise un réseau de capteurs, c'est que ses éléments sont des appareils très petits, dotés de capacités de transmission sans fil, autonomes en énergie et dont le positionnement est, le plus souvent, libre (dans le sens où il n'est pas toujours contrôlé, anticipé, volontaire, parfois confié au hasard, par dispersion, par exemple) [29]. La figure 1.2 illustre un réseau de capteurs.

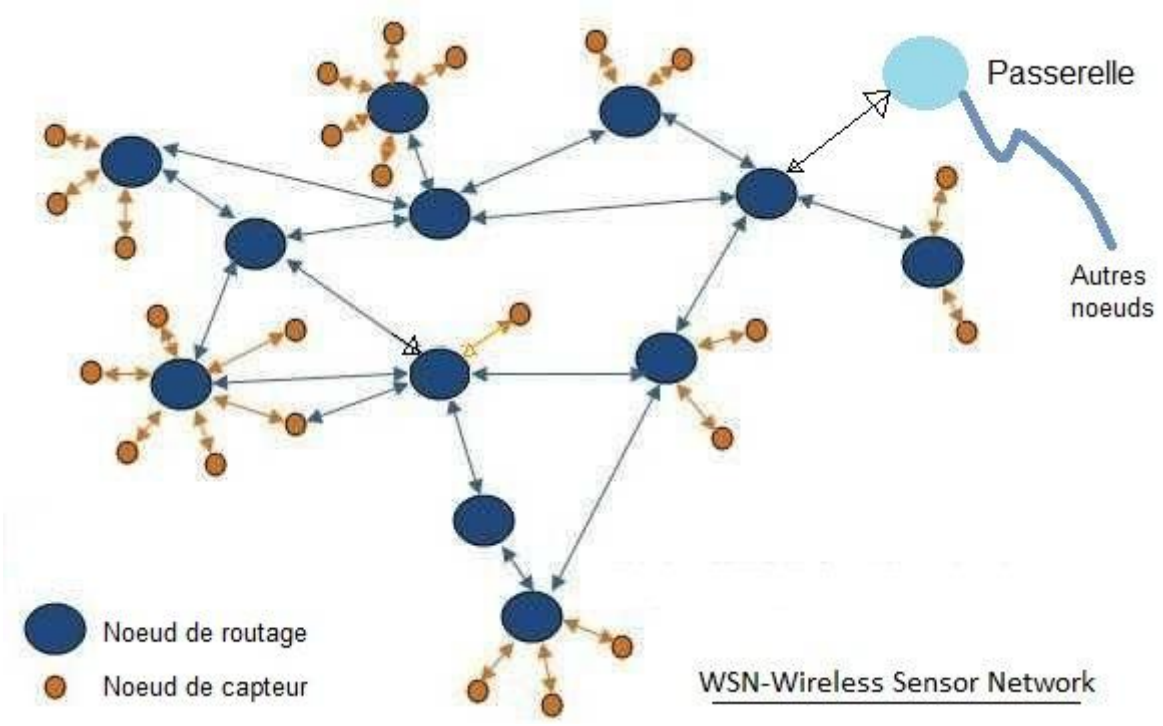


Figure 1.2 *Réseau de capteurs*

1.2.4. RFID

Le terme RFID englobe toutes les technologies qui utilisent les ondes radio pour identifier automatiquement des objets ou des personnes [29].
Le système RFID est une technologie qui permet de mémoriser et de récupérer des informations à distance grâce à une étiquette qui émet des ondes radio.
Le système RFID fonctionne de la manière suivante :

- L'étiquette RFID (transpondeur ou tag) est elle-même équipée d'une puce reliée à une antenne, l'antenne permet à la puce de transmettre les informations (numéro de série, poids...) qui peuvent être lues grâce à un lecteur émetteur-récepteur.
- Une fois les informations transmises au lecteur RFID équipée d'une antenne intégrée ou externe, celui-ci n'a plus qu'à convertir les ondes-radios en données et celles-ci peuvent être lues par un logiciel RFID.

1.2.5. Les applications de l'IoT

À l'heure actuelle, l'IoT est devenu l'une des technologies d'avenir les plus attrayantes pouvant être utilisées à différentes fins [33]. Par exemple, de nos jours, presque tous les appareils électroniques embarqués ont besoin de capteurs et d'opérateurs pour faire fonctionner ces appareils. Ces capteurs peuvent bénéficier de la connectivité IoT et peuvent être gérés plus efficacement. L'IoT est désormais en mesure de connecter la plupart des appareils de l'industrie et est devenu un réseau mondial pour les appareils et les machines et la communication machine à machine (M2M) et appareil à appareil (D2D) dans une industrie. Non seulement dans les cas industriels, mais aussi dans d'autres cas, par exemple, l'IoT peut également être utilisé pour garder une trace des appareils électroniques domestiques. Afin d'économiser de l'argent et de l'énergie, les appareils électroniques dans chaque maison, par exemple le réfrigérateur, la lumière, le ventilateur et le refroidisseur d'air peuvent être surveillés à l'aide de l'IoT. De la même manière, l'IoT joue désormais un rôle important dans le dispositif portable intelligent, la ville intelligente, le réseau intelligent, le système de santé intelligent, l'agriculture intelligente et le service de logistique intelligent. Par exemple, un capteur de température intelligent IoT peut être utilisé pour suivre la température du conteneur de fret, ce qui aide l'utilisateur à prendre des mesures en temps réel pour maintenir les marchandises en bon état. Pour hiérarchiser les cas d'utilisation de l'IoT, il peut être classé en deux groupes comme suit: l'IoT massif et l'IoT critique [34]. Les cas d'utilisation les plus courants de ces deux cas sont présentés dans le tableau 1.1 suivant.

Tableau 1.1 *Les groupes des applications IoT*

IoT massif	IoT critique
Bâtiment intelligent	Contrôle du trafic
Agriculture intelligente	Soins de santé à distance
Suivi logistique	Smart grid
Agriculture intelligente	Industrie intelligente
Comptage intelligent	Fabrication à distance
Réseaux capillaires	Chirurgie à distance

En outre, l'IoT peut être qualifié de réseau intelligent et son application inclut également la nécessité d'un traitement intelligent des données des capteurs ou des appareils. Le serveur d'applications IoT a filtré les données inutiles et ne stocke que les données précieuses.

- **Les villes intelligentes**

En 2020, nous allons voir le développement des routes et des couloirs des grandes villes, et plus de 60 % de la population mondiale pourrait vivre dans les centres urbains en 2025.

L'urbanisation comme une tendance aura des impacts et influences sur les futures vies personnelles.

En 2023, il y aura 30 grandes villes à l'échelle mondiale, avec 55% de développement de l'économie en Inde, la Chine, la Russie et l'Amérique latine [32]. Cela conduira à l'évolution des villes intelligentes avec huit fonctions intelligentes, y compris économie intelligente, Bâtiments intelligents, mobilité intelligente, énergie intelligente, communication intelligente, planification intelligente, citoyens et gouvernance intelligente. Il y aura environ 40 villes intelligentes à l'échelle mondiale d'ici 2025.

Le rôle des gouvernements des villes sera essentiel pour le déploiement de l'IOT. L'exécution des opérations et la création des stratégies de développement de la ville tous les jours conduira à l'utilisation de l'IOT. Par conséquent, les villes et leurs services représentent une plate-forme presque idéale pour la recherche dans le domaine de l'IOT.

De même, le projet OUTSMART [33], se concentre sur les services publics et les services de l'environnement dans les villes et adresse le rôle de l'IOT dans la gestion de l'eau, l'éclairage public et des systèmes de transport intelligent ainsi que la surveillance de l'environnement.

Une vision de la ville intelligente comme «domaine horizontal» est proposé par le projet de BUTLER [34], dans laquelle de nombreux scénarios verticaux sont intégrés et s'accordent pour permettre la notion de vie intelligente.

Dans ce contexte, il y a de nombreux défis de recherche importants pour l'application de la ville intelligente :

- L’intégration des objets à large échelle.
- Protocoles et algorithmes pour une basse consommation d’énergie.
- Algorithmes pour l’analyse, le traitement et la compréhension des données acquises dans la ville.
- Création des algorithmes et des schémas pour décrire l'information fournit par les capteurs dans différentes applications pour permettre l'échange d'informations utiles entre les différents services de la ville

- **Soins de santé à distance**

Les La notion d’E-santé, désignée également par E-health, télésanté ou cyber santé, est utilisée pour la première fois en 1999 par Jhon Mitchelle [35]. La définition la plus connue et la plus utilisée est celle proposée par Eysenbach [36] : « E-health est un domaine émergeant créé par l'intersection entre les domaines de l'informatique médicale, la santé publique et le secteur privé. Ce domaine fait référence au service de santé et les informations en matière de santé à travers Internet ou d'autres technologies connexes..."

L'intégration des nouvelles technologies dans le domaine de la santé publique est la clé qui a permis d'ouvrir une nouvelle époque d'évolution au niveau matériel afin de fournir une multitude d'informations qui n'étaient pas disponibles par le passé. Cette évolution est à l'origine de l'amélioration de la qualité des données fournies aux équipes médicales pour les aider à prendre des décisions qui seront de plus en plus précises et concrètes dans le futur. L'émergence des technologies médicales, telles que les technologies de suivi et de contrôle, dans le monde entier, a permis à de nouvelles applications d'être installées et utilisées dans de nombreux environnements. L'exploitation de cette technologie dans les domiciles et les résidences représente une bonne solution pour le bien-être des personnes âgées puisque les garder dans le même environnement assure la stabilité psychologique et en même temps un suivi meilleur tout en gardant les services offerts par les centres médicaux et les hôpitaux. La détection des situations anormales se fait d'une manière instantanée et l'intervention humaine s'exécute seulement en cas de besoin. Différentes applications sont proposées dans ce cadre et peuvent ^etre réparties en trois classes [37]:

_ Soins à domicile,

_ Soins à la résidence spécialisée,

_ Soins intensifs.

Afin d'assurer l'équilibre entre la qualité de vie et le cout des soins, un compromis entre les deux doit être trouvé. Pour augmenter la qualité de vie, il faut conserver les conditions d'une vie ordinaire (chez soi) et exécuter le contrôle d'une manière non intrusive sans que cela ne soit trop couteux.

Cependant, pour augmenter la qualité des soins, il faut disposer d'une équipe médicale spécialiste qui veille sur la santé de la personne âgée, ce qui est onéreux.
L'amélioration du concept de soin est passée par plusieurs étapes ou les inventions technologiques représentent un catalyseur très important (Smartphone, capteurs. . .) permettant la détection et le transfert d'information. Il devient alors nécessaire de mettre en évidence le problème de la différenciation des services relatifs _a ces informations.
Le nombre de WPAN (Wireless Personal Area Networks) et WLAN (Wireless Local Area Networks) utilisés dans les hôpitaux, maisons de retraite ou _a domicile est en constante augmentation. La qualité et l'importance des données collectées demandent un certain niveau d'assurance en terme de fiabilité du réseau : l'information doit arriver au récepteur ou au point de collecte d'information de façon certaine, avec une latence maitrisée et en temps réels avec différents niveaux de priorité.
Les services e-santé doivent être totalement fiables et efficaces. Les technologies utilisées dans l'e-santé doivent soutenir différents niveaux de qualité de services (QoS). Plusieurs travaux de recherche académiques et industriels ont été initiés afin de créer une nouvelle solution technologique qui puisse satisfaire les exigences des applications e-santé en matière de bande passante, fiabilité et faible latence.

1.3. Protocoles et normes de mise en réseau pour l'Internet des objets

Cette partie traite des différentes normes proposées par l'IEEE, l'IETF et l'UIT pour permettre des technologies correspondant à la croissance rapide de l'IoT. Ces normes incluent les couches de communication, de routage, de réseau et de session de la pile réseau qui sont développées uniquement pour répondre aux exigences de l'IoT.
Les technologies de l'IoT permettent aux objets ou aux appareils qui ne sont pas des ordinateurs d'agir intelligemment et de prendre des décisions collaboratives bénéfiques pour certaines applications [41]. Ils permettent aux choses d'entendre, de voir, de penser ou d'agir en leur permettant de communiquer et de se coordonner avec les autres afin de prendre des décisions qui peuvent être aussi importantes que sauver des vies ou des bâtiments. Ils transforment les «choses» de l'informatique passive et de la prise de décisions individuelles en communications et collaborations actives et omniprésentes pour prendre une seule décision critique. Les technologies sous-jacentes de l'informatique omniprésente, des capteurs intégrés, de la communication lumineuse et des protocoles Internet permettent à l'IoT de fournir ses éléments significatifs, mais ils imposent de nombreux défis et introduisent le besoin de normes et de protocoles de communication spécialisés.

1.3.1. Écosystème de l'IoT

La figure 1.3 montre un modèle à 7 couches de l'écosystème IoT [39]. À la couche inférieure se trouve le domaine d'application, qui peut être un réseau intelligent, une maison connectée ou une santé intelligente, etc. La deuxième couche se compose de capteurs qui permettent l'application. Des exemples de tels capteurs sont les capteurs de température, les capteurs d'humidité, les compteurs électriques ou les caméras. La troisième couche est constituée d'une couche d'interconnexion qui permet aux données générées par les capteurs d'être communiquées, généralement à une installation informatique, un centre de données ou un cloud. Là, les données sont agrégées avec d'autres ensembles de données connus tels que des données géographiques, des données démographiques ou des données économiques. Les données combinées sont ensuite analysées à l'aide de techniques d'apprentissage automatique et d'exploration de données. Pour activer ces applications distribuées de grande envergure, nous avons également besoin des logiciels de collaboration et de communication de niveau application les plus récents, tels que les réseaux définis par logiciel (SDN), l'architecture orientée services (SOA), etc. Enfin, la couche supérieure se compose de services qui permettent au marché et peuvent inclure la gestion de l'énergie, la gestion de la santé, l'éducation, le transport, etc. En plus de ces 7 couches qui sont construites les unes sur les autres, des applications de sécurité et de gestion sont requises pour chacune des couches et sont donc affichées sur le côté.

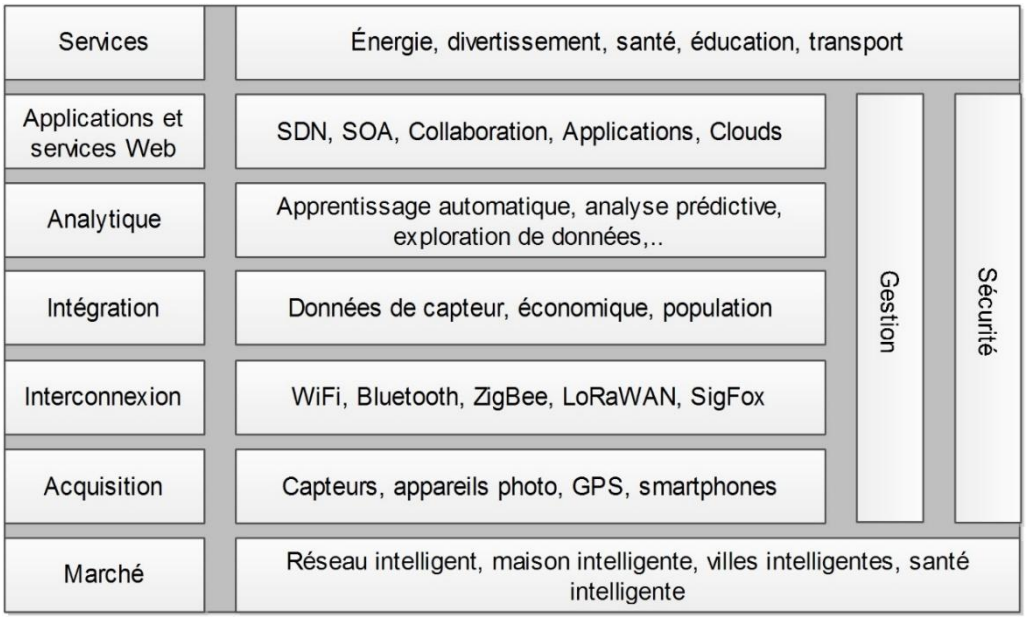


Figure 1.3 *Modèle de l'écosystème IoT [40]*

Dans cette thèse, nous nous concentrons sur la couche d'interconnexion. Cette couche elle-même peut être affichée dans une pile multicouche comme le montre la figure 1.3. Nous avons montré uniquement les couches liaison de données, réseau et transport / session. La couche de liaison de

données connecte deux éléments IoT qui peuvent généralement être deux capteurs ou le capteur et le périphérique passerelle qui connecte un ensemble de capteurs à Internet.

Il est souvent nécessaire de disposer de plusieurs capteurs pour communiquer et agréger les informations avant d'accéder à Internet. Des protocoles spécialisés ont été conçus pour le routage entre les capteurs et font partie de la couche de routage. Les protocoles de couche session permettent la messagerie entre divers éléments du sous-système de communication IoT. Un certain nombre de protocoles de sécurité et de gestion ont également été développés pour l'IoT, comme le montre la figure 1.4.

<table>
<tr><td colspan="2">Session</td><td>MQTT, SMQTT, CoRE, DSS, AMQP, XMPP, CoAp, …</td><td>Sécurité</td><td>Gestion</td></tr>
<tr><td rowspan="2">Réseau</td><td>Encapsulation</td><td>6LowPAN, 6TiSCH, 6Lo, Thread, …</td><td rowspan="3">TCG, Oath 2.0, SMACK, SASL, ISASecure, ace, DTLS, Dice, …</td><td rowspan="3">IEEE 1905, IEEE 1451</td></tr>
<tr><td>Acheminement</td><td>RPL, CORPL, CARP, …</td></tr>
<tr><td colspan="2">Liaison de données</td><td>WiFi, BLE, Z-Wave, Zigbee, DECT/ULE, 3G/LTE, NFC, HomePlug GP, 802.11ah, LoRaWAN, SigFox</td></tr>
</table>

Figure 1.4 *Couche d'interconnexion de l'IoT*

1.3.2. Protocoles de liaisons de données

Dans cette section, nous discutons des normes de protocole de la couche liaison de données. La discussion comprend les protocoles de couche physique (PHY) et MAC qui sont combinés par la plupart des normes.

- **IEEE 802.15.4**

IEEE 802.15.4 est la norme IoT la plus utilisée pour MAC [38]. Il définit un format de trame, des en-têtes, y compris les adresses source et de destination, et comment les nœuds peuvent communiquer entre eux. Les formats de trame utilisés dans les réseaux traditionnels ne conviennent pas à la mise en réseau multi-sauts de faible puissance dans l'IoT en raison de leur surcharge. En 2008, IEEE802.15.4e a été créé pour étendre IEEE802.15.4 et prendre en charge les communications à faible consommation. Il utilise la synchronisation de l'heure et le saut de canal pour permettre une haute fiabilité, un faible coût et répondre aux exigences de communication IoT. Ses fonctionnalités MAC spécifiques peuvent être résumées comme suit :

- **IEEE 802.11 ah**

EEE 802.11ah est une version légère (à faible énergie) de la norme d'accès sans fil IEEE 802.11 d'origine. Il a été conçu avec moins de frais généraux pour répondre aux exigences de l'IoT. Les normes IEEE 802.11 (également appelées Wi-Fi) sont les normes sans fil les plus couramment utilisées. Ils ont été largement utilisés et adoptés pour tous les appareils numériques, y compris les ordinateurs portables, mobiles, tablettes et téléviseurs numériques. Cependant, les normes WiFi d'origine ne conviennent pas aux applications IoT en raison de leur surcharge de trame et de leur consommation d'énergie. Par conséquent, le groupe de travail IEEE 802.11 a lancé un groupe de travail 802.11ah pour développer une norme qui prend en charge les communications à faible surcharge et à faible consommation d'énergie adaptées aux capteurs et aux moteurs [38].

- **Bluetooth basse énergie BLE**

Bluetooth basse énergie ou Bluetooth intelligent est un protocole de communication à courte portée avec les couches PHY et MAC largement utilisé dans les réseaux embarqués. Sa faible énergie peut atteindre dix fois moins que le Bluetooth classique tandis que sa latence peut atteindre 15 fois. Son contrôle d'accès utilise un MAC sans conflit avec une faible latence et une transmission rapide. Il suit l'architecture maître / esclave et propose deux types de trames : la publicité et les trames de données. La trame publicitaire est utilisée pour la découverte et est envoyée par des esclaves sur un ou plusieurs canaux publicitaires dédiés. Les nœuds maîtres détectent les canaux de publicité pour trouver des esclaves et les connecter. Après la connexion, le maître indique à l'esclave son cycle de réveil et sa séquence de planification. Les nœuds ne sont généralement éveillés que lorsqu'ils communiquent sinon ils vont dormir pour économiser leurs énergies [39][40].

- **Zigbee**

ZigBee est conçue pour une large gamme d'applications IoT, y compris les maisons intelligentes, les télécommandes et les systèmes de santé. Elle prend en charge une large gamme de topologies de réseau, notamment en étoile, point à point ou en cluster. Un coordinateur contrôle le réseau et est le nœud central dans une topologie en étoile, la racine dans une topologie d'arbre ou de cluster et peut être situé n'importe où en peer-to-peer. La norme ZigBee définit deux profils de pile : ZigBee et ZigBee Pro. Ces profils de pile prennent en charge un réseau maillé complet et fonctionnent avec différentes applications permettant des implémentations avec une faible mémoire et une faible puissance de traitement. ZigBee Pro offre plus de fonctionnalités, notamment la sécurité à l'aide de l'échange de clés symétriques, l'évolutivité à l'aide de l'attribution d'adresses stochastiques et de meilleures performances à l'aide de mécanismes de routage plusieurs-à-un efficaces [41].

- **LTE-A**

Long-Term Evolution Advanced (LTE-A) est un ensemble de normes conçues pour s'adapter aux communications M2M et aux applications IoT dans les réseaux cellulaires. Le LTE-A est un

protocole évolutif et moins coûteux par rapport aux autres protocoles cellulaires. Le LTE-A utilise OFDMA (Orthogonal Frequency Division Multiple Access) comme technologie d'accès à la couche MAC, qui divise la fréquence en plusieurs bandes et chacune peut être utilisée séparément. L'architecture du LTE-A se compose d'un réseau central (CN), d'un réseau d'accès radio (RAN) et des nœuds mobiles. Le CN est responsable du contrôle des appareils mobiles et du suivi de leurs adresses IP. RAN est responsable de l'établissement de contrôle de données et de la gestion de la connectivité sans fil et du contrôle d'accès radio [42].

- **SigFox**

Sigfox utilise une modulation à décalage de phase binaire différentiel (DBPSK) et le détrempage à décalage de fréquence gaussien (GFSK) qui permettent la communication à l'aide de la bande radio ISM industrielle, scientifique et médicale qui utilise 868 MHz en Europe et 902 MHz aux États-Unis. Il utilise un signal de grande portée qui passe librement à travers des objets solides, appelé «bande ultra-étroite» et nécessite peu d'énergie, appelé «réseau étendu à faible puissance (LPWAN)». Le réseau est basé sur une topologie en étoile à un saut et nécessite un opérateur mobile pour transporter le trafic généré. [43] Le signal peut également être utilisé pour couvrir facilement de grandes surfaces et atteindre des objets souterrains. En octobre 2018, le réseau Sigfox IoT avait couvert un total de 4,2 millions de kilomètres carrés dans un total de 50 pays et était en voie d'atteindre 60 pays d'ici la fin de 2018. [44]

- **LoRa**

LoRa est la couche physique ou la modulation sans fil utilisée pour créer le lien de communication à longue portée. De nombreux systèmes sans fil traditionnels utilisent la modulation FSK (Frequing Keying Keying) comme couche physique car il s'agit d'une modulation très efficace pour atteindre une consommation d'énergie faible. LoRa est basé sur une modulation à spectre étalé en modulation, qui maintient les mêmes caractéristiques de faible puissance que la modulation FSK, tout en augmentant considérablement la portée de la communication. Le spectre étalé en chirp est utilisé dans les communications militaires et spatiales depuis des décennies en raison des longues distances de communication pouvant être atteintes et de la résistance aux interférences, mais LoRa® est la première implémentation à faible coût pour un usage commercial [45].
LoRaWAN ™ définit le protocole de communication et l'architecture du système pour le réseau tandis que la couche physique LoRa® permet la liaison de communication à longue portée [45].

- **Résumé**

Une technologie ne peut pas desservir l’ensemble des applications et des volumes projetés pour l’IoT. WiFi et BLE sont des normes largement adoptées et servent assez bien aux applications liées à la communication de périphériques personnels. La technologie cellulaire convient parfaitement

aux applications nécessitant un débit de données élevé et disposant d'une source d'alimentation. LPWAN offre une durée de vie de la batterie de plusieurs années et est conçu pour les capteurs et les applications qui doivent envoyer de petites quantités de données sur de longues distances plusieurs fois par heure à partir de divers environnements.

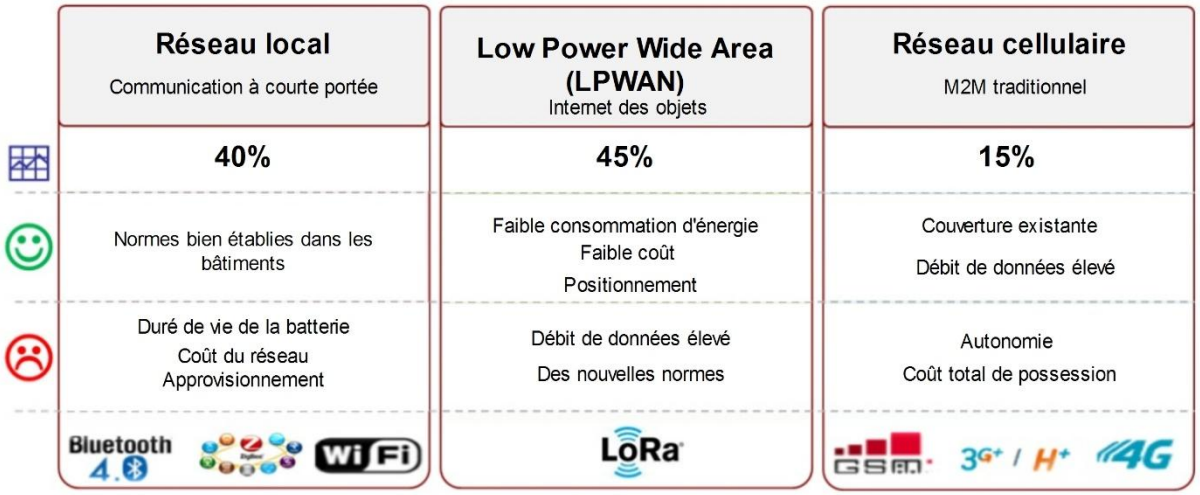


Figure 1.5 *Caractéristiques de protocoles*

- **Sigfox vs LoRa**

Les deux technologies ont leur propre infrastructure, de sorte que l'utilisateur n'a pas besoin de déployer de nouvelles antennes sur la région où le nœud d'extrémité va fonctionner. Ils opèrent également dans les mêmes bandes sans licence : 868 en Europe et 815 aux États-Unis. La topologie du réseau est la même que dans toutes les autres technologies IoT : étoile. Le nœud central est la passerelle et les éléments environnants sont les nœuds d'extrémité.

L'une des principales différences entre eux est la bande passante utilisée dans la communication. SIGFOX utilise une bande passante à bande ultra-étroite (UNB), qui permet une plus grande portée car il y a moins de bruit dans le canal. Le bruit se propage dans le spectre. Par conséquent, si la bande passante est aussi large que celle utilisée dans LoRa, le bruit sera également important. En ce qui concerne la charge utile, SIGFOX ne permet pas de transmettre plus de 12 octets par paquet, tandis que LoRa peut transmettre jusqu'à 255 octets [46]. Le débit de données dans LoRa (50 kbps) est également supérieur à celui de SIGFOX (100 bps), ce qui permet d'envoyer plus de données en moins de temps.

L'une des principales raisons pour lesquelles ces technologies sont à faible consommation d'énergie est le type de synchronisation mis en œuvre. Les appareils n'écoutent le support qu'après chaque transmission, au lieu d'écouter en permanence comme le font les autres technologies.

Les principales caractéristiques de chaque technologie sont résumées dans le tableau 1.2 [47].

Tableau 1.2 *SigFox vs LoRa*

	SIGFOX	LORA
Modulation	Bande ultra étroite BPSK	Chip Spread Spectrum modulation (CSS)
Bande passante par canal	100Hz	UE : 125 kHz et 250 kHz États-Unis : 125 kHz et 500 kHz
Bande de fréquence	UE : sans licence 868 MHz États-Unis : sans licence 915 MHz	UE : 433, 868 MHz non homologués États-Unis : sans licence 915 MHz
budget de lien	162 dB	155 dB
Débit de données	100 bps	De 250 bps à 50 kbps
Limitation msgs / jour	140 msgs / jour	Illimité
Taille de paquet	12 octets	Jusqu'à 255 octets
Synchronisation	Asynchrone	Asynchrone
Caractéristiques du réseau	Étoile	Étoile
Les problèmes de sécurité	Sauts de fréquence et anti-rejeu. Pas de cryptage	Cryptage AES 128 bits
Open source?	Non	Oui
Portée	Rurale: 30-50 km. Urbain: 3-10 km	Rural: 10-15 km Urbain: 3-5 km
Évolutif	Oui	Oui

LoRa a été choisie comme technologie IoT pour le système de suivi pour plusieurs raisons:

Portée : SIGFOX a une meilleure portée (de 10 à 15 km), mais la portée en LoRa est suffisante pour la réalisation du projet.

Open source : Il existe de nombreuses informations sur son implémentation, ses couches, ses structures de paquets, ses protocoles de communication et d'autres fonctionnalités de LoRa, qui peut être privé ou public. A l'inverse l'entreprise toulousaine SigFox diffusait peu d'informations sur son réseau qui nécessite obligatoirement un abonnement.

Bande passante : la bande passante dans LoRa est supérieure, il est donc préférable de distinguer différents trajets du même signal (utile pour les capacités de suivi dans les scénarios urbains où des réflexions sont présentes).

1.3.3. Protocoles de la couche session

Cette section passe en revue les normes et les protocoles de passage de messages dans la couche de session IoT proposés par différentes organisations de normalisation. La plupart des applications IP, y compris les applications IoT, utilisent TCP ou UDP pour le transport. Cependant, il existe plusieurs fonctions de distribution de messages qui sont communes à de nombreuses applications IoT; il est souhaitable que ces fonctions soient implémentées de manière standard interopérable par différentes applications. Ce sont les protocoles dits «de couche session» décrits dans cette section.

- **MQTT**

MQTT a été introduit par IBM en 1999 et normalisé par OASIS en 2013 [48]. Il est conçu pour fournir une connectivité intégrée entre les applications et les middlewares d'un côté et les réseaux et communications de l'autre. Il suit une architecture de publication / abonnement, où le système se compose de trois composants principaux : les éditeurs, les abonnés et un courtier. Du point de vue IoT, les éditeurs sont essentiellement les capteurs légers qui se connectent au courtier pour envoyer leurs données et se rendormir chaque fois que possible. Les abonnés sont des applications qui s'intéressent à un certain sujet ou à des données sensorielles, ils se connectent donc aux courtiers pour être informés chaque fois que de nouvelles données sont reçues. Les courtiers classent les données sensorielles en thèmes et les envoient aux abonnés intéressés par les thèmes.

- **SMQTT**

Une extension de MQTT est SMQTT qui utilise un cryptage basé sur un cryptage léger basé sur des attributs. Le principal avantage de l'utilisation d'un tel chiffrement est la fonction de chiffrement de diffusion, dans laquelle un message est chiffré et remis à plusieurs autres nœuds, ce qui est assez courant dans les applications IoT. En général, l'algorithme comprend quatre étapes principales : configuration, chiffrement, publication et déchiffrement. Dans la phase de configuration, les abonnés et les éditeurs s'enregistrent auprès du courtier et obtiennent une clé secrète principale en fonction du choix de leur développeur d'algorithme de génération de clés. Ensuite, lorsque les données sont publiées, elles sont chiffrées, publiées par le courtier qui les envoie aux abonnés et enfin déchiffrées chez les abonnés qui ont la même clé secrète principale. Les algorithmes de génération et de chiffrement des clés ne sont pas standardisés. SMQTT est proposé uniquement pour améliorer la fonction de sécurité MQTT [49].

- **AMQP**

Le protocole AMQP est un autre protocole de couche session conçu pour l'industrie financière. Il fonctionne sur TCP et fournit une architecture de publication / abonnement similaire à celle de

MQTT. La différence est que le courtier est divisé en deux composants principaux : échange et files d'attente. L'échange est responsable de la réception des messages de l'éditeur et de leur distribution dans les files d'attente en fonction des rôles et conditions prédéfinis. Les files d'attente représentent essentiellement les sujets et sont souscrites par les abonnés qui obtiendront les données sensorielles dès qu'elles seront disponibles dans la file d'attente [50]

- **CoAP**

CoAP est un autre protocole de couche session conçu par le groupe de travail IETF Constrained RESTful Environment (Core) pour fournir une interface RESTful (HTTP) légère. Le transfert d'état représentatif (REST) est l'interface standard entre le client HTTP et les serveurs. Cependant, pour les applications légères telles que l'IoT, REST peut entraîner des frais généraux et une consommation d'énergie importante. CoAP est conçu pour permettre aux capteurs de faible puissance d'utiliser les services RESTful tout en respectant leurs contraintes d'alimentation. Il est construit sur UDP, au lieu de TCP couramment utilisé dans HTTP et dispose d'un mécanisme léger pour assurer la fiabilité. L'architecture CoAP est divisée en deux sous-couches principales : la messagerie et la demande / réponse. La sous-couche messagerie est responsable de la fiabilité et de la duplication des messages tandis que la sous-couche demande / réponse est responsable de la communication. CoAP a quatre modes de messagerie : confirmable, non confirmable, superposé et séparé. Les modes confirmables et non confirmables représentent les transmissions fiables et non fiables, respectivement tandis que les autres modes sont utilisés pour la demande / réponse. Le ferroutage est utilisé pour la communication directe client / serveur où le serveur envoie sa réponse directement après avoir reçu le message, c'est-à-dire dans le message d'accusé de réception. D'un autre côté, le mode séparé est utilisé lorsque la réponse du serveur arrive dans un message distinct de l'accusé de réception et peut mettre un certain temps à être envoyé par le serveur. Comme dans HTTP, CoAP utilise les demandes de messages GET, PUT, PUSH, DELETE pour récupérer, créer, mettre à jour et supprimer, respectivement [51].

- **XMPP**

XMPP est un protocole de messagerie conçu à l'origine pour les applications de conversation et d'échange de messages. Il a été normalisé par l'IETF il y a plus d'une décennie [52]. Par conséquent, il est bien connu et s'est révélé très efficace sur Internet. Récemment, il a été réutilisé pour des applications IoT ainsi qu'un protocole pour SDN. Cette réutilisation du même standard est due à son utilisation du XML qui le rend facilement extensible. XMPP prend en charge l'architecture de publication / abonnement et de demande / réponse et il appartient au développeur de l'application de choisir l'architecture à utiliser. Il est conçu pour les applications en temps quasi réel et prend donc

en charge efficacement les petits messages à faible latence. Il n'offre aucune garantie de qualité de service et, par conséquent, n'est pas pratique pour les communications M2M. De plus, les messages XML créent une surcharge supplémentaire en raison de nombreux en-têtes et formats de balises qui augmentent la puissance critique pour l'application IoT. Par conséquent, XMPP est rarement utilisé dans l'IoT mais a gagné un certain intérêt pour l'amélioration de son architecture afin de prendre en charge les applications IoT.

- **DDS**

DDS est un autre protocole de publication / abonnement conçu par l'OMG pour les communications M2M. L'avantage de base de ce protocole est l'excellente qualité des niveaux de service et les garanties de fiabilité car il repose sur une architecture sans courtier, adaptée aux communications IoT et M2M. Il offre 23 niveaux de qualité de service qui lui permettent d'offrir une variété de critères de qualité, notamment : sécurité, urgence, priorité, durabilité, fiabilité, etc. Le premier prend la responsabilité de la remise des messages aux abonnés tandis que le second est facultatif et permet une intégration simple du DDS dans la couche application. La couche Publisher est responsable de la distribution des données sensorielles. Le rédacteur de données interagit avec les éditeurs pour convenir des données et des modifications à envoyer aux abonnés. Les abonnés sont les destinataires des données sensorielles à livrer à l'application IoT. Les lecteurs de données lisent essentiellement les données publiées et les fournissent aux abonnés et les sujets sont essentiellement les données qui sont publiées. En d'autres termes, les rédacteurs de données et les lecteurs de données prennent les responsabilités du courtier dans les architectures basées sur le courtier [53].

- **Résumé**

L'IoT possède de nombreux protocoles de couche session standardisés qui ont été brièvement mis en évidence dans cette section. Ces protocoles de couche session dépendent de l'application et le choix entre eux est très spécifique à l'application. Il convient de noter que le MQTT est le plus largement utilisé dans l'IoT en raison de sa faible surcharge et de sa faible consommation d'énergie. C'est une organisation et des applications spécifiques pour choisir entre ces normes. Par exemple, si une application a déjà été construite avec XML et peut donc accepter un peu de surcharge dans ses en-têtes, XMPP peut être la meilleure option pour choisir parmi les protocoles de couche session. D'un autre côté, si l'application est vraiment au-dessus et sensible à la puissance, choisir MQTT serait cependant la meilleure option qui accompagne l'implémentation supplémentaire du courtier. Si l'application nécessite une fonctionnalité REST car elle sera basée sur HTTP, alors CoAP serait la meilleure option si c’est ne pas la seule. Le tableau 1.3 résume les points de comparaison entre ces différents protocoles de couche session.

Tableau 1.3 *Comparaison des normes de la couche de transport IoT*

Protocoles	UDP / TCP	Architecture	Sécurité et QoS	Taille d'en-tête (octets)	Longueur maximale (octets)
MQTT	TCP	Pub / Sub	Les deux	2	5
AMQP	TCP	Pub / Sub	Les deux	8	-
CoAP	UDP	Req / Res	Les deux	4	20 (typique)
XMPP	TCP	Les deux	Sécurité	-	-
DDS	TCP / UDP	Pub / Sub	QoS	-	-

1.4. La communication M2M

Machine-to-Machine (M2M) représente un futur IOT où des milliards d'objets quotidiens et des environnements environnants sont connectés et gérés à travers une gamme de dispositifs, de réseaux de communication et de serveurs en cloud [54]. La communication M2M, également appelée MTC, permet d'échanger des informations entre machines et machines sans interaction humaine. En effet, La communication M2M est une nouvelle technologie de communication par laquelle un grand nombre de "dispositifs intelligents" peuvent communiquer entre eux de façon autonome et prendre des décisions collaboratives sans intervention humaine directe [55] pour améliorer la rentabilité et la gestion du temps. La communication Machine-to-Machine a son origine dans les systèmes de contrôle de supervision et d'acquisition de données (SCADA), où des capteurs et d'autres appareils connectés par câble ou sans fil sont utilisés avec des ordinateurs pour surveiller et contrôler les processus industriels.

Les communications machine-to-machine sont définies comme l'échange d'informations entre machines et machines sans interaction humaine. Avec l'interconnexion à internet, un grand nombre de dispositifs sont organisés de manière autonome pour constituer un réseau M2M. Les réseaux M2M devraient être largement utilisés dans de nombreux domaines des applications omniprésentes [39], notamment l'automatisation industrielle et agricole, les soins de santé, les systèmes de transport, les réseaux électriques, etc. Deux principales caractéristiques des réseaux M2M :

1) Un nombre énorme de dispositifs dans la couverture de service et la tentative d'accès réseau simultané à partir de ces dispositifs.

2) Haut niveau d'automatisation du système dans lequel les dispositifs et les systèmes peuvent échanger et partager des données.

Par conséquent, la gestion massive des accès et le protocole d'accès au support sont les principaux problèmes des communications M2M pour la mise en place d'un système de communication

évolutif, flexible et automatique [56]. Un exemple des communications M2M est montré dans la figure 1.6.

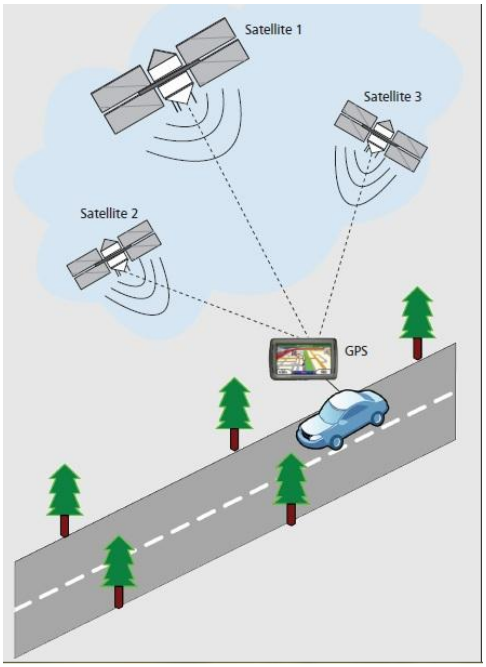


Figure 1.6 *Exemple de communication M2M [13]*

1.4.1. Caractéristiques de la communication M2M

Les communications M2M ont des caractéristiques différentes de celles des communications interhumaines (H2H), en termes de génération de trafic, de qualité de service (QoS) et de caractéristiques de l'appareil [57]. L'intégration d'une multitude hétérogène d'appareils dans un même réseau est une tâche difficile et nécessite beaucoup de recherches. Avoir une gestion de réseau et une gestion de service fiables est important. De plus, une faible latence et une haute sécurité sont des critères critiques dans des applications telles que le réseau intelligent et l'e-santé. En outre, les compteurs intelligents intégrés et les appareils intelligents dotés de fonctionnalités limitées nécessitent un protocole à faible consommation d'énergie [58].

Les périphériques M2M génèrent généralement des petites quantités de données rarement, tandis que d'autres génèrent leurs données périodiquement [59]. Certains périphériques M2M doivent envoyer périodiquement des paquets, tels que des dispositifs médicaux, tandis que d'autres peuvent avoir un schéma piloté par un événement qui doit envoyer un paquet chaque fois qu'un événement est déclenché par le serveur. Les périphériques M2M génèrent plus de trafic sur la liaison montante, alors que H2H génère plus de trafic sur la liaison descendante. Les dispositifs M2M sont généralement à faible coût, fonctionnant sur batterie avec des ressources énergétiques limitées.

1.4.2. Les exigences des protocoles MAC

Pour soutenir les communications M2M, les protocoles MAC doivent être conçus avec un ensemble d'exigences riche afin de satisfaire les besoins des applications et des scénarios [59]. Cette section décrit ces exigences en détail.

- Débit des données : En raison des ressources canal / spectre limitées et le grand nombre de dispositifs ayant accès au canal, il est souhaitable que le protocole MAC minimise la perte de temps due à des collisions ou à l'échange des messages de contrôle. De manière équivalente, le débit doit être élevé afin d'accueillir le très grand nombre d'appareils [59].
- Extensibilité : Les scénarios avec les communications M2M sont censés avoir un grand nombre de nœuds. On prévoit que la densité de nœud va augmenter comme le déploiement des scénarios d'application avec les communications M2M devient plus répandu. En outre, les types de réseau peuvent être dynamiques, avec des nœuds qui entrent et sortent (ou en alternance entre des états actif et inactif). Ainsi, il est impératif que le protocole MAC soit facilement évolutif et ajusté grâce à l'évolution des densités de nœuds avec peu ou pas d'échange d'informations de contrôle, et maintenir l'équité, même après l'ajout de nouveaux appareils [59].
- L'efficacité énergétique est l'une des plus importantes considérations de conception pour les communications M2M en raison des trois facteurs principaux, qui sont: 1) le fait que de nombreux dispositifs dans les réseaux M2M sont censés être alimentés par batterie et donc la puissance est limitée; 2) l'impact économique (tels que les coûts d'exploitation et les marges bénéficiaires) de la puissance consommée par l'infrastructure de communication; et 3) l'impact environnemental de la puissance consommée [59].
- La latence : Pour la plupart des applications qui reposent sur les communications M2M, la latence du réseau est un facteur critique qui détermine l'efficacité et l'utilité des services offerts. Par exemple, dans des scénarios tels que les systèmes de transport intelligents avec contrôle en temps réel des véhicules, et les applications e-santé, il est extrêmement important de rendre la communication rapide et fiable. Ainsi, les retards au cours de l'accès au canal ou l'encombrement du réseau sont des problèmes graves dans les réseaux M2M [59].
- La rentabilité : Enfin, dans le but de rendre les systèmes basés communication M2M une réalité, les appareils doivent être rentables pour qu'il soit abordable de les déployer. Un protocole MAC qui possède de nombreuses propriétés souhaitables, mais repose sur l'utilisation de matériel complexe et coûteux, n'est pas pratique [59].

1.5. Interopérabilité IoT

Le problème de l'interopérabilité des systèmes d'information existe depuis 1988 ; et peut-être même plus tôt. Il existe plusieurs définitions d'interopérabilité dans la littérature. Parmi les diverses définitions de l'interopérabilité, nous citons celles liées à notre contexte. Le dictionnaire Oxford donne une définition générale de l'interopérabilité comme pouvant fonctionner conjointement. Cela implique que deux systèmes interopérables peuvent se comprendre et utiliser leurs fonctionnalités respectives. ISO / CEI définit l'interopérabilité comme étant la capacité à communiquer, exécuter des programmes ou transférer des données entre différentes unités fonctionnelles, ce qui oblige l'utilisateur à avoir une connaissance minimale voire inexistante des caractéristiques uniques de ces unités [60]. Dans une perspective plus large, l'IEEE définit l'interopérabilité comme étant la capacité de deux systèmes ou composants ou plus à échanger des informations et à utiliser les informations échangées. Selon cette définition, l'interopérabilité est réalisée par l'élaboration de normes. Dans l'IoT, l'interopérabilité peut être définie comme la capacité de deux systèmes à communiquer et à partager des services l'un avec l'autre [61].

La capacité d'interopérabilité de deux systèmes peut également être présentée à l'aide de différents types de modèles en couches. Par exemple, une structure à six niveaux comprenant: aucune connexion (aucune interopérabilité entre systèmes), technique (connectivité de base et connectivité réseau), syntaxique (interopérabilité des échanges de données), sémantique (compréhension du sens des données), pragmatique / dynamique (applicabilité). de l'information) et conceptuelle (vision partagée du monde) est élaborée par Tolk et al. Un modèle similaire à six niveaux est proposé dans [62] par Pantsar Syvaniemi et al. Contient: connexion, communication, sémantique, dynamique, comportemental et conceptuel. Ces six niveaux correspondent aux niveaux de modèle de Tolk, respectivement technique, syntaxique, sémantique, pragmatique / dynamique et conceptuel.

1.5.1. Interopérabilité dans l'IoT: une taxonomie

Pour comprendre l'interopérabilité dans l'IoT, nous devons adopter une approche de classification. Cette section de l'étude décrit une vue d'ensemble de la taxonomie d'interopérabilité IoT. Les problèmes d'interopérabilité dans IoT peuvent être vus de différentes perspectives en raison de l'hétérogénéité. L'hétérogénéité n'est pas un nouveau concept ni limitée à un domaine. Même dans le monde physique, il existe de nombreux types d'hétérogénéité, par exemple, les gens parlent des langues différentes, mais ils peuvent toujours communiquer entre eux par le biais d'un traducteur (homme / outils) ou en utilisant un langage commun. De même, les divers éléments composant l'IoT (appareils, communication, services, applications, etc.) devraient coopérer et communiquer sans

faille pour réaliser le plein potentiel de l'écosystème de l'Internet des objets. L'interopérabilité IoT peut être vue sous différents angles, tels que l'interopérabilité des périphériques, l'interopérabilité des réseaux, l'interopérabilité syntaxique, l'interopérabilité sémantique et l'interopérabilité des plates-formes.

- **Interopérabilité des appareils**

L'IoT est composé d'une variété d'appareils, encore plus que l'Internet traditionnel. Ces dispositifs, appelés "objets intelligents", peuvent être des dispositifs haut de gamme ou bas de gamme [63]. Les appareils IoT haut de gamme disposent de suffisamment de ressources et de capacités de calcul, telles que Raspberry Pi et les smartphones. D'autre part, les périphériques IoT bas de gamme sont limités en ressources en énergie, en puissance de traitement et en capacités de communication, par rapport aux hôtes classiques tels que les tags RFID, les capteurs minuscules et économiques, et les actionneurs, Arduino et OpenMote, pour en nommer un peu. L'architecture de microcontrôleur (MCU) et les caractéristiques systèmes clés des périphériques IoT, telles que la vitesse du processeur, la mémoire vive, la technologie de communication et la capacité de la batterie, diffèrent largement selon les marques et les modèles. De plus, divers protocoles de communication ont vu le jour en raison des exigences différentes des marchés de l'IoT. Par exemple, les périphériques IoT tels que Smart TV, les imprimantes et les climatiseurs prennent en charge les technologies Wi-Fi omniprésentes et les communications cellulaires 3G / 4G. Les dispositifs médicaux IoT les plus récents sont basés sur la norme ANT +; les autres périphériques portables prennent généralement en charge les technologies Bluetooth SMART et NFC, tandis que les capteurs environnementaux utilisent ZigBee basé sur la norme IEEE 802.15.4. Outre ces protocoles, les protocoles de communication standard sont utilisés pour les appareils intelligents, les capteurs et les actionneurs (c'est-à-dire Z-Wave, ZigBee principalement), ainsi que pour la solution propriétaire non standard (c'est-à-dire LoRa, SIGFOX).

Dans certains cas, les périphériques souhaitant échanger des informations peuvent utiliser différentes technologies de communication, ce qui nécessite une interopérabilité entre les différents types de périphériques hétérogènes coexistant dans l'écosystème IoT. L'interopérabilité des dispositifs consiste à permettre l'intégration et l'interopérabilité de tels dispositifs hétérogènes avec divers protocoles et normes de communication pris en charge par des dispositifs IoT hétérogènes. L’interopérabilité des dispositifs concerne (i) l’échange d’informations entre dispositifs hétérogènes et protocoles de communication hétérogènes et (ii) la possibilité d’intégrer de nouveaux dispositifs dans n’importe quelle plate-forme IoT.

- **L'interopérabilité des réseaux**

Les réseaux sur lesquels les appareils IoT fonctionneront continueront d'être hétérogènes, multi-services, multi-fournisseurs et largement distribués. Différents des ordinateurs de bureau, les appareils IoT reposent généralement sur diverses technologies de communication et de mise en réseau sans fil à courte portée, qui sont plutôt intermittentes et peu fiables [63]. L'interopérabilité au niveau du réseau traite des mécanismes permettant un échange de messages transparent entre les systèmes via différents réseaux (réseaux de réseaux) pour une communication de bout en bout. Pour rendre les systèmes interopérables, chaque système devrait pouvoir échanger des messages avec d'autres systèmes via différents types de réseaux. En raison de l'environnement réseau hétérogène et dynamique de l'IoT, le niveau d'interopérabilité du réseau devrait traiter des problèmes tels que l'adressage, le routage, l'optimisation des ressources, la sécurité, la qualité de service et la prise en charge de la mobilité [64].

- **L'interopérabilité syntaxique**

L'interopérabilité syntaxique fait référence à l'interopérabilité du format ainsi que de la structure de données utilisée dans tout échange d'information ou de service entre des entités de système hétérogènes IoT. Une interface doit être définie pour chaque ressource, exposant une structure en fonction d'un schéma. Les API WSDL et REST sont des exemples. Le contenu des messages doit être sérialisé pour être envoyé sur le canal et le format pour le faire (tel que XML ou JSON). L'expéditeur du message code les données d'un message à l'aide de règles syntaxiques, spécifiées dans certaines règles grammaticales. Le destinataire du message décode le message reçu en utilisant des règles syntaxiques définies dans la même grammaire ou dans une autre. Des problèmes d'interopérabilité syntaxique surviennent lorsque les règles de codage de l'expéditeur sont incompatibles avec les règles de décodage du destinataire, ce qui entraîne une discordance des arborescences d'analyse des messages.

- **Interopérabilité sémantique**

Le W3C définit l'interopérabilité sémantique comme un moyen permettant à différents agents, services et applications d'échanger des informations, des données et des connaissances de manière significative, sur le Web et en dehors de celui-ci [65]. TheWoT résout la fragmentation actuelle en exposant des données d'objets et de systèmes ainsi que des métadonnées via l'API. Toutefois, ces efforts ont été entravés par le fait que les parties concernées doivent partager la connaissance d'une API et que de nombreux périphériques ne parlent pas le même langage et ne peuvent pas échanger entre passerelles et hubs intelligents différents [66]. Pour être plus précis, les données générées par des éléments relatifs à l'environnement peuvent avoir un format de données défini (par exemple, JSON, XML ou CSV), mais les modèles de données et les schémas utilisés par différentes sources

sont généralement différents et pas toujours compatibles. En outre, les données peuvent être représentées dans diverses unités de mesure et consister en d'autres informations. Cette incompatibilité sémantique entre les modèles de données et les modèles d'information fait que les systèmes IoT ne peuvent pas interagir de manière dynamique et automatique car ils ont des descriptions ou des conceptions différentes des ressources et des procédures opérationnelles, même si les systèmes IoT exposent leurs données et leurs ressources à d'autres .

- **Interopérabilité de la plateforme**

Les problèmes d'interopérabilité des plates-formes dans l'IoT sont dus à la disponibilité de divers systèmes d'exploitation, systèmes d'exploitation, langages de programmation, structures de données, architectures et mécanismes d'accès aux objets et aux données. Il existe actuellement de nombreux systèmes d'exploitation développés spécifiquement pour les appareils IoT, tels que Contiki8, RIOT9, TinyOS [67] et OpenWSN [68], chacun avec plusieurs versions, afin de fournir des services aux utilisateurs. En outre, les fournisseurs de plate-forme IoT tels que Apple HomeKit, Google Brillo, Amazon AWS IoT et IBM Watson fournissent différents systèmes d'exploitation, langages de programmation et structures de données. Par exemple, Apple HomeKit prend en charge son propre langage open source Swift, Google Brillo utilise Weave et Amazon AWS IoT propose des SKD pour C et NodeJS intégrés. Cette non-uniformité empêche les développeurs d'applications de développer des applications IoT multi-plateformes et multi-domaines.

Les développeurs doivent acquérir une connaissance approfondie des API spécifiques à la plate-forme et des modèles d'informations de chaque plate-forme différente pour pouvoir adapter leurs applications d'une plate-forme à une autre. Une application IoT multiplate-forme peut accéder à différentes plates-formes IoT et intégrer des données provenant de différentes plates-formes. Par exemple, considérons le scénario d'application suivant: un utilisateur qui a des problèmes de santé utilise quotidiennement une application multiplate-forme IoT pour l'aider dans ses tâches quotidiennes. L'application IoT se connecte à la plateforme de santé intelligente de l'utilisateur, composée de capteurs portables, pour surveiller en permanence ses problèmes de santé (fréquence cardiaque, situation de chute et niveau de glucose) et, en cas d'urgence, le localise et envoie une ambulance. L'application peut également accéder à une plateforme de ville intelligente pour acheter un billet pour la destination souhaitée par l'utilisateur et indique l'itinéraire le plus rapide pour se rendre à la gare routière ou ferroviaire. Dans ce scénario, l'interopérabilité multiplate-forme entre les objets et les données permet l'interopérabilité entre des plates-formes IoT spécifiques à un domaine vertical telles que la maison intelligente, les soins de santé intelligents, le jardin intelligent, etc. réalisé dans lequel différentes plates-formes au sein de domaines hétérogènes sont fédérées pour construire des applications IoT horizontales. La figure 1.7 illustre le concept de

l'interopérabilité entre domaines dans lequel différentes plates-formes IoT de différents domaines IoT (santé, maison, transport, etc.) peuvent être intégrées pour créer de nouvelles applications innovantes. Par exemple, une plate-forme domestique intelligente peut fournir des facilitateurs spécifiques à un domaine, tels que la température de l'air et les conditions d'éclairage. Ces outils peuvent ensuite être exploités par d'autres plates-formes IoT, telles que les systèmes de santé intelligents, pour fournir des applications et des scénarios plus innovants.

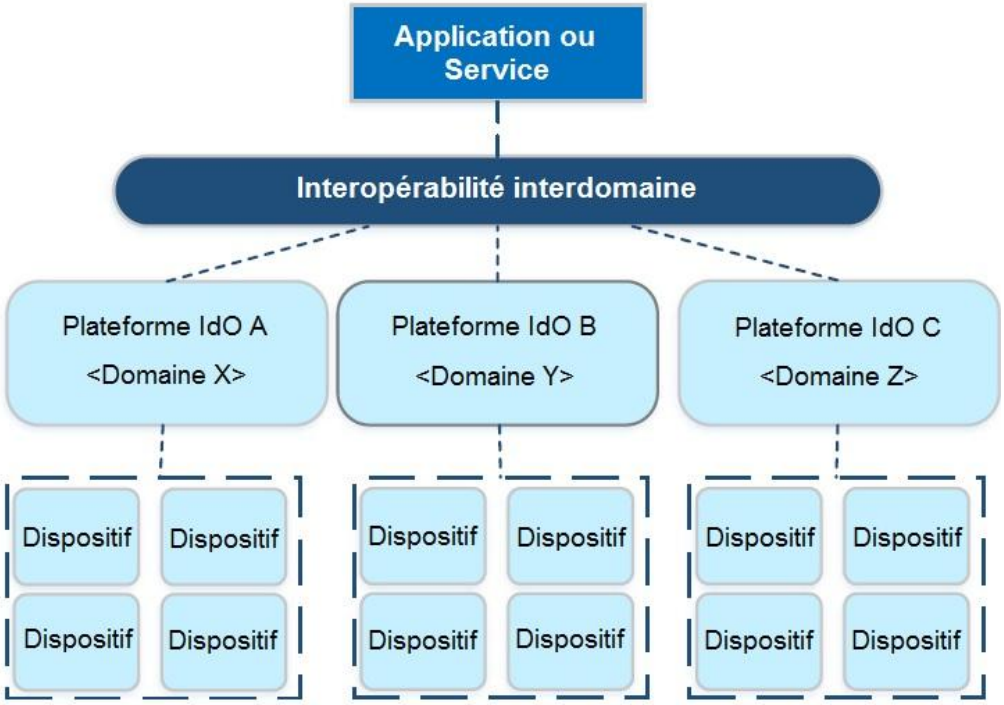


Figure 1.7 *Interopérabilité inter-domaine*

1.5.2. Approches de traitement d'interopérabilité dans l'IoT

Pour améliorer l'état de l'interopérabilité IoT, les chercheurs ont exploité de nombreuses approches et technologies, que nous appelons approches de traitement d'interopérabilité. Dans ce qui suit, nous donnons un aperçu des différentes approches de traitement d'interopérabilité permettant de résoudre les problèmes d'interopérabilité liés à l'Internet des objets. En outre, nous présentons dans le tableau 1 un échantillon représentatif de propositions relatives à l'IoT. L'objectif est de fournir une vue d'ensemble de la perspective d'interopérabilité sur laquelle elles se concentrent et des approches qu'elles adoptent en matière d'interopérabilité. En particulier, pour chaque proposition, nous considérons la perspective d'interopérabilité (interopérabilité de périphérique, de réseau, syntaxique, sémantique, multi-plateforme et multi-domaine), l'approche d'interopérabilité, l'ouverture, la connectivité, les protocoles d'application et les mesures de sécurité / confidentialité. Les différentes propositions sont divisées en cadres, projets et plates-formes standard IoT.

- **Adaptateurs / passerelles**

Les passerelles ou adaptateurs sont la classe de systèmes qui traitent de l'interopérabilité via le développement d'un outil intermédiaire, parfois appelé médiateur, destiné à améliorer l'interopérabilité entre les dispositifs IoT. L'objectif ici est de faire le pont entre différentes spécifications, données, normes, middleware, etc. Pour effectuer une conversion entre le protocole du périphérique émetteur et le protocole du périphérique récepteur, la passerelle peut être étendue à l'aide de plug-ins. Par exemple, lorsque les périphériques IoT utilisent des technologies de communication différentes (Bluetooth et ZigBee, par exemple) ou qu'ils utilisent des protocoles de couche d'application différents (XMPP et MQTT). Les passerelles peuvent être du matériel dédié ou la fonction peut être intégrée dans le micrologiciel ou le logiciel d'un périphérique intelligent tel qu'un automate programmable (PLC), une interface homme-machine (IHM) ou un ordinateur. Une passerelle de protocole un à un permet l'interopérabilité entre deux types de protocoles. Cette approche limite l'évolutivité en termes de nombre de produits IoT différents interagissant entre eux nécessitant des connecteurs spécifiques (complexité du temps de conception) et du nombre élevé de produits IoT dans un déploiement nécessitant un courtage (complexité d'exécution). Si nous supposons lier n produits IoT distincts, la complexité éventuelle sera n (n-1) / 2. L'utilisation d'un seul protocole pour l'IoT serait impossible. Par conséquent, plusieurs passerelles de protocole one-to-any sont utilisées pour assurer une interopérabilité transparente.

Il existe de nombreux travaux industriels et universitaires axés sur la normalisation et la conception des passerelles IoT. Par exemple, Apple HomeKit, l'écosystème Net Alphabet (Google), If-This-Then-That (IFTTT) 10 et Ponte [69] conçoivent différents connecteurs pour prendre en charge divers protocoles de communication d'appareils IoT. Par exemple, Ponte [69] a été initialement développé sous le nom de QEST. Il s'agit d'un framework qui permet de publier et de recevoir des données provenant de capteurs et d'actionneurs via des protocoles M2M, accessibles via un RESTAPI. Il permet au programmeur de convertir et d'échanger automatiquement des données entre HTTP, CoAP et MQTT. Cependant, la principale limite de Ponte est qu'il suppose que les périphériques sous-jacents prennent en charge TCP / IP et que les périphériques à ressources limitées n'ont pas été pris en compte. De plus, Zhu et al. [70] propose une passerelle IoT basée sur un logiciel programmable dans l'espace utilisateur pour relier l'hétérogénéité entre les protocoles WSN et les réseaux de communication mobiles ou Internet, et inclut des fonctionnalités telles que le transfert de données, la conversion de protocole et la gestion. La fonctionnalité de passerelle est réalisée par un smartphone et connecte des réseaux avec différents protocoles tels que ZigBee, Bluetooth, GPRS et Ethernet. Cependant, la principale limite de leur approche réside dans le fait que les utilisateurs ne peuvent accéder aux données du capteur que s'ils installent le logiciel serveur

sur leur PC. Les auteurs de [71] discutent du manque d'interopérabilité dans les applications et les services IoT. La passerelle proposée est responsable de l'adaptation des différents protocoles de périphérique et de la bonne gestion et des fonctionnalités de sécurité. L'architecture prend en charge les interfaces standard et propriétaires, ce qui lui permet également d'étendre les capacités de la passerelle. Mais les fonctionnalités d'évolutivité ne sont pas discutées. De même, des efforts comme [72, 73] présentent les Smartphones sur-mesure comme des passerelles mobiles pour l'interopérabilité IoT. Cependant, leur principale limitation est la consommation d'énergie excessive. Asensio propose le protocole CTP (Common Thing Protocol) afin de fournir une spécification permettant d'introduire des éléments dans l'IoT en utilisant une passerelle IoT intelligente comme composant principal de l'architecture. La passerelle sémantique en tant que service (SGS) est présentée comme une passerelle entre le monde physique et les couches de haut niveau d'un système IoT. Selon l'architecture SGS, les données de capteur brutes sont transférées des nœuds de puits externes au nœud de passerelle central via le proxy multiprotocole. Avant d'être transmises, les données sont annotées sémantiquement à l'aide de l'ontologie W3C SSN, de l'outil SemSOS et d'autres ontologies spécifiques à un domaine. L'annotation sémantique des données de capteur fournit une interopérabilité sémantique entre les messages et fournit des connaissances exploitables de niveau supérieur pour la mise en œuvre.

- **Réseaux virtuels / solutions basées sur la superposition**

Des réseaux virtuels ou des solutions reposant sur la superposition ont été proposés dans [74] dans le document "MENO" ("Managed Ecosystems of Networked Objects"), dans le but d'intégrer des capteurs, des actionneurs et d'autres objets intelligents IP de manière transparente à Internet, de bout en bout. la communication. MENO a pour objectif principal de créer un réseau virtuel au-dessus des réseaux physiques et de permettre ainsi la communication avec d'autres types de périphériques, notamment les nœuds de capteurs. Au sein de chaque réseau virtuel, une communication de bout en bout est possible en utilisant différents protocoles. Une fois que la communication de bout en bout est activée, les développeurs d'applications ont désormais la possibilité d'écrire de nouvelles applications utilisant des capteurs, des actionneurs et d'autres périphériques. Il semble être sur la bonne voie pour utiliser une approche claire pour intégrer le travail physique à Internet de manière transparente. Le concept utilisé par MENO est utilisé pour développer le réseau virtuel de l'Internet des objets (IoT-VN) [75] illustré à la afin d'intégrer des périphériques à ressources limitées dans Internet. Ceci est réalisé en créant un réseau virtuel de tous les périphériques souhaitant communiquer et coopérer. Leur solution est axée à la fois sur les ressources limitées et les ressources limitées. Cette intégration est réalisée en intégrant tous les périphériques impliqués dans un réseau virtuel sécurisé, appelé réseau virtuel Internet des objets

(IoT-VN). Cette approche présente l'avantage de permettre une communication de bout en bout entre les périphériques. Toutefois, les problèmes clés sont l'évolutivité et la liaison à des protocoles spécifiques.

1.5.3. Technologies de mise en réseau

Différents protocoles et technologies de réseau ont été utilisés pour assurer l'interopérabilité des réseaux dans l'IoT. Par exemple, les protocoles classiques UPnP (Universal Plug and Play) et DLNA sont utilisés pour la communication entre les périphériques IoT et la passerelle. Dans ce qui suit, nous discutons des principales technologies / solutions d'interopérabilité au niveau du réseau.

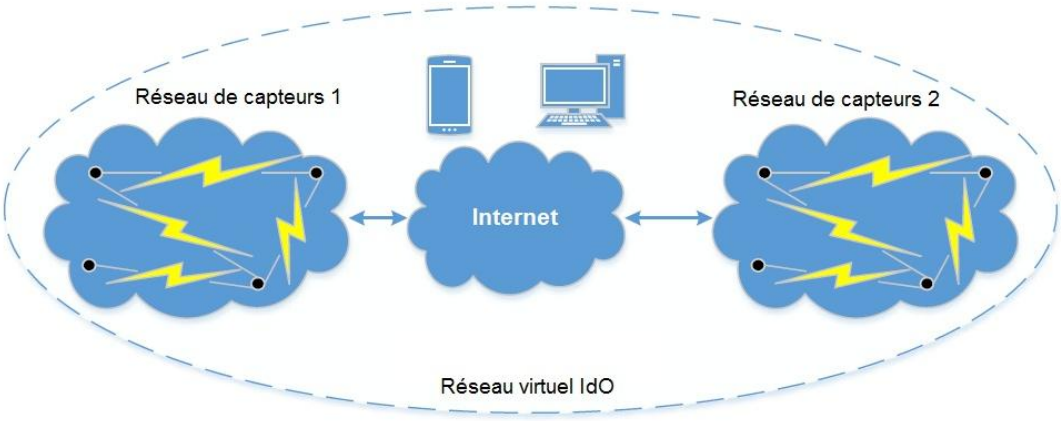


Figure 1.8 *Réseau virtuel*

- **Approches IP**

Les approches basées sur IP incorporent la pile TCP / IP complète sur des périphériques intelligents. En intégrant la pile TCP / IP sur la figure 1.8, le capteur et les actionneurs sont directement connectés au réseau IP pour permettre une communication de bout en bout entre le réseau de capteurs et le réseau IP. Par conséquent, le capteur et les actionneurs sont directement connectés au réseau IP pour permettre une communication de bout en bout entre le réseau de capteurs et le réseau IP. Certains ont tenté d'implémenter la pile TCP / IP sur des nœuds de capteur tels que uIP [75], TinyTCP [76] et lwIP [77]. Le principal avantage de la mise en œuvre de la pile TCP / IP sur les nœuds de capteur est que les passerelles et les traductions de protocole ne sont pas nécessaires. Cependant, les auteurs de [78] affirment qu'un réseau de capteurs entièrement IP n'est pas possible sur les nœuds de capteurs en raison de leur propriété de contrainte de ressource. En raison du succès de ces implémentations, l'IETF a constitué des groupes de travail au niveau de la couche réseau, tels que Routage sur réseaux ROLL (Low Routing et Lowy Networks) [79], Protocole WPAN (6LoWPAN) IPv6 sur réseaux Low Loss, CoAP) qui repose sur UDP et sur un environnement de repos contraint pour résoudre le problème de connectivité des périphériques aux ressources limitées. Cette approche utilise toujours des passerelles pour convertir entre les protocoles standards utilisés

sur Internet et les protocoles propriétaires utilisés sur le réseau de capteurs, par ex. IPv6 à 6LoWPAN. Par conséquent, en raison de l'utilisation de protocoles standards, cette approche ne présente pas les limitations des approches basées sur la passerelle. Le principal avantage est que la passerelle et les nœuds de capteur ne doivent pas nécessairement provenir du même fournisseur, ce qui améliore l'interopérabilité entre les périphériques. IP, le standard de facto d'Internet, fournit une interface standard ouverte unique pour un billion de choses. Cependant, en permettant un accès direct avec les périphériques resourceconstrained, des problèmes liés à la sécurité, tels que l'authentification et le contrôle d'accès, sont présentés. Les problèmes de sécurité posés par les approches basées sur IP sont détaillés dans [80].

- **Réseau défini par logiciel (SDN)**

Le réseau défini par logiciel (SDN) [81] est un nouveau paradigme de mise en réseau visant à rendre les réseaux sans fil et mobiles actuels plus "intelligents", efficaces, sécurisés et évolutifs afin de gérer la grande quantité de données produites dans l'IoT. L'une des principales nouveautés du SDN pour la suppression des silos verticaux dans l'IoT consiste à séparer les plans de contrôle et de données dans les périphériques réseau. La figure 1.9 illustre une vue simplifiée de l'intégration de l'IoT et du SDN.

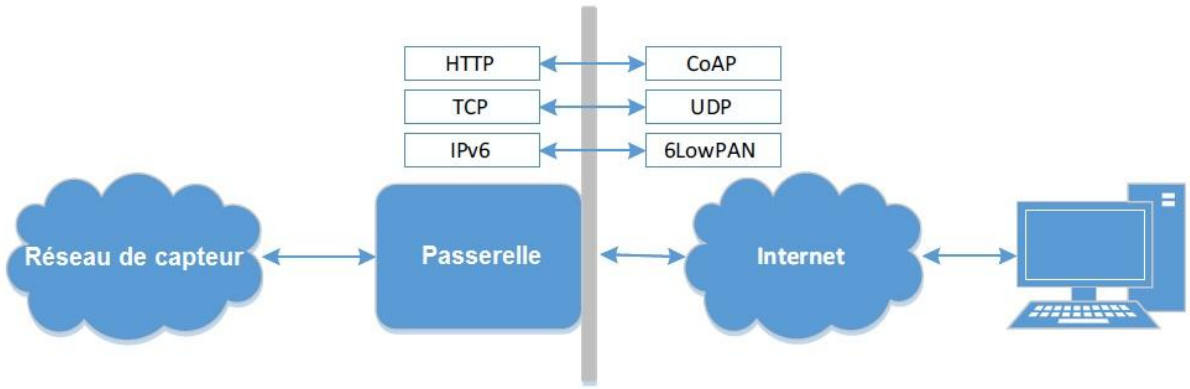


Figure 1.9 *Les approches IP*

Le SDN a été appliqué à l'IoT pour faciliter les applications réseau telles que l'hétérogénéité, la gestion de la mobilité, la gestion de la qualité de service et la sécurité [82]. Par exemple, Martinez-Julia et Skarmeta [77] ont utilisé SDN pour permettre à différents objets de différents réseaux de communiquer entre eux via IPv6 tout en simplifiant les opérations de gestion et de contrôle de différents types d'objets en ajoutant un contrôleur IoT supplémentaire au-dessus du réseau. Contrôleur SDN. Ainsi, même si les périphériques ont des protocoles différents, les périphériques de transmission du routeur le convertissent sous une forme compréhensible pour le destinataire. Cela permet la communication de divers périphériques du réseau. Dans [83], un autre travail insistant sur la nécessité de gérer l'hétérogénéité des divers dispositifs et applications IoT est

présenté. Les auteurs concluent que l'utilisation de l'IPv6 peut constituer un choix approprié pour gérer le grand nombre d'appareils connectés, mais l'hétérogénéité en termes de caractéristiques et de capacités diverses reste un sujet de recherche ouvert. Pour y remédier, ils fournissent une architecture de haut niveau plutôt qu'un contrôleur IoT, ce qui, au niveau générique, semble être un cadre adéquat pour gérer des flux hétérogènes d'IoT.

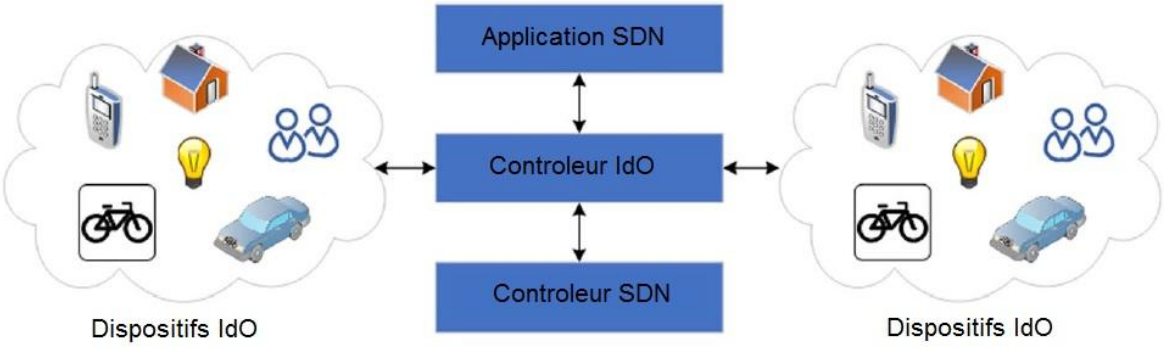


Figure 1.10 *Integration de l'IoT et SDN*

Dans [81], les auteurs ont proposé un nouveau service de mobilité adapté au concept sSDN pour résoudre les problèmes de performance du protocole PMIPv6. Les auteurs soutiennent que leur solution peut être utilisée pour la gestion de la mobilité au lieu de PMIPv6 sans utiliser le protocole IPv4 hérité. Un middleware est conçu et mis en œuvre par Qin, Z. et al. [82], qui est composé d'un contrôleur SDN IoT en couches permettant de gérer des réseaux multiples IoT distribués, hétérogènes et dynamiques. Dans leurs recherches, un contrôleur central surveille les ressources existantes et planifie la transmission en continu des données en fonction des exigences de service spécifiques, par exemple un débit de données minimal, un délai tolérable maximum ou une perte de paquets pour chaque flux séparé. IoT SDN exploite le calcul réseau pour modéliser les performances de flux de bout en bout dans les environnements multi-réseaux IoT, la modélisation sémantique pour la mise en correspondance des ressources et les algorithmes génétiques planifiant les flux, afin d'optimiser l'utilisation des opportunités de réseau IoT existantes. Les résultats de performance montrent que l'algorithme d'ordonnancement de flux basé sur un algorithme génétique offre de meilleures performances que les algorithmes de compression des fichiers et d'équilibrage de charge.

- **Virtualisation de la fonction réseau**

Une approche complémentaire du SDN est la virtualisation de la fonction réseau (NFV). Le NFV sépare les équipements physiques du réseau (traducteur d'adresses réseau, pare-feu) des fonctions qui les exécutent. De cette manière, de nombreux fournisseurs de services peuvent créer plusieurs

réseaux virtuels isolés pouvant ensuite partager les équipements de réseau physique fournis par les fournisseurs d'infrastructure réseau. NFV a le potentiel de réduire les coûts des dépenses opérationnelles (OPEX) et des dépenses d'investissement (CAPEX) en partageant l'infrastructure réseau, la mise à l'échelle dynamique, à la volée et le déploiement flexible des fonctions réseau [84].

Un exemple où NFV est utilisé dans l'IoT est [59], ils ont défini leur propre architecture abstraite IoT qui est ensuite combinée à l'architecture SDN (couches Application, Control et Infrastructure) pour produire un cadre général SDN-IoT. Il s'agit d'une couche supérieure avec des serveurs fournissant aux développeurs les API nécessaires aux applications IoT, d'une couche intermédiaire contenant un système d'exploitation réseau distribué, commandant plusieurs contrôleurs SDN distribués physiquement, d'une couche sud contenant les commutateurs réseau activés pour le SDN et la passerelle IoT, qui les connecte à la couche intermédiaire. En substance, il ne s'agit que de l'architecture SDN classique, avec les applications IoT à l'esprit. Les auteurs vont encore plus loin en affirmant que, pour réaliser un réseau optimisé pour l'IoT, il faut concevoir le système d'exploitation du réseau, qui se situe dans la couche intermédiaire, à l'aide de techniques de virtualisation. Le système d'exploitation réseau doit être utilisé de manière à reconnaître la diversité des cas d'utilisation et des périphériques IoT. Les détails exacts de l'utilisation de la virtualisation dans la couche intermédiaire sont manquants, mais il convient de relier les techniques NFV à une logique d'orchestration SDN pour un réseau IoT.

- **l'informatique géo distribuée**

Le nuage a été utilisé comme support d'interopérabilité appelé Fog of Things [85], dans lequel les services d'informatique, de stockage et de réseau sont placés à la périphérie du réseau plutôt que sur des serveurs cloud centralisés, c'est-à-dire aussi près que possible du serveur. appareils de l'utilisateur final. Cela réduit la latence du réseau qui survient lors de la conversion des données brutes générées par les appareils mobiles et les capteurs soumis à des contraintes de ressources en instructions de connaissance ou explicatives. Le paradigme de l'informatique dans le brouillard valorise les données avant de les rendre disponibles sur le Web, ce qui facilite l'interopérabilité dans les environnements IoT, 5G, IA, Internet tactile, réalité virtuelle et autres applications complexes utilisant de nombreuses données et réseaux [86], et prépare les données gérées pour d'autres applications être interopérable [87]. L'informatique dans le brouillard assure l'interopérabilité des écosystèmes locaux dans le brouillard et également au niveau des nuages.

- **API ouverte**

L'API est une interface fournie par des fournisseurs de services qui expose des données ou des fonctions à une application écrite dans un langage évolué. Les API accessibles au public, destinées

à fournir une interopérabilité multi-plateforme et multi-domaine, se concentrent sur des API ouvertes et bien documentées qui offrent aux développeurs un accès simplifié aux fonctionnalités et aux services. Il existe de nombreuses API populaires telles que Google Maps, YouTube, Flickr, Twitter, Amazon et Facebook. Les plates-formes IoT actuelles fournissent presque toutes une API publique pour aider les développeurs à accéder à leurs services. Les API reposent généralement sur les principes RESTful et permettent des opérations courantes telles que PUT, GET, PUSH ou DELETE. Seules trois des plates-formes IoT étudiées n'incluaient pas d'API REST pour faciliter le développement de services Web (à savoir LinkSmart11, IFTTT et OpenIoT12), mais utilisaient des moyens d'interaction différents. Cependant, la majorité des fournisseurs de plate-formes IoT développent et déploient des API spécifiques à la plate-forme et propriétaires, qui reposent sur des modèles d'information internes pour définir la syntaxe d'opérations spécifiques à utiliser par leurs consommateurs. Par exemple, une application mobile peut proposer de contrôler votre réfrigérateur connecté à Internet. Il peut comporter des fonctionnalités telles que l'affichage des éléments à l'intérieur du réfrigérateur, la notification de la date de péremption des ingrédients ou le démarrage / l'arrêt d'une opération. Sans une API standard, si l'application mobile souhaite intégrer plus d'un fournisseur de réfrigérateurs, elle doit écrire un code personnalisé pour utiliser une autre API spécifique à la plate-forme, ce qui représente une charge considérable pour les développeurs d'applications. Cependant, une API standard permet une interopérabilité multiplateforme entre les solutions existantes avec un minimum de modifications de l'application. Avec le développement massif des fournisseurs de plates-formes IoT, un vaste silo d'API variées a été créé, ce qui augmente la difficulté de développement d'applications ainsi que les problèmes d'interopérabilité. Pour surmonter l'effet de l'hétérogénéité des API dans l'IoT, certaines plates-formes telles que ThingSpeak13 permettent la création de widgets écrits en Javascript, HTML et CSS qui peuvent être distribués sur la plate-forme à d'autres utilisateurs. HyperCat14 est une spécification qui fournit une interopérabilité syntaxique entre différents API et services basés sur un catalogue pouvant être étiquetés avec des métadonnées. Le catalogue contient de nombreuses ressources identifiées par son URI. De plus, les projets européens symbIoTe15 et Big-IoT16 travaillent sur une API d'interfonctionnement générique afin de fournir un accès uniforme aux ressources de toutes les plates-formes IoT existantes et futures afin de traiter l'interopérabilité syntaxique et multiplate-forme. L'API d'interfonctionnement se comporte comme un adaptateur qui doit être implémenté par d'autres plates-formes.

- **Architecture orientée service (SOA)**

Pour assurer une interopérabilité syntaxique entre des périphériques hétérogènes et sur tous les systèmes, les chercheurs ont proposé l'architecture SOA (Service Oriented Architecture) comme

technologie majeure de différentes manières [89]. La SOA est construite sur la couche réseau de sorte que le traitement des données et des informations puisse être facilement géré via différents composants de service [90]. Dans la SOA de l'IoT, les interactions et les opérations de différents périphériques sans fil sont classées en différents composants de service et le logiciel de couche d'application peut accéder aux ressources exposées par les périphériques en tant que services. Exposer les fonctionnalités de chaque composant en tant que service standard peut considérablement augmenter l'interopérabilité du réseau et des appareils. En particulier, la technologie de service Web a été proposée pour réaliser la promesse de la SOA d'un partage, d'une réutilisation et d'une interopérabilité de service optimaux [91]. Les approches classiques orientées services Web [89] et orientées ressources (services Web REST) [71, 72] ont été utilisées pour traiter l'interopérabilité syntaxique. Une étude menée par Pautasso et al [90] a comparé les services Web REST aux serveurs WS- * et a conclu que les services RESTful sont préférés pour l'intégration ad hoc ad hoc sur le Web, tandis que WS- * sont préférés pour les scénarios d'intégration d'applications d'entreprise professionnelles .

Une extension à la SOA appelée EDSOA (Event-Driven SoA) [91] a été proposée pour la construction de services IoT. L'architecture EDA (Eventdriven Architecture) est intégrée à la SOA pour composer les services IoT. La SOA divise l'application en plusieurs services indépendants décrits dans la spécification d'interface standard, tandis que l'EDA coordonne les services indépendants à l'aide de flux d'événements. Les auteurs se concentrent sur la construction d'un EDSOA évolutif qui pourrait utiliser les informations de ressources pour composer des services IoT, utiliser des événements indépendants et partagés pour exécuter ces services, puis utiliser des sessions d'événements pour coordonner les services.

- **Technologies du Web sémantique**

À l'origine, les technologies Web sémantique développées par le W3C, telles que RDF (Resource Description Framework), SPARQL et le langage d'ontologie Web (OWL) ont été utilisées pour décrire les ressources sur le Web. Actuellement, les mêmes normes sont utilisées dans de nombreux domaines, y compris l'IoT. Le paradigme du Web sémantique des objets (SWoT) [92] est proposé pour l'intégration du Web sémantique avec le WoT, afin de réaliser une compréhension commune des différentes entités qui forment l'IoT. Des recherches récentes ont conclu que les technologies du Web sémantique sont un facteur majeur d'interopérabilité dans des environnements hétérogènes [93]. La littérature utilise les technologies du Web sémantique pour réaliser l'interopérabilité sémantique en utilisant des normes ou des accords sur le format et la signification des données ou de manière dynamique en utilisant des vocabulaires partagés, sous forme de schéma et / ou selon une approche ontologique. Les ontologies (ou vocabulaires) dans l'IoT sont un ensemble d'objets et

de relations utilisés pour définir et représenter un domaine de préoccupation. Ils représentent une technologie d'abstraction qui vise à masquer l'hétérogénéité d'IoTentities, agissant en tant que médiateur entre le fournisseur d'applications IoT et les consommateurs, et à soutenir leur rapprochement sémantique [93]. De nombreuses ontologies ont été proposées dans le contexte de l'Internet des objets, telles que le réseau de capteurs sémantiques (SSN) du W3C [64], l'IoT-Ontology, SAREF et OpenIoT.

Une étude complète des ontologies existantes prêtes à être utilisées dans trois domaines différents: les ontologies IoT générales, la santé, le transport et la logistique peut être trouvée dans [93]. Ils décrivent également une approche utilisant des ontologies pour obtenir une interopérabilité sémantique entre des plates-formes IoT hétérogènes. Les auteurs estiment que l'ontologie SSN a été adoptée de la manière la plus forte et a inspiré d'autres projets. Cependant, aucun domaine n'a de standard ontologique global et la plupart des ontologies spécifiques à une application sont propriétaires.

Plusieurs projets de recherche IoT utilisant les capacités des ontologies ou d'autres technologies sémantiques susmentionnées pour améliorer l'interopérabilité sémantique, tels que Semantic Sensor Web (SSW) [94], OpenIoT, HYDRA17, SPITFIRE [80], SENSEI18, pour en nommer quelques-uns . Le SSW est l'une des premières études sur le concept sémantique d'IoT / WoT, généralement compris comme un mariage des technologies Sensor Web et Web sémantique. L'Open Geospatial Consortium (OGC) a développé SensorML19, qui n'est qu'un standard syntaxique pour l'activation Web de capteurs (SWE) utilisant des protocoles et des API basés sur XML, sans toutefois fournir d'interopérabilité sémantique ni de base de raisonnement. UbiROAD [95] réalise l'interopérabilité sémantique par deux couches : 1) interopérabilité des niveaux de données et 2) interopérabilité et coordination fonctionnelles au niveau du protocole. Serrano [96] discute des problèmes d'interopérabilité sémantique dans le contexte de l'IoT et présente la méthodologie SEG 3.0 pour fournir une interopérabilité sémantique entre applications hétérogènes. La méthodologie utilise les technologies du Web sémantique pour combiner des données hétérogènes IoT, ainsi que pour ajouter de la valeur aux données afin d'aider les développeurs et les praticiens de l'IoT à créer des applications IoT. Le cadre se compose de 12 couches qui se concentrent sur l'hétérogénéité des dispositifs, des réseaux de communication, des données, du raisonnement et des services. Les auteurs de [97] présentent l'idée de "détection en tant que service", dans laquelle les technologies de service standard sont utilisées comme interface représentant les ressources IoT (c'est-à-dire les dispositifs du monde physique) et permettent d'accéder aux fonctions et aux capacités de ces ressources. . Dans ce travail, un ensemble de modèles sémantiques pour les ressources, entités et

services IoT est présenté. Ces modèles sémantiques pour les descriptions de composants IoT offrent une interopérabilité au niveau des couches de données et de services.

- **Norme ouverte**

Les normes ouvertes constituent un moyen important d'assurer l'interopérabilité entre différents domaines. Une norme est un cadre de spécification qui a été approuvé par un organisme reconnu ou qui est généralement accepté et largement utilisé par l'ensemble du secteur [95]. À l'heure actuelle, plusieurs organismes, consortiums et alliances standard tentent de résoudre les problèmes liés aux normes IoT, notamment le consortium Open Interconnect Consortium (OIC) fournissant IoTivity20, AllSeen Alliance fournissant AllJoyn, oneM2M21, OMA LWM2M22 et ETSI M2M23. L'alliance IPSO est axée sur l'interopérabilité sémantique dans l'Internet des objets et la normalisation du modèle objet basé sur les ressources, basé sur des normes telles que SenML, CoAP et 6LoWPAN. Des structures telles que LWM2M et IoTvitiy fonctionnent avec l'alliance IPSO. L'IoTivity se concentre sur l'interopérabilité des périphériques, indépendamment du facteur de forme, du système d'exploitation ou du fournisseur de services, au travers de plug-in de protocole. Le framework AllJoyn fonctionne comme un bus logiciel entre périphériques facilitant l'interopérabilité des périphériques pour les applications de domotique et d'éclairage industriel. Les périphériques contraints utilisent une bibliothèque mince et n'ont pas de liaison de bus. Ce cadre introduit des frais généraux élevés pour les périphériques bas de gamme. Le cadre comprend également une base de code open source et divers services modulaires assurant l'interopérabilité. OneM2M permet une interopérabilité au niveau de la plate-forme en utilisant une couche de service horizontale pour les communications M2M et IoT, indépendante du réseau et offrant une interconnexion de réseaux à différents systèmes verticaux M2M existants. L'interopérabilité syntaxique et sémantique entre plates-formes est obtenue à l'aide d'ontologies.

1.6. Conclusion

L'amélioration de l'interopérabilité dans l'IoT est fondamentale pour son succès. Depuis l'émergence de l'IoT, de nombreuses propositions différentes se sont concentrés sur cette question cruciale. Les propositions sont diverses et promouvoir différentes approches. Ce chapitre prend ces travaux en compte et présente un aperçu complet du sujet. Ce faisant, la taxonomie de l'interopérabilité IoT a été identifié. De plus, nous avons étudié et classé les stratégies connexes pour gérer des types spécifiques d'interopérabilité. L'amélioration de l'interopérabilité dans l'IoT est fondamentale pour le succès de l'IoT. Depuis l'émergence de l'IoT, de nombreuses propositions différentes se sont concentrés sur cette question cruciale. Les propositions sont diverses et promouvoir différentes approches. Cet article prend ces travaux en compte et présente un aperçu complet du sujet. Ce

faisant, la taxonomie de l'interopérabilité IoT a été identifié. De plus, nous avons étudié et classé les stratégies connexes pour gérer des types spécifiques d'interopérabilité.

L'évolution future de l'IOT repose sur le développement d’un réseau qui supporte la communication M2M. Nous avons présenté un aperçu de la couche MAC et les limites dans les communications M2M.

Chapitre 2 : Conception d'un protocole MAC hybride pour les réseaux M2M hétérogènes

2.1. Introduction

Ce chapitre est consacré à la présentation du modèle de notre protocole MAC. D'abord nous présentons brièvement la structure de ce protocole, ensuite nous détaillons son fonctionnement et les hypothèses prises en compte. Enfin un problème d'optimisation est formulé pour déterminer les paramètres qui maximisent le débit global du système.

2.2. Les protocoles MAC sans fil :

La conception et le développement des protocoles MAC pour les environnements sans fil est un domaine riche qui a reçu une attention considérable dans la littérature existante. Les protocoles MAC existants peuvent être classés comme : à base de contention, sans contention ou hybrides qui combinent les deux aspects [34].

2.2.1. Les protocoles MAC à base de contention

Les protocoles MAC à base de contention sont parmi les protocoles les plus simples en termes de configuration et de mise en œuvre. Dans ces protocoles, les nœuds contestent le canal de diverses manières dans le but d'acquérir le canal et transmettre des données. Le principal inconvénient de ces protocoles est le manque d'évolutivité, notamment en raison de l'augmentation du nombre de collisions par la transmission simultanée de différents nœuds comme le nombre de nœuds augmentent.

a) Exemples des protocoles à base de contention.

Dans les protocoles d'accès aléatoires tels que ALOHA et slotted-ALOHA, les nœuds qui ont des données à envoyer, transmettent le paquet dès qu'il arrive, ou l'envoient au début de la prochaine période, respectivement [22]. Le principal inconvénient de ces protocoles est le taux élevé de collisions, ce qui limite les valeurs de débit asymptotique à 18% et 36%, de la bande passante du canal, respectivement [22].

Les protocoles CSMA représentent une étape vers la réduction des collisions subies par les protocoles de type ALOHA [22]. CSMA ne supprime pas les collisions et peut subir une dégradation de débit en raison des problèmes des terminaux cachés et exposés. Le problème de terminal caché peut être résolu par l'utilisation des tonalités d'occupation où les émetteurs et / ou récepteurs sont obligés de transmettre une tonalité constante occupée pendant qu'un paquet est transmis ou reçu.

Les solutions du canal unique pour réduire le problème de terminal caché sont principalement basées sur le protocole MACA.

L'un des protocoles d'accès aléatoire le plus largement déployé est IEEE 802.11, il est basée sur CSMA avec évitement de collision (CSMA / CA) [22]. La performance de la norme IEEE 802.11 a été largement étudiée [98], [99]. Bien que le protocole fonctionne bien pour les petites tailles de réseau, comme le nombre de nœuds actifs augmente, ses performances en termes de délai et de débit se dégradent rapidement, surtout lorsque la charge de chaque nœud s'approche de la saturation.

b) La communication M2M et les protocoles à base de contention

Les protocoles MAC à base de contention sont largement inadaptées pour les communications M2M en raison des collisions et de la mauvaise performance résultante quand la charge du nœud augmente (exemple CSMA et ALOHA) [59].

Les protocoles à base de tonalité occupée tels que DBTMA [12] offrent une meilleure performance. Toutefois, cela se fait par du coût supplémentaire du matériel et de la complexité (deux émetteurs radio et l'exigence de bande passante pour la tonalité d'occupation) qui limite son applicabilité pour les dispositifs M2M à faible coût.

Les protocoles basés sur CSMA/CA tels qu'IEEE 802.11 sont parmi les protocoles MAC les plus largement déployés. Cependant, leur capacité à satisfaire les exigences de la communication M2M est à discuter. Cela est principalement dû à leur incapacité de changement d'échelle à mesure que la taille du réseau augmente. D'autres préoccupations sont l'énergie gaspillée par des protocoles basés sur CSMA/CA en raison des collisions, et les frais généraux des paquets de contrôle, qui peuvent consommer plus d'énergie que les paquets de données (à cause des probabilités de collision plus élevées pour les paquets de contrôle) [100].

2.2.2. Les protocoles MAC sans contention

Les protocoles sans contention éliminent le problème de collision par pré-allocation des ressources de transmission aux nœuds du réseau. Les protocoles sans contention communs incluent le TDMA, CDMA et FDMA. Dans FDMA, une fraction de la largeur de bande de fréquences est attribuée à chaque utilisateur tout le temps, alors que dans TDMA, la totalité de la bande passante est allouée à un utilisateur pour une fraction de temps [22]. CDMA fonctionne en assignant des codes orthogonaux à chaque utilisateur, qui sont ensuite utilisés pour moduler les motifs de bits [22], [41].

Les protocoles sans contention dynamiques proposés dans la littérature sont principalement à base de TDMA. Les protocoles TDMA dynamiques sont principalement basés sur la réallocation de périodes ou sur l'adaptation du nombre de périodes, en fonction du nombre de nœuds actifs et de leur intensité de trafic.

L’avantage principal des protocoles sans contention est la meilleure utilisation du canal à des charges élevées. Toutefois, l'utilisation se baisse à faible charge, les protocoles sont difficiles à adapter, lorsque le nombre de nœuds dans le réseau varie, et ont généralement des exigences strictes sur le matériel. Dans le contexte des communications M2M, les inconvénients dépassent les avantages et il est difficile pour les protocoles sans contention de fournir la flexibilité et l'évolutivité qui est souhaitée dans ces scénarios.

Les protocoles sans contention qui adaptent dynamiquement leur fonctionnement selon les conditions du réseau sont mieux adaptés pour les réseaux avec variabilité (en termes de trafic et de nœuds actifs). Cependant, la facilitation du fonctionnement dynamique exige des frais généraux supplémentaires qui limitent l'amélioration globale. Par exemple, dans des protocoles TDMA dynamiques tels que FPRP [99], NAMA [103], et leurs dérivés, des collisions peuvent se produire au cours de certaines étapes de leur fonctionnement, ce qui limite leur applicabilité dans les scénarios avec une forte densité des nœuds.

Les protocoles basés sur CDMA ne sont pas adaptés pour les dispositifs M2M à faible coût, essentiellement à cause de leur complexité [59]. La communication basée sur CDMA exige un contrôle de puissance stricte. La nécessité de contrôle de puissance impose des exigences de calcul et de matériel qui augmentent le coût global du système. En outre, CDMA nécessite des opérations de calcul coûteuses pour les messages de codage et de décodage, ce qui les rend moins appropriés pour les réseaux où les dispositifs manquent de matériel spécial et qui ont une puissance de calcul limitée.

Par rapport à TDMA et CDMA, FDMA est moins approprié pour le fonctionnement avec des appareils à faible coût. La première raison est que les nœuds compatibles avec FDMA nécessitent des circuits supplémentaires pour communiquer et basculer entre les différents canaux. Les filtres passe-bande complexes nécessaires à cette opération sont relativement coûteux. Un autre inconvénient de FDMA qui limite son utilisation pratique est l'exigence de linéarité assez stricte sur le support.

2.2.2. Les protocoles MAC hybrides

Les protocoles basés sur la contention s’adaptent facilement à l'évolution des scénarios de réseau et sont mieux adaptés pour les réseaux avec faibles charges. D'autre part, les protocoles sans contention éliminent les collisions et ont une meilleure utilisation des canaux à des charges plus élevées. Pour exploiter les avantages des deux classes de protocoles, des protocoles hybrides ont été proposés qui combinent les aspects des protocoles basés sur contention et sans contention.

a) Les protocoles hybrides : TDMA/FDMA/CDMA avec contention

Les protocoles MAC hybrides proposés dans la littérature combinent généralement des éléments de type CSMA avec TDMA, FDMA et CDMA. Les protocoles qui combinent TDMA et CSMA tels que [104] et [105] se comportent comme CSMA à des niveaux de trafic faibles et passent à un fonctionnement de type TDMA à des niveaux de trafic élevés.

Des protocoles tel que le protocole Hymac (hybrid MAC) proposé dans [106], combinent CSMA avec TDMA et FDMA dans lequel les nœuds se sont attribués une fréquence et un intervalle de temps pour transmettre des données une fois qu'ils envoient une demande de bande passante avec succès en utilisant une transmission à base de contention.

b) Les protocoles hybrides et la communication M2M

Les protocoles hybrides résolvent certains des problèmes de performance qui se posent avec les protocoles basés sur contention et sans contention. Les protocoles qui passent entre l'opération sur la base d'accès aléatoire à faible charge et l'accès planifié à des charges élevées, évitent le débit dégradé et les collisions des protocoles d'accès aléatoires à des charges élevées et la faible utilisation des canaux d'accès planifié à faibles charges. Par conséquent, les protocoles hybrides sont une approche prometteuse pour la conception de protocoles MAC pour les communications M2M [59].

Le principal inconvénient des protocoles hybrides qui a été proposé dans le contexte des réseaux ad-hoc sans fil et les réseaux de capteurs est leur évolutivité. De nombreux scénarios avec les communications M2M ont des densités de nœuds qui sont d'un ordre de grandeur plus important que les réseaux sans fil actuellement déployés. Avec une telle densité élevée, l'incidence des collisions au cours de l'accès aléatoire devient l'obstacle qui empêche le réseau d'atteindre un taux d'utilisation élevé [59].

Les protocoles hybrides basés sur FDMA et CDMA ont une meilleure évolutivité que le pur FDMA et CDMA. Cependant, l'inconvénient de FDMA en termes de l'exigence de matériel coûteux et de CDMA pour un fonctionnement complexe et la nécessité d'un contrôle de puissance résident encore. Par conséquent, les protocoles hybrides à base de TDMA sont les plus prometteurs des protocoles hybrides dans le cadre des communications M2M [59].

2.3. Les protocoles MAC spécifiques à la communication M2M

Afin de répondre aux exigences uniques des communications M2M, une approche intuitive est d'élaborer des protocoles MAC spécifiques à ces environnements. Des recherches récentes le long de ces lignes ont proposé divers protocoles. Une taxonomie des protocoles étudiés dans cette

section est représentée sur la figure 2.1 et leur comparaison en termes de besoins de communication M2M est donnée dans le tableau 2.1.

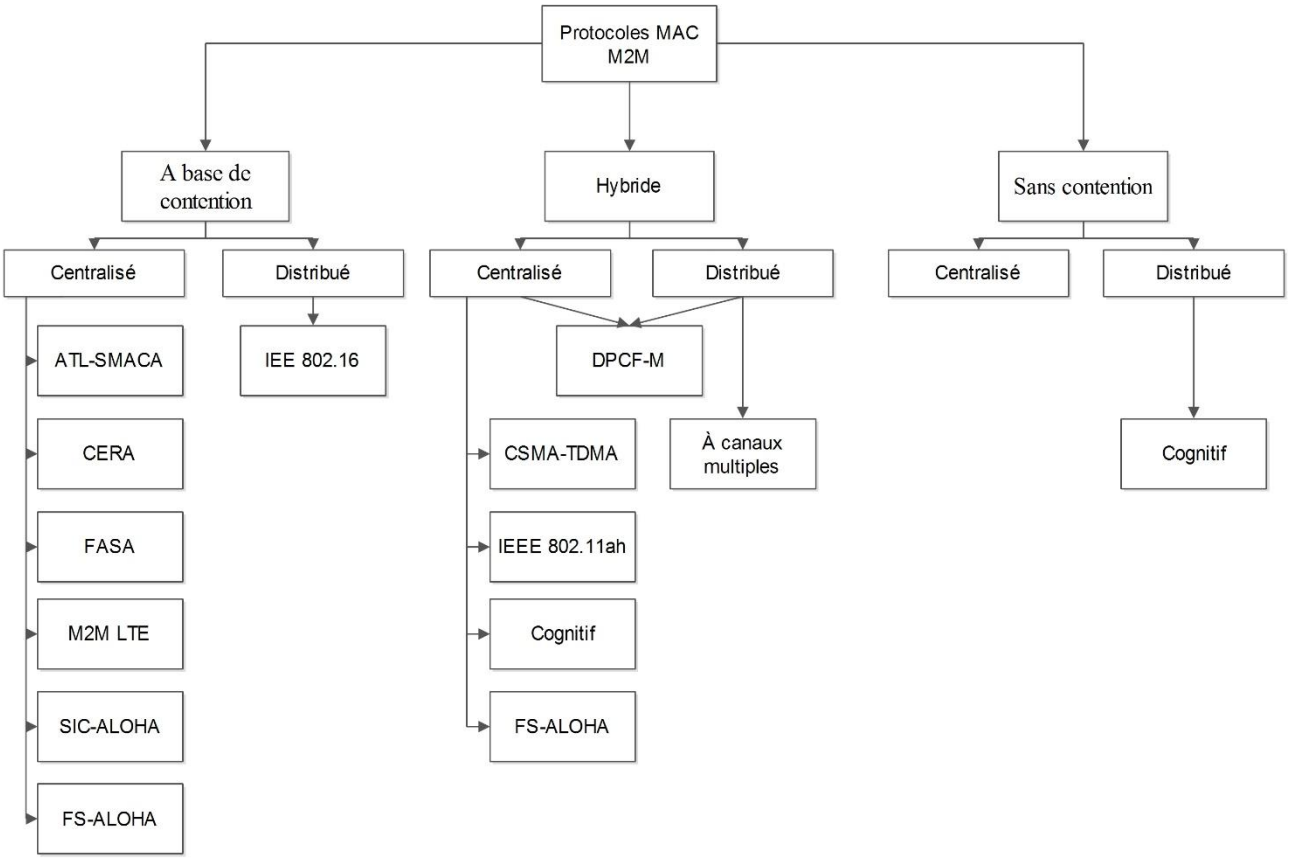


Figure 2.1 *Taxonomie des Protocoles MAC [56]*

Tableau 2.1 *Comparaison des protocoles MAC spécifiques à la communication M2M*

Protocoles	Débit de données	Extensibilité	efficacité énergétique	Latence	Rentabilité
DPCF-M [53]	Modéré	Modérée	Modérée	Modérée	Faible
MAC Hybride Evolutif [108] [109]	Modéré	Modérée	Modérée	Faible	Faible
protocole Adaptatif multi canal [107]	Modéré	Modérée	Faible	Haute	Faible
ATL-SMACA [114]	Faible	Faible	Faible	Haute	Faible
CERA [115]	Haut	Modérée	Modérée	Faible	Haute
IEEE 802.11 [116]	Haute	Haute	Modérée	Modérée	Faible
FASA [117]	Faible	Faible	Faible	Haute	Faible
M2M LTE [118]	Modéré	Faible	Modérée	Modérée	Haute
M2M LTE [119]	Haut	Modérée	Modérée	Modérée	Haute
Cognitif [120]	Haut	Modérée	Modérée	Modérée	Haute
Cognitif avec réservation [121]	Modéré	Faible	Haute	Haute	Haute

2.4. Le protocole proposé

Dans ce chapitre, on propose un protocole MAC hybride qui combine les avantages des protocoles à base de contention et des protocoles sans contention. Tout d'abord on divise le trafic en Q classes selon la priorité d'envoi de paquets. Dans ce protocole on suppose qu'un canal dédié a été assigné pour les communications M2M et que la communication est entre les machines et le serveur. Nous considérons uniquement les communications de liaison montante et proposons un protocole MAC hybride qui fournit à la fois des communications basées sur la contention et la réservation. Le protocole divise le temps en cycles et chaque cycle se compose de trois périodes : 1) période de notification (NP) ; 2) période de contention (COP) et 3) la période de transmission (TOP), comme représenté sur la Figure 2.2.

Chaque cycle commence par une NP où la station de base (BS) annonce le début de COP à tous les nœuds. Au cours de COP, des nœuds qui ont des données à transmettre utilisent CSMA p-persistant pour envoyer des demandes de transmission à la BS. Les nœuds qui réussissent se sont attribués une

période pour transmettre des données dans la TOP et les nœuds sont informés de leurs créneaux de transmission en recevant un ACK de la part de BS.

Nous avons utilisé TDMA pour l'accès au canal sans contention et CSMA/CA pour l'accès avec contention.

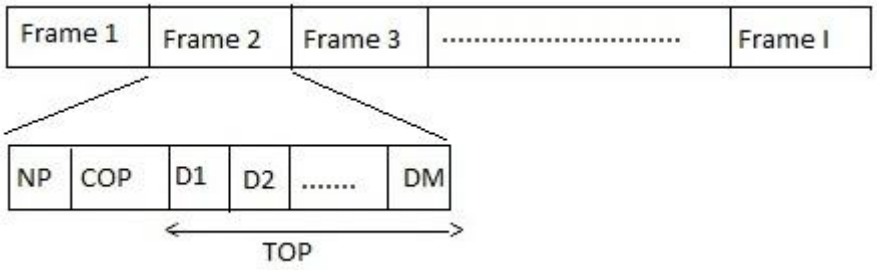


Figure 2.2 *Structure du protocole MAC hybride*

2.5. Modèle du réseau M2M

Comme représenté sur la figure 2.3, On considère un réseau M2M hétérogène qui se compose d'une station de base BS et de k dispositifs $\{D_1,\ldots,D_k\}$. Dans ce réseau, il y a L dispositifs qui ont des données à transmettre pendant un cycle et par conséquent K-L appareils silencieux qui peuvent entrer en mode de veille pour ne pas consommer de l'énergie. Dans notre système, les différents types de dispositifs sont classés dans Q classes de priorité $\{C_1,\ldots,C_Q\}$, chacune a K_q , $\{q=1,\ldots,Q\}$ dispositifs et $K=\sum_{q=1}^{Q} Kq$. Nous supposons que les classes supérieures des dispositifs ont des exigences plus élevées en matière de performances de transmission, telles qu'une utilisation du canal plus élevée et un taux de perte des paquets inférieur à celui des classes inférieures de périphériques.

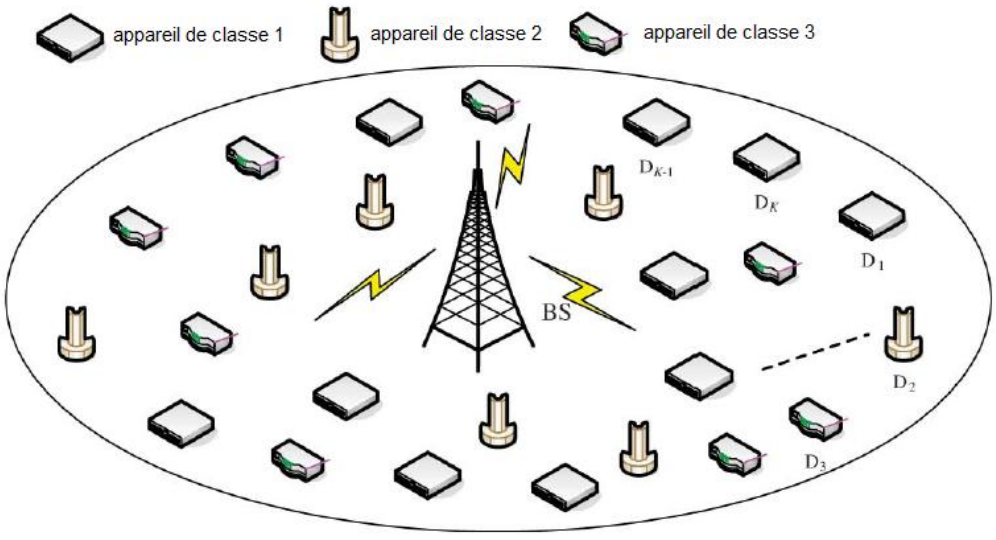


Figure 2.3 *Modèle de réseau M2M.*

BS est responsable de l'exploitation de MAC pour les différentes classes de dispositifs actifs (les dispositifs qui ont un paquet à transmettre) en attribuant différentes probabilités de contention $\{p_1,\ldots,p_q\}$ à la classe $\{C_1,\ldots,C_Q\}$, respectivement. Nous supposons que le dispositif ayant une priorité supérieure a une probabilité de contention plus élevée que celle avec une priorité inférieure, c.à.d, $\{p_1<p_2<\ldots.<p_Q\}$. Nous supposons que les probabilités de contention p_q, $\{q=1,\ldots,Q\}$ ont la relation comme suit :

$$p_q=\max\{\ 1, (1+\alpha)^{q-1}\, p_1\ \},\quad 0 \le p_1 \le\ 1 \qquad (2.1)$$

Où α est définie comme l'indicateur d'incrémentation.

Pour chaque dispositif actif, le processus d'arrivée des paquets de données est modélisé en tant que processus d'arrivée Poisson avec taux d'arrivée de paquets λ.

Tableau 2.2 *Caractéristiques des trois protocoles CSMA*

Protocol CSMA	**Mode de transmission**
Non-persistant	1. Si le médium est libre, transmettre. 2. Si le médium est occupé, attendre un délai aléatoire et répéter l'étape 1.
1-persistant	1. Si le médium est libre, transmettre. 2. Si le medium est occupé, continuer l'écoute jusqu'à ce que le canal soit libre ; puis transmettre immédiatement. 3. S'il y a collision, la station attend pendant un délai aléatoire et répète l'étape 1.
p-persistant	1. Si le médium est libre, transmettre avec une probabilité *p*. 2. Si le médium est occupé, continuer l'écoute jusqu'à ce que le canal soit libre et transmettre avec la même probabilité p ; 3. En cas de collision, la station attend un temps aléatoire avant de recommencer la procédure.

Nous supposons que tous les appareils ont le même taux d'arrivée de paquets, qui est connu par la BS. Un nouveau paquet qui arrive à un dispositif est mis en tampon jusqu'à ce que le périphérique conteste avec succès l'opportunité de transmission et finisse la transmission. Si un nouveau paquet arrive à l'appareil avant la transmission, le paquet tampon sera remplacé par le nouveau. Par conséquent, il existe un paquet au maximum dans la mémoire tampon de chaque dispositif. Nous considérons le fonctionnement du réseau M2M sur une base cycle par cycle. Chaque période est composée de trois parties, comme représenté sur la figure 2.2: période de notification NP, période de contention COP et période de transmission TOP. Pendant NP, le BS diffuse un message de notification à tous les périphériques pour annoncer le début de la contention. Les périphériques

actifs contesteront le canal pendant COP. La COP est basé sur la méthode d'accès CSMA p-persistant [22], et est utilisé pour que les périphériques envoient de manière aléatoire la demande de transmission à BS. Après COP, les dispositifs qui ont réussi à la contention ont la permission de transmettre des paquets pendant le temps restant d'un cycle, qui est spécifié comme TOP. Le TOP fournit un type de communication TDMA pour les appareils. Nous supposons que tous les créneaux de transmission assignés ont la même longueur et qu'il n'y a pas d'erreur de transmission pour chaque appareil [113], [114].

2.5.1. Fonctionnement

a) Période de notification

Au début de chaque cycle, la BS diffuse un message de notification pour tous les dispositifs afin de notifier le début de la contention. Lors de la réception du message de notification, les dispositifs actifs se préparent à contester les créneaux de temps de transmission. Les autres dispositifs qui n'ont pas de paquets à envoyer entrent en mode veille pour préserver l'énergie. En connaissant le taux d'arrivée des paquets de chaque appareil, la BS estime le nombre de dispositifs actifs et calcule les paramètres de contention optimaux : durée de contention, probabilité de contention initiale et indicateur incrémental en résolvant un problème d'optimisation. Ces paramètres sont inclus dans le message de notification et diffusés par la BS pendant NP. Lors de la réception du message de notification, les dispositifs actifs calculent leurs propres probabilités. Le calcul est basé sur un mécanisme de priorité incrémental. Ensuite, le réseau M2M entre en COP.

b) Période de contention

Dans cette période, les dispositifs contestent les possibilités de transmission en se basant sur le mécanisme CSMA p-persistant, selon leurs propres probabilités de contention. Les dispositifs envoient de manière aléatoire le message de demande de transmission (Tran-REQ) à la BS. La contention est déclarée comme un succès uniquement lorsqu'un seul périphérique envoie le message Tran-REQ. Lorsque plus qu'un périphérique envoie Tran-REQ pendant le même créneau, une collision se produit. La période de repos est un intervalle de temps dans lequel la contention ne se produit pas. Sous le mécanisme CSMA p-persistant, la période de réussite et la période de collision peuvent être données comme :

$$\delta_{coll} = BIFS + T_{req} \quad (2.2)$$

$$\delta_{succ} = T_{req} + SIFS + T_{ACK} + BIFS \quad (2.3)$$

avec T_{req} est la longueur de Tran-REQ, T_{ACK} la durée de l'accusé de réception, et BIFS et SIFS sont respectivement le Backoff inter-frame space et le short inter-frame space. Figure 2.4 présentes le fonctionnement du mécanisme CSMA/CA.

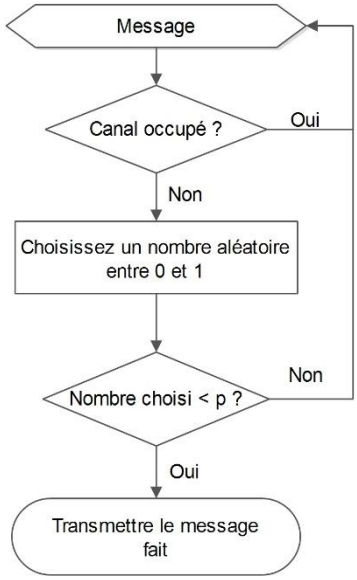


Figure 2.4 *Le mécanisme CSMA/CA*

Lors de la réception du message ACK de la part de BS, l'appareil arrêtera d'envoyer le message Tran-REQ et attend le début de la TOP. En outre, le message ACK inclut l'information de l'index du créneau temporel de transmission pendant lequel le périphérique est autorisé à transmettre en TOP.
Si un message Tran-REQ est reçu avec succès à partir d'un périphérique, la BS envoie un message ACK et l'index du créneau de transmission à ce périphérique. Pour une période de contention optimale donnée $T_{COP,opt}$, nous pouvons avoir un nombre de périphériques qui réussissent la contention plus grand que celui qui est autorisé pour un cycle donné (le nombre attendu de périphériques réussis pendant $T_{COP,opt}$ est désigné comme M_{opt}). Par conséquent, $T_{COP,opt}$ et M_{opt} sont utilisés comme deux seuils pour contrôler la durée de COP en pratique comme dans la figure 2.5. Lorsque le nombre réel de périphériques réussis dans la contention est supérieur à M_{opt} ou la T_{COP} est supérieur à $T_{COP,opt}$, la BS arrête la COP et déclare la prochaine période.

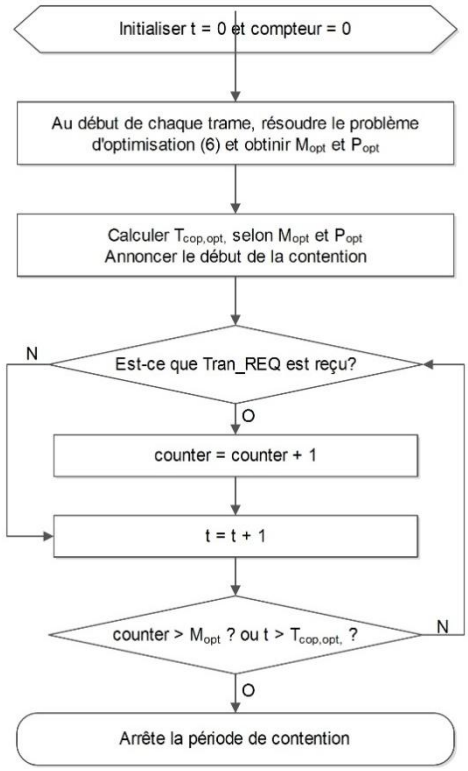


Figure 2.5 *L'organigramme du schéma à deux seuils.*

c) Période de transmission

Les dispositifs actifs qui ont réussi la contention transmettent séquentiellement suivant le mécanisme TDMA (figure 2.6). Ces appareils allument leurs modules radio et transmettent le paquet de données lors de leurs propres créneaux de temps de transmission. Les périphériques éteignent le module radio à d'autres intervalles de temps. Lorsque la minuterie de TOP est éteinte, la BS déclare le début d'un nouveau cycle.

On s'attend à ce qu'un plus grand nombre de périphériques aient réussi la contention si la T_{COP} est plus longue. Cependant, en tenant compte de la durée d'un cycle T_{frame}, le T_{TOP} diminuera à mesure que la T_{COP} augmentera, ce qui peut réduire le temps total de transmission. Par conséquent, il existe un compromis entre les durées de COP et TOP. Pour équilibrer ce compromis, nous avons l'intention de proposer un système hybride de contrôle d'accès, qui met l'accent sur l'obtention de T_{COP}, P_{inl}, M et α Optimaux, pour maximiser le débit global.

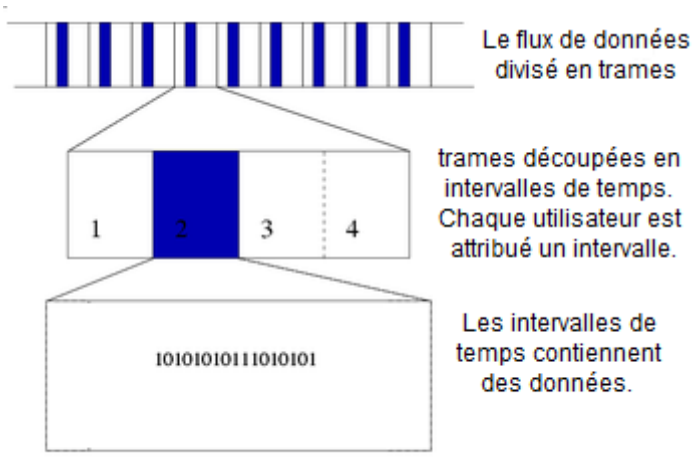


Figure 2.6 *Structure du protocole TDMA*

2.5.2. Mécanisme de priorité croissante

Selon le mécanisme CSMA p-persistant, les périphériques peuvent échouer dans la contention pendant COP et perdre les possibilités de transmission pendant TOP. Si un périphérique échoue fréquemment dans la contention, ses performances de transmission se dégraderont. Par conséquent, nous proposons un modèle de priorité croissante. Dans ce modèle, nous augmentons la probabilité de contention du périphérique si un tel dispositif n'a pas contesté les possibilités de transmission dans les cycles précédents. Lorsque le périphérique transmet avec succès un paquet de données, le processus croissant sera arrêté et la priorité de l'appareil revient au niveau préliminaire. Pour les appareils de type q qui ont une nouvelle arrivée de paquets, la BS attribue la probabilité de contention préliminaire p_q. Si les périphériques de type q ont échoué dans la contention pendant les cycles précédente, la BS augmentera leurs probabilités de contention pendant le cycle actuel selon

$$p_{q,d} = \max\{\, 1, (1+\alpha)^d p_q \,\}, \quad 0 \le p_q \le 1 \qquad (2.4)$$

avec d = 0,1,2,… le nombre de cycles pendant lesquels les dispositifs ont échoué à la contention et α l'indicateur incrémental.

On suppose que la probabilité de contention définie dans (2.1) et (2.4) a le même indicateur α.

Par conséquent, nous notons qu'il pourrait y avoir plus d'une classe de périphériques qui ont les mêmes probabilités de contentions dans un certain laps de temps. On définit la classe virtuelle ϱ, {ϱ=1,…,Q} dans laquelle les dispositifs, à un certain cycle, ont la même probabilité de contention $p_ϱ$. Alors, on a

$$p_ϱ = \max\{\, 1, (1+\alpha)^ϱ p_{inl} \,\}, \quad 0 \le p_{inl} \le 1$$
$$\text{avec } p_{inl} = p_1 \text{ et } ϱ = q+d-1,\ \{q=1,\ldots,Q,\ d=0,1,2,\ldots\} \qquad (2.5)$$

2.6. Exemple illustratif

Un exemple d'utilisation du protocole proposé est illustré dans la Figure 2.7, nous avons considéré les opérations d'accès hybrides de huit dispositifs. Pour décrire clairement notre protocole, nous considérons un seul type de classe de priorité dans l'exemple, c'est-à-dire, q=1, puis, ϱ = d, {d = 0,1,2,…} .Le fonctionnement de chaque dispositif dans le réseau M2M comprend deux processus : 1) processus de contention et de transmission et 2) processus d'arrivée des nouveaux paquets. Dans le cycle 0, il n'y a pas de processus de contention et de transmission pour tous les appareils. Nous pouvons voir que les dispositifs actifs sont D_1, D_2, D_5, et D_7 à la fin du cycle 0. Notez que pendant ce cycle, D_2 a deux arrivées de paquets et le premier paquet arrivé sera remplacé par le dernier. Dans le cycle 1, D_1, D_2, D_5 et D_7 font partie de la contention avec la probabilité de contention p_1. D_1 et D_2 qui ont réussi dans la contention sont autorisés à transmettre des données au cours du TOP suivante. D_5 et D_7, qui ont échoué dans la contention, devraient de nouveau attendre la contention dans le cycle suivant. Entre-temps, leurs probabilités de contention augmentent de p_1 à p_2, où $p_2 = (1 + \alpha)\, p_1$. En outre, nous pouvons voir que D_2, D_3, D_4, D_5 et D_8 ont une nouvelle arrivée de paquet dans le cycle 1. Par conséquent, les dispositifs qui sont concernés par la contention dans le cycle 2 sont D_2, D_3, D_4, D_5, D_7 et D_8 où la probabilité de contention de D_5 et D_7 est p_2 et celle du reste des appareils est p_1. Après le cycle 2, nous pouvons voir que D_7 a échoué dans la contention de nouveau et sa probabilité de contention p2 augmente à p_3, où $p_3 = (1 + \alpha)\, p_2$.

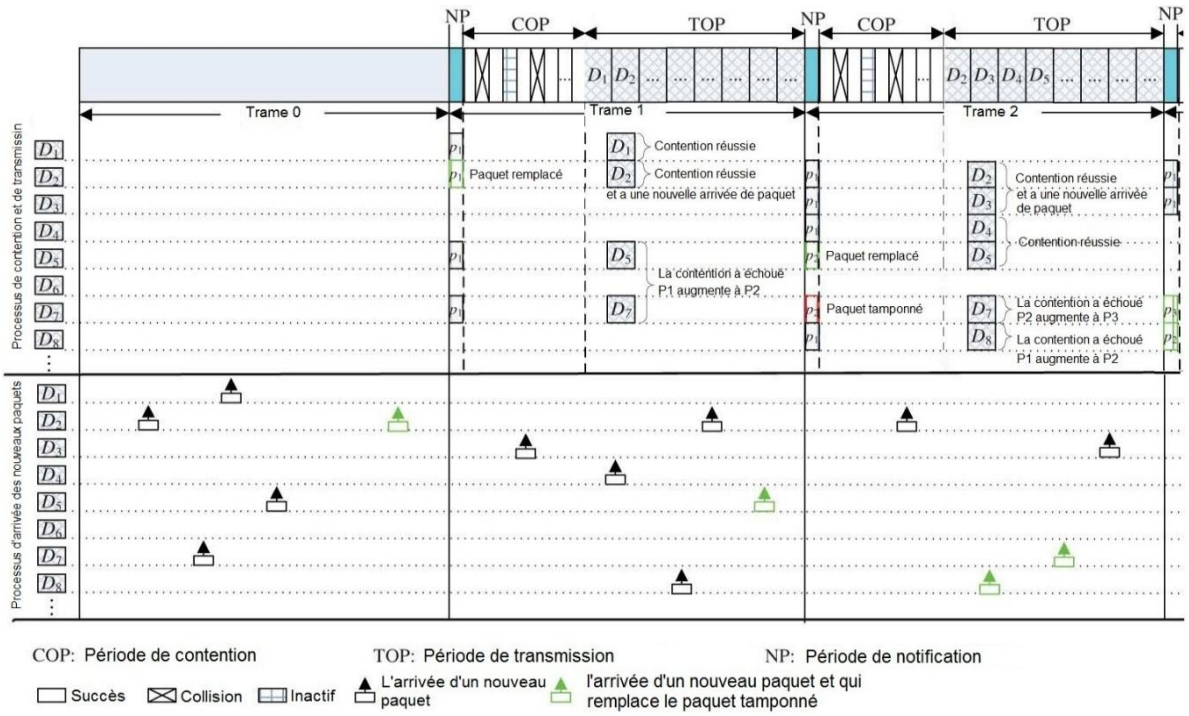


Figure 2.7 *Processus d'accès hybride*

2.7. Dérivation de Tcop

Selon notre protocole MAC proposé, les dispositifs actifs dans la classe virtuelle ϱ ont la probabilité de contention $p_ϱ$ et contestent les créneaux de transmission pendant COP. Pour obtenir l'expression de T_{COP}, nous avons besoin de connaître le temps de contention moyen de chaque appareil. Premièrement, nous faisons les hypothèses et les notations suivantes :

1) Le taux d'arrivée de paquet (λ) et la durée de chaque cycle (T_{frame}) sont constants.
2) Pour un cycle i, {i=1,2,…,I}, il y a Θ classes virtuelles de dispositifs, chacune contient $N_ϱ^{(i)}$ dispositifs ($1 \leq ϱ \leq Θ$), avec

$$N_ϱ^{(i)} = N_{ϱ-1}^{(i-1)} - M_{ϱ-1}^{(i-1)} + U_ϱ^{(i-1)},\ M_{ϱ-1}^{(i-1)} \tag{2.6}$$

$M_{ϱ-1}^{(i-1)}$est le nombre de dispositifs de la (ϱ-1)ème classe qui ont réussi la contention dans le (i-1)ème cycle, $U_ϱ^{(i-1)}$ est le nombre de dispositifs de la classe ϱ qui ont une nouvelle arrivée de paquet dans le (i-1)ème cycle.

3) Un dispositif de la classe ϱ utilise la probabilité $p_ϱ = (1+α)^ϱ\ p_{inl}$ dans le CSMA p-persistant ($0 \leq p_{inl} \leq 1$, $α > 0$) pour contester les opportunités de transmission [52].

Basé sur CSMA p-persistant dans la COP, lorsqu'une tentative de contention est terminée (avec succès ou avec collision), le dispositif actif démarrera une nouvelle tentative de contention avec une probabilité $p_ϱ$, ϱ =1,…,Θ. Ici, nous définissons la contention réussie comme l'événement que la demande de transmission d'un périphérique a été reçue avec succès par BS. Soit t_i le temps entre la (i-1)ième et la iième contention réussie. Soit N_i^c le nombre de collisions qui se produisent pendant t_i, alors

$$t_i = \sum_{j=1}^{N_{m,i}^c} [Idle_{i,j} + Coll_{i,j}] + Idle_{N_i^c+1} + S_i \tag{2.7}$$

Avec $Idle_j$ la durée du jème temps de repos qui précède la période d'occupation du canal (collision ou réussite) pendant chaque t_i, $Coll_{i,j}$ la durée du jème collision sachant qu'une collision se produit, et S_i la longueur du message de requête. Soit T_{cop} la durée de COP pendant chaque cycle. Alors, on a :

$$T_{COP} = \sum_{m=1}^{M(i)} t_i \tag{2.8}$$

$$T_{COP} = \sum_{m=1}^{M(i)} \{\sum_{j=1}^{N_{m,i}^c} [Idle_{i,j} + Coll_{i,j}] + Idle_{N_i^c+1} + S_i\} \tag{2.9}$$

Puisque $T_{COP,i}$ est la somme de variables aléatoires t_m, (m = 1,…, $M^{(i)}$), $T_{COP,i}$ est aussi une variable aléatoire avec $E[T_{COP,i}]$ le temps moyen pour $M^{(i)}$ contentions réussies. Pour obtenir l'expression

rapprochée de $T_{COP,i}$, Nous nous concentrons alors sur la dérivation de la valeur attendue de $T_{COP,i}$ désignée par $E[T_{COP,i}]$. on a

$$E[T_{COP,i}] = \sum_{i=1}^{M} E[t_i]$$

$$E[T_{COP,i}] = \sum_{i=1}^{M} \{ (E[N_i^c]+1)) E[Idle_i]+ E[N_i^c] E[Coll_i] + E[S_i] \} \quad (2.10)$$

Avec $[N_i^c]$, $E[Idle_i]$, $E[Coll_i]$ et $E[S_i]$ sont le nombre moyen de collisions, la durée moyenne d'un temps de repos, d'une collision et un message requête à un cycle i, respectivement.

Puis, on dérive $E[N_i^c]$, $E[Idle_i]$ et $E[Coll_i]$ dans le cas de classes de priorité multiple.

- **Dérivation de $E[N_i^c]$:**

Soit N_{cd} le nombre de dispositifs en contention dans un créneau de contention immédiatement après une période de repos, soit $P_{collision}$ et $P_{success}$, respectivement la probabilité qu'une collision se produit et qu'une transmission est réussie, les deux conditionnées par le fait qu'au moins un périphérique envoi le message de contention. Alors,

$$P_{collision} = P (N_{cd} \geq 2 \mid N_{cd} \geq 1)$$

$$= \frac{1-P(Ncd=0)- P(Ncd=1)}{1-P(Ncd=0)}$$

$$= 1 - \frac{\sum_{\varrho=1}^{\mathcal{O}} N_\varrho^{(i)} (1- p\varrho)^{N_\varrho^{(i)}-1} \prod_{\varrho \neq l} (1- pl)^{N_l^{(i)}}}{1- \prod_{i=\varrho}^{\mathcal{O}} (1- p\varrho)^{N_\varrho^{(i)}}} \quad (2.11)$$

Et

$$P_{success} = P (N_{cd} = 1 \mid N_{cd} \geq 1)$$

$$= \frac{\sum_{i=\varrho}^{\mathcal{O}} N_\varrho^{(i)} (1- p\varrho)^{N_\varrho^{(i)}-1} \prod_{\varrho \neq l} (1- pl)^{N_l^{(i)}}}{1- \prod_{\varrho=1}^{\mathcal{O}} (1- p\varrho)^{N_\varrho^{(i)}}} \quad (2.12)$$

La distribution de probabilité de N_i^c peut être exprimée comme

$$P(N_i^c = l) = P_{collision}^{l} P_{success} \quad (2.13)$$

Et $E[N_i^c]$ peut être obtenue comme

$$E[N_i^c] = \sum_{\varrho=1}^{\mathcal{O}} \varrho P(N_i^c = \varrho)$$

$$= \frac{1- \prod_{\varrho=1}^{\mathcal{O}} (1- p\varrho)^{N_\varrho^{(i)}}}{\sum_{\varrho=1}^{\mathcal{O}} N_\varrho^{(i)} (1- p\varrho)^{N_\varrho^{(i)}-1} \prod_{\varrho \neq l} (1- pl)^{N_l^{(i)}}} \quad (2.14)$$

- **Dérivation de E[Idle$_i$] :**

Puisque les dispositifs de la classe ϱ peuvent contester dans un créneau temporel avec la probabilité $p_ϱ$, on a

$$E[Idle_i] = \delta_{idle} \sum_{\varrho=1}^{\mathcal{O}} \varrho P(N_{cd} \geq 0)\,(P(N_{cd} = 0))^{\varrho}$$

$$= \delta_{idle} \frac{\prod_{\varrho=1}^{\mathcal{O}}(1-p\varrho)^{N_\varrho^{(i)}}}{1-\prod_{\varrho=1}^{\mathcal{O}}(1-p\varrho)^{N_\varrho^{(i)}}} \tag{2.15}$$

Avec δ_{idle} constante [52].

Soit $\delta_{coll} = E[coll_i]$ et $\delta_{succ} = E[S_i]$. alors, $E[T_{COP,i}]$ est fonction de $M^{(i)}$ et $p_ϱ$. Soit $T_{COP}^{(i)}(M^{(i)},p_ϱ)=E[T_{COP,i}]$, finalement :

$$T_{COP}^{(i)}(M^{(i)},p_ϱ)= M^{(i)}\left\{\begin{array}{c} \delta idle \dfrac{\prod_{\varrho=1}^{\mathcal{O}}(1-p\varrho)^{N_\varrho^{(i)}}}{\sum_{\varrho=1}^{\mathcal{O}} N_\varrho^{(i)}(1-p\varrho)^{N_\varrho^{(i)}-1}\prod_{\varrho\neq l}(1-pl)^{N_l^{(i)}}} + \\ \delta coll\left(\dfrac{1-\prod_{\varrho=1}^{\mathcal{O}}(1-p\varrho)^{N_\varrho^{(i)}}}{\sum_{\varrho=1}^{\mathcal{O}} N_\varrho^{(i)}(1-p\varrho)^{N_\varrho^{(i)}-1}\prod_{\varrho\neq l}(1-pl)^{N_l^{(i)}}}-1\right)+\ \delta succ \end{array}\right\} \tag{2.16}$$

On utilisera $T_{COP}^{(i)}(M^{(i)},\alpha,p_{inl})$pour exprimer $T_{COP}^{(i)}(M^{(i)},p_ϱ)$, comme $p_ϱ=(1+\alpha)^{\varrho}\, p_{inl}$, avec ϱ=q+d-1.

- **Relation entre la durée de COP et le taux de transmission de données**

Le taux de transmission de données est une performance très importante du protocole MAC. Ainsi, on dérive la relation entre la durée de COP et le taux de transmission de données. Soit TTD le taux de transmission de données qui est défini comme :

$$TTD = \frac{M.D}{Tcop+M.Ttran+Ttop} \tag{2.17}$$

Avec D la taille des données envoyées au BS.

De (2.10), (2.14) et (2.15) on peut obtenir

$$M = \frac{Tcop}{E[idle]\left(\frac{\prod_{\varrho=1}^{\mathcal{O}}(1-p\varrho)^{N_\varrho^{(i)}}}{1-\prod_{\varrho=1}^{\mathcal{O}}(1-p\varrho)^{N_\varrho^{(i)}}}\right)+E[coll]\left(\frac{\prod_{\varrho=1}^{\mathcal{O}}(1-p\varrho)^{N_\varrho^{(i)}}}{1-\prod_{\varrho=1}^{\mathcal{O}}(1-p\varrho)^{N_\varrho^{(i)}}}\right)+E[S]} \tag{2.18}$$

On utilise ϭ pour remplacer$N_\varrho^{(i)}$, $p\varrho, E[idle], E[coll]\ et\ E[S]$, on obtient

$$\text{Ϭ} = E[idle]\left(\frac{\prod_{\varrho=1}^{\mathcal{O}}(1-p\varrho)^{N_\varrho^{(i)}}}{1-\prod_{\varrho=1}^{\mathcal{O}}(1-p\varrho)^{N_\varrho^{(i)}}}\right) + E[coll]\left(\frac{\prod_{\varrho=1}^{\mathcal{O}}(1-p\varrho)^{N_\varrho^{(i)}}}{1-\prod_{\varrho=1}^{\mathcal{O}}(1-p\varrho)^{N_\varrho^{(i)}}}\right) + E[S] \tag{2.19}$$

Ainsi, on obtient l'expression simplifiée de la relation entre M et Tcop comme :

$$M = \frac{Tcop}{6}. \quad (2.20)$$

Par conséquent on peut obtenir l'expression simplifiée de la relation entre TTD et Tcop comme suit :

$$TTD = \frac{Tcop.D}{6.Tcop+Tcop.Ttran+6.Ttop} \quad (2.21)$$

Tableau 2.3 *Résumé de la notation utilisée*

Symbole	Définition
K	Nombre total de dispositifs
L	Nombre de dispositifs actifs
Q	Nombre de classes de priorité
M	Nombre de dispositifs qui ont réussi la contention
P_q	Probabilité d'envoi pour un dispositif de classe q
T_{frame}	Durée totale d'un cycle
T_{top}	Durée de la période de transmission
T_{cop}	Durée de la période de contention
K_q	Nombre de dispositifs appartenant à la classe q
α	Indicateur d'incrémentation
λ	Taux d'arrivée des paquets
Tack	Durée du message ACK
Treq	Durée du message de requête
BIFS	Backoff Interframe Spacing
SIFS	Short Interframe Spacing

2.8. Le problème d'optimisation

Pour T_{frame} donné, $T_{COP}^{(i)}(M^{(i)}, \alpha, p_{inl})$ plus longue permet à plus de dispositifs de réussir à la contention. Toutefois, le $T_{COP}^{(i)}(M^{(i)}, \alpha, p_{inl})$ réduira la TOP soumettant à la contrainte que $T_{COP}^{(i)}(M^{(i)},$

α, p_{inl}) + $T_{TOP}^{(i)} \leq T_{frame}$. Pour équilibrer ce compromis, nous formulons un problème d'optimisation pour maximiser le débit global dans chaque cycle. Le débit, désigné par D, est défini comme :

$$D = R.T_{top} = M.R.T_{tr} \quad (2.22)$$

Avec T_r la durée d'un créneau de transmission et R le débit de données. Alors, on peut maximiser le débit global comme suit :

$$\max_{T_{COP},\alpha,pinl}^{(i),i=1,\ldots,I} D \quad (2.23)$$

$$\text{Soumis à } T_{COP}^{(i)}(M^{(i)}, \alpha, p_{inl}) + T_{TOP}^{(i)} \leq T_{frame} \quad (2.24)$$

i= 1,…,I

$$N_{\varrho}^{(i)} = N_{\varrho-1}^{(i-1)} - M_{\varrho-1}^{(i-1)} + U_{\varrho}^{(i-1)} \quad (2.25)$$

i= 1,…,I

$$M_{\varrho}^{(i)} = [M^{(i)} P_{pck}(\varrho)], \; i= 1,\ldots,I \quad (2.26)$$

$$0 \leq p_{inl} \leq 1, \qquad \alpha > 0 \quad (2.27)$$

Dans la contrainte (2.26), $P_{pck}(\varrho)$ est défini comme la probabilité qu'un périphérique de classe ϱ conteste avec succès dans la période de contention.

$$P_{pck}(\varrho) = \frac{N_{\varrho}^{(i)} p_{\varrho} (1- p_{\varrho})^{N_{\varrho}^{(i)}-1} \prod_{\varrho \neq l}(1- p_l)^{N_l^{(i)}}}{\sum_{\varrho=1}^{\Theta} N_q^{(i)}(1- p_{\varrho})^{N_{\varrho}^{(i)}-1} \prod_{\varrho \neq l}(1- p_l)^{N_l^{(i)}}} \quad (2.28)$$

Par conséquent, le nombre de périphériques de classe ϱ qui contestent avec succès les possibilités de transmission pendant le cycle i est donné par

$$M_{\varrho}^{(i)} = [M^{(i)} P_{pck}(\varrho)] \quad (2.29)$$

Notons que $T_{COP}^{(i)}$ est fonctions de $M^{(i)}$ comme montré dans (2.16). Pour la simplicité d'expression, on utilise la variable $M^{(i)}$ au lieu de $T_{COP}^{(i)}$. Le problème d'optimisation peut être écrit comme

$$\max_{M,\alpha,pinl}^{(i),i=1,\ldots,I} M(i) \quad (2.30)$$

Soumis à Contraintes (2.10) – (2.13)(2.16)

- **Dérivation de $U_{\varrho}^{(i-1)}$**

$U_{\varrho}^{(i-1)}$, i = 1,…,I est définie comme le nombre de machines de la classe ϱ qui ont une nouvelle arrivée de paquet durant le (i-1)ème cycle. Le processus d'arrivée de paquets est un

processus d'arrivée poisson avec un taux d'arrivée λ pour chaque appareil. Soit $g_ϱ$ la probabilité qu'un appareil de type ϱ a au moins une nouvelle arrivée de paquet durant T_{frame}. Alors on a :

$$g_ϱ = 1 - e^{-\lambda T frame}. \quad (2.31)$$

On calcule d'abord $U_ϱ^{(i-1)}$ lorsque i = 1. Dans ce cas, $U_ϱ^0$ représente le nombre de machines de la classe ϱ qui ont une nouvelle arrivée de paquet durant le cycle 0. Dans le cycle 0, $K_ϱ = K_q$, ϱ,q = 1,…,Q. soit $N_ϱ^0$ le nombre de machines de la classe ϱ qui ont au moins une nouvelle arrivée de paquet durant le cycle 0. La probabilité que $N_ϱ^0$ = n est :

$$P\{N_ϱ^0 = n\} = \binom{Kq}{n} [1 - (1 - g_ϱ)^{Tframe}]^n . (1- g_ϱ)^{Tframe\ (Kq-n)} \quad (2.32)$$

Ainsi on obtient

$$U_ϱ^0 = \sum_{n=1}^{Kq} nP\{N_ϱ^0 = n\}. \quad (2.33)$$

Pour i = 2,…,I, le nombre de machines de type ϱ, $K_ϱ^{(i-1)}$ = Kq - $M_ϱ^{(i-1)}$ avec $M_ϱ^{(i-1)}$ = [$M^{(i-1)}$ P_{pck} (ϱ)] et P_{pck} (ϱ) est donnée par (2.29). Soit $N_ϱ^{(i-1)}$ le nombre d'appareils de la classe ϱ qui ont au moins une nouvelle arrivée de paquet durant le $(i-1)^{ème}$ cycle et $P\{N_ϱ^{n-1} = n\}$ la probabilité que $N_ϱ^{(i-1)}$ = n, on a :

$$P\{N_ϱ^{(i-1)} = n\} = \binom{K_ϱ^{(i-1)}}{n} [1 - (1 - g_ϱ)^{Tframe}]^n . (1- g_ϱ)^{Tframe(K_ϱ^{(i-1)}-n)} \quad (2.34)$$

De la même manière, on peut calculer

$$U_ϱ^{i-1} = \sum_{n=1}^{K_ϱ^{(i-1)}} nP\{N_ϱ^{(i-1)} = n\},\ i = 2,\ldots,I. \quad (2.35)$$

- **La convexité du problème d'optimisation :**

Puisque la fonction objective dans (2.9) est une fonction linéaire de $M^{(i)}$ et les contraintes (2.11)-(2.13) sont linéaires, on peut montrer que la contrainte (2.10) est une fonction convexe, comme suit :

Soit L = $\sum_{ϱ=1}^{Θ} N_ϱ^{(i)}$. Lorsque L → ∞ et (1+α)p_{inl} ≤ 1, $T_{COP}^{(i)}$(($M^{(i)}$,α,p_{inl}) peut être obtenue comme une fonction convexe de $M^{(i)}$, α et p_{inl}.

Preuve :

En fait, Puisque la durée de T_{frame} a une valeur finie, lorsque L → ∞, on obtient L >> $M^{(i)}$, alors on a :

$$T_{COP}^{(i)}(M^{(i)},\alpha,p_{inl}) = M^{(i)}.\{\frac{(1-(1+\alpha)pinl)^L}{L(1+\alpha)pinl(1-(1+\alpha)pinl)^{L-1}}.\ \delta_{idle} + (\frac{1-(1-(1+\alpha)pinl)^L}{L(1+\alpha)pinl\ (1-(1+\alpha)pinl)^{L-1}} - 1)\ \delta_{coll} + \delta_{succ}\} \quad (2.36)$$

De plus, $(1 - (1+\alpha)pinl)^{L-1}$ tend vers $(1 - (1+\alpha)pinl)^{L}$ si L est suffisamment large. Par conséquent on peut obtenir la transformation approchée de cette équation comme

$$T_{COP}^{(i)}(\ (M^{(i)},\alpha,p_{inl}) = M^{(i)}.\{\frac{1}{L(1+\alpha)pinl}.\ \delta_{idle} + (\ \frac{1}{L(1+\alpha)pinl\ (1-(1+\alpha)pinl)^{L-1}} - \frac{1}{L(1+\alpha)pinl} - 1)\ \delta_{coll} + \delta_{succ}\ \} \quad (2.37)$$

Prenant la dérivée seconde de $T_{COP}^{(i)}(\ (M^{(i)},\alpha,p_{inl})$ par rapport à $M^{(i)}$, α et p_{inl}, respectivement, la matrice Hessienne est donnée par :

$$H = \begin{bmatrix} \frac{d2\ T_{COP}^{(i)})}{dM(i)2} & \frac{d2\ T_{COP}^{(i)}}{dM(i)dPinl} & \frac{d2\ T_{COP}^{(i)}}{dM(i)d\alpha} \\ \frac{d2\ T_{COP}^{(i)}}{dPinl\ dM(i)} & \frac{d2\ T_{COP}^{(i)}}{dp_{inl}^2} & \frac{d2\ T_{COP}^{(i)}}{dPinl\ d\alpha} \\ \frac{d2\ T_{COP}^{(i)}}{d\alpha\ dM(i)} & \frac{d2\ T_{COP}^{(i)}}{d\alpha\ dPinl} & \frac{d2\ T_{COP}^{(i)}}{d\alpha 2} \end{bmatrix} \quad (2.38)$$

Rappeler que L → ∞, il est facile d'obtenir

$$\frac{d2\ T_{COP}^{(i)}}{dM(i)2} = 0 \quad (2.39)$$

$$\frac{d2\ T_{COP}^{(i)}}{d\ p_{inl}^2} = \frac{2}{L(1+\alpha)\ p_{inl}^3}\ .\ \delta_{idle} + (\ \frac{1+(1-(1+\alpha)pinl)^{L+1}+L(1+\alpha)pinl}{(1+\alpha)(1-(1+\alpha)pinl))^{L+2}})\ \delta_{coll} > 0 \quad (2.40)$$

$$\frac{d2\ T_{COP}^{(i)}}{d\alpha 2} = \frac{2}{Lpinl(1+\alpha)^3}\ .\ \delta_{idle} + (\ \frac{1+(1-(1+\alpha)pinl)^{L+1}+L(1+\alpha)pinl}{(1+\alpha)^2Pinl(1-(1+\alpha)pinl))^{L+2}})\ \delta_{coll} > 0 \quad (2.41)$$

$$\frac{d2\ T_{COP}^{(i)}}{dM(i)dPinl} = \frac{d2\ T_{COP}^{(i)}}{dPinl\ dM(i)} = \frac{-1}{L(1+\alpha)\ p_{inl}^2}\ .\ \delta_{idle} + (\ \frac{(1-(1+\alpha)pinl)^{L}+(L-1)(1+\alpha)^2pinl}{(L-1)(1+\alpha)pinl(1-(1+\alpha)pinl))^{L+1}})\ \delta_{coll} > 0 \quad (2.42)$$

$$\frac{d2\ T_{COP}^{(i)}}{dM(i)d\alpha} = \frac{d2\ T_{COP}^{(i)}}{d\alpha\ dM(i)} = \frac{-1}{L(1+\alpha)^2Pinl}\ .\ \delta_{idle} + (\ \frac{(1-(1+\alpha)pinl)^{L-1}+L(1+\alpha)p_{inl}^2}{L(1+\alpha)pinl(1-(1+\alpha)pinl))^{L+1}})\ \delta_{coll} > 0 \quad (2.43)$$

$$\frac{d2\ T_{COP}^{(i)}}{d\alpha\ dPinl} = \frac{d2\ T_{COP}^{(i)}}{dPinl\ d\alpha} = \frac{2}{L(1+\alpha)^2\ p_{inl}^2}\ .\ \delta_{idle} + (\ \frac{(1-(1+\alpha)pinl)^{L}+L(1+\alpha)pinl}{(1+\alpha)pinl(1-(1+\alpha)pinl))^{L+2}})\ \delta_{coll} > 0 \quad (2.44)$$

Par conséquence, la matrice Hessienne de T_{cop}, H ≥ 0, nous concluons que $T_{COP}^{(i)}(M^{(i)},\alpha,p_{inl})$ est une fonction convexe de $M^{(i)}$,α et p_{inl} [125].

Par suite le problème d'optimisation est un problème de programmation convexe et la période optimale de COP est :

$$T_{COP,opt}^{(i)} = T_{COP}^{(i)}\ (M_{opt}^{(i)},\alpha_{opt},p_{inl,opt}). \quad (2.45)$$

2.9. Environnement de travail

2.9.1. Environnement logiciel

Notre simulation a été réalisée dans l'environnement logiciel suivant :

- **Système d'exploitation :** Windows 7 Professionnel
- **Simulateur :** omnet++ 5.0

2.9.2. Justification du choix d'Omnet++

La simulation des réseaux consiste principalement en la reproduction du comportement et du fonctionnement des nœuds dans un environnement informatique pour des raisons tels que : la

répétition d'expérience, l'adressage des systèmes complexes, le gain de temps et la variation des paramètres de simulation, alors que la simulation réelle s'avère couteuse voire impossible dans quelque cas.

Tableau 2.4 *Comparaison des logiciels de simulation*

Simulateur	Avantages	Inconvénients
Omnet++	-architecture modulaire -utilisation du C++ et du C# pour le développement du noyau -Les classes de base peuvent être étendues et personnalisées -conception de modèles proches de la réalité -Interface graphique puissante. -Simule le problème de consommation d'énergie.	- Ne prend pas en charge le cas des réseaux de capteurs -Manque de modèles pour les réseaux sans fils - Omnet++ est un peu lent à cause de sa longue simulation et la consommation de mémoire élevée.
NS2	-Orienté objet -simulation des protocoles standards -Simulateur multicouches	-Conçu pour les réseaux filaires -difficulté d'ajout de nouveaux modèles -Intégration difficile à d'autres applications -Faible performance lorsque le réseau est important -Scénario de simulation décrit en Otcl
NS3	-NS3 n'est pas une extension de Ns2. C'est un nouveau simulateur. -open source -support de la virtualisation.	-Les liaisons Python ne fonctionnent pas sur Cygwin. -Seulement IPv4 est supporté.
Opnet	-Opnet communique avec les autres simulateurs. -moteur de simulation à évènement discret rapide. -Support de simulation sans fil évolutif -débogage et analyse intégrés, basés sur l'interface graphique	-produit commercial. -modèles consommant de la mémoire -Didacticiels insuffisants.
JSIM	-prise en charge de la modélisation de l'énergie à l'exception de l'énergie radio -Prise en charge des réseaux mobile sans fil et les réseaux de capteurs. -architecture orienté objet.	-Faible efficacité de simulation. -Le seul protocole MAC fourni pour les réseaux sans fil est 802.11. -Coûts d'exécution inutiles.
QualNet	-Interface graphique puissante. -très bonne évolutivité : temps de simulation raisonnable.	-Produit commercial -Installation difficile sur le système d'exploitation Linux

La simulation est souvent moins chère que l'expérimentation et comporte beaucoup moins de risques lorsque l'homme fait partie du système étudié. Les résultats peuvent être obtenus beaucoup

plus rapidement. La simulation (surtout numérique) est basée sur une connaissance des phénomènes qui ne peut être obtenue que par l'expérimentation.

Une simulation ne peut donc être réalisée que si on dispose d'un acquis sur des phénomènes antérieurs et analogues. Quelle que soit la qualité de la simulation, elle ne remplace pas totalement l'expérimentation.

Grace aux progrès réalisés dans le domaine du développement et des techniques de programmation, nous disposons aujourd'hui de langages de programmation très puissants. Ainsi, il devient possible de réaliser un simulateur dans un environnement de programmation existant.

En fonction du type d'évènements dans la simulation, on distingue deux types de systèmes de simulation : les systèmes discrets et les systèmes continus. Les systèmes de simulation discrète sont des systèmes pour lesquels les variables concernés ne changent d'état qu'en nombre fini de points sur l'axe du temps. On les appelle aussi « systèmes de simulation à évènements discrets ». Les systèmes de simulation continue sont des systèmes pour lesquels les variables peuvent changer d'état à n'importe quel instant pendant la simulation.

Il existe plusieurs simulateurs de réseau tel que : NS2, Omnet++, Opnet, JSIM,… Le tableau 2.4 présente les avantages et les inconvénients de quelques simulateurs y compris Omnet++.

2.10. Résultats obtenus et évaluation des performances

2.10.1. Résultats du problème de l'optimisation

Nous avons utilisé le solveur de Microsoft office Excel 2013 pour la résolution de notre problème d'optimisation. C'est un programme de complément dans Excel. Il permet de résoudre des problèmes non linéaires, Simplex et évolutionnaire. D'abord il faut placer les données nécessaires et les contraintes à respecter dans les cellules d'une feuille, aussi il faut réserver des cellules pour les variables de décision. Et la fonction objectif L'étape suivante est d'entrer les paramètres du solveur. C'est-à-dire l'objectif à définir (Max, Min, Valeur) pour la cellule de la fonction objectif, les contraintes, les cellules variables et la méthode de résolution. Si le solveur trouve une solution qui satisfait toutes les contraintes, il peut nous fournir un rapport de solution (figure 2.8), un rapport de limites (figure 2.9) et un rapport de sensibilité comme représenté dans la figure 2.10.

Tableau 2.5 présente l'effet de variation de la durée d'un cycle (T_{frame}) lorsque le réseau se compose de 1000 appareils appartenant à trois classes de priorité. La classe 1 contient 900 machines, la classe 2 qui est plus prioritaire regroupe 90 machines et 10 machines appartiennent à la classe 3 qui a des exigences de QOS très élevés.

Tableau 2.5 *Effet variation de Tframe*

T_{frame} = 100 ms		T_{frame} = 200 ms	
P_{opt}	0.01	P_{opt}	0.01
M_{opt}	95	M_{opt}	192
α_{opt}	1	α_{opt}	1
$T_{cop,opt}$	4 ms	$T_{cop,opt}$	8 ms

Microsoft Excel 15.0 Rapport de solution
Feuille : [Classeur2.xlsx]Feuil1
Date du rapport : 20/05/2018 17:19:42
Résultat : Le Solveur a trouvé une solution satisfaisant toutes les contraintes et les conditions d'optimisation.
Moteur du solveur
Moteur : GRG non linéaire
Heure de la solution : 0,031 secondes.
Itérations : 0 Sous-problèmes : 0
Options du solveur
Temps max Illimité, Itérations Illimité, Precision 0,000001
Convergence 0,0001, Taille de la population 100, Valeur de départ aléatoire 0, Dérivées - Central
Sous-problèmes max Illimité, Solutions de nombre entier max Illimité, Tolérance des nombres entiers 1%, Supposé non négatif

Cellule objectif (Max)

Cellule	Nom	Valeur initiale	Valeur finale
R2	max	165410,9683	165410,968

Cellules variables

Cellule	Nom	Valeur initiale	Valeur finale	Entier
K2	alpha	1,024482424	1,02448242	Suite
H2	M	95,7	95,7	Suite
G2	pinl	0,012631605	0,0126316	Suite

Contraintes

Cellule	Nom	Valeur de la cellule	Formule	État	Marge
S2	cop+mt	100000	S2<=B2	Lié	0
G2	pinl	0,012631605	G2<=1	Non lié	0,9873684
G2	pinl	0,012631605	G2>=0	Non lié	0,0126316
K2	alpha	1,024482424	K2>=0	Non lié	0,92448242

Figure 2.8 *Rapport de solution*

Microsoft Excel 15.0 Rapport des limites
Feuille : [Classeur2.xlsx]Feuil1
Date du rapport : 20/05/2018 17:19:43

Objectif		
Cellule	Nom	Valeur
R2	max	2E+05

Variable			inférieure	Objectif	supérieure	Objectif
Cellule	Nom	Valeur	Limite	Résultat	Limite	Résultat
K2	alpha	1,024	#N/A	#N/A	1,0245455	165411
H2	M	95,7	95,7	#######	95,7	#######
G2	pinl	0,013	#N/A	#N/A	#N/A	#N/A

Figure 2.9 *Rapport de limites*

Microsoft Excel 15.0 Rapport de sensibilité
Feuille : [Classeur2.xlsx]Feuil1
Date du rapport : 20/05/2018 17:19:42

Cellules variables

		Finale	Valeur
Cellule	Nom	Valeur	Gradient
K2	alpha	1,02448242	0
H2	M	95,72394	0
G2	pinl	0,0126316	0

Contraintes

		Finale	de Lagrange
Cellule	Nom	Valeur	Multiplicateur
S2	cop+mt	100000	1,654109638

Figure 2.10 *Rapport de sensibilité*

2.10.2. Métriques pour l'étude des performances

Ici, on compare notre protocole MAC hybride avec un protocole à base de contention (CSMA p-persistant) et un protocole à base de réservation (TDMA).Nous étudions les performances de notre méthode d'accès monocanal en considérant trois métriques essentielles : le débit, le délai de

transmission moyen et l'utilité qui sont représentés en ordonnée sur nos courbes, par rapport à la charge du trafic réseau qu'on augmente progressivement, ce que l'on peut voir en abscisse. Les paramètres de simulation sont montrés dans le tableau 2.6.

a) Débit : Le débit peut être défini comme le taux de livraison réussie des messages sur un canal de communication (mesuré en bit/s ou bien bps). Ces données peuvent être transmises via une liaison physique ou bien logique, ou passer par un certain nœud du réseau. En plus, le débit du système est la somme des débits des données qui sont fournis à tous les terminaux d'un réseau. Nous avons comparé le débit du système en termes de nombre total des machines en contention, et en termes des machines réussis pendant la contention pour différentes valeurs de T_{frame}. Le débit du protocole proposé reste toujours supérieur à celui du TDMA, et lorsqu'on augmente la valeur de K (à partir de 200 appareils), il est également supérieur à celui du CSMA p-persistant. C'est-à-dire que le protocole hybride proposé peut contrôler la probabilité de contention p et le nombre de dispositifs réussis de manière optimale pour maximiser le débit du système. Alors que CSMA p-persistant ne peut bien fonctionner que dans la condition de faible charge et TDMA fonctionne bien seulement dans la condition de charge élevé, notre schéma hybride ne peut pas donner les meilleurs résultats dans des conditions de faible trafic. Figure 2.11 montre la comparaison des trois protocoles dans le cas de 500 appareils.

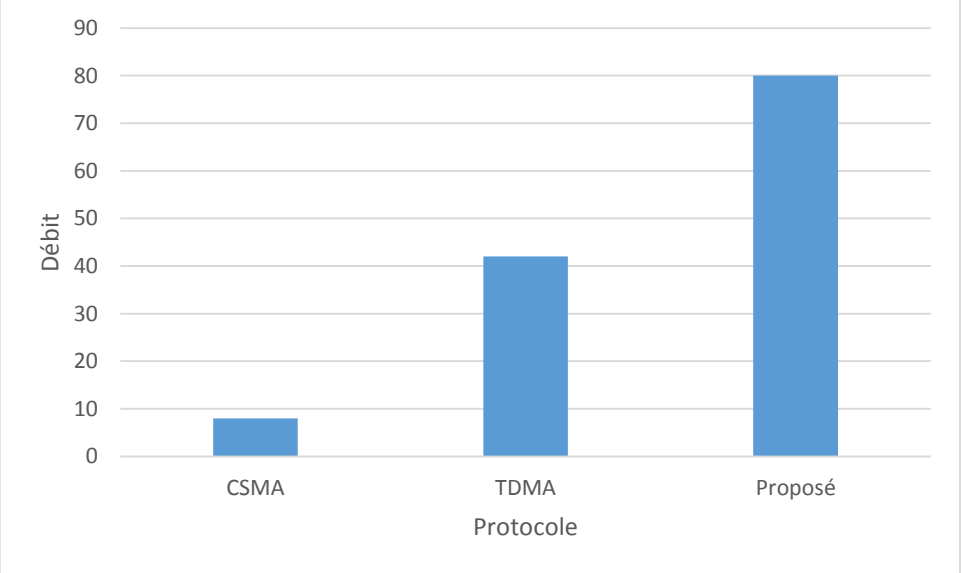


Figure 2.11 *Comparaison de débit dans le cas de 500 appareils*

Tableau 2.6 *Paramètres de simulation*

Nom	Valeur
La durée d'un cycle	T_{frame} = 100 ms
Le temps de transmission pour chaque appareil	T_{tran} = 1 ms
Longueur du période de notification	T_{nof}= 10 µs
Longueur du message ACK	T_{ack} = 7.5 µs
Longueur du message de requête	T_{req} = 22.2 µs
Débit des données	R = 1.728 Gbps
Durée de Short Interframe Spacing	SIFS = 2.5 µS
Durée de Backoff Interframe Spacing	BIFS = 7.5 µs
Energie de transmission d'un appareil	P_t = 1.5 W
Energie de réception d'un appareil	P_r = 1 W
Energie de veille d'un appareil	P_i = 0.5 W

b) Délai de transmission moyen

Nous avons comparé le délai de transmission de notre protocole avec celui de CSMA p-persistant et TDMA. Le délai de transmission moyen est le temps passé entre le début d'une trame et la fin de sa transmission à la station de base pendant un cycle. Il peut être calculé comme le rapport entre la longueur de la connexion et la vitesse de transmission sur le support. soit T_{delai} le délai de transmission moyen de notre protocole MAC hybride, alors

$$T_{delai} = T_{NP} + T_{cop} + T_{top} \quad (2.46)$$

avec $T_{top} = T_{slot} * N_s$ et N_s le nombre de slots TDMA.

Figure 2.12 Montre la comparaison entre le délai de transmission moyen de CSMA p persistant, TDMA et du protocole proposé. Cette comparaison montre que notre protocole atteint délai considérablement inférieur à celui de CSMA p-persistant car, dans notre schéma, les nœuds ne transmettent que des petits paquets de requête de transmission pendant la période de contention. Par conséquent, lorsque des collisions se produisent, le temps d'attente pour les nœuds est considérablement réduit. En outre, à mesure que le nombre de dispositifs augmente, notre protocole proposé contrôle le nombre de nœuds pendant la période de transmission. De plus, il contrôle la probabilité de transmission de chaque nœud pour réduire la congestion du support. Aussi, le protocole proposé a un délai de transmission moyen proche de celui de TDMA.

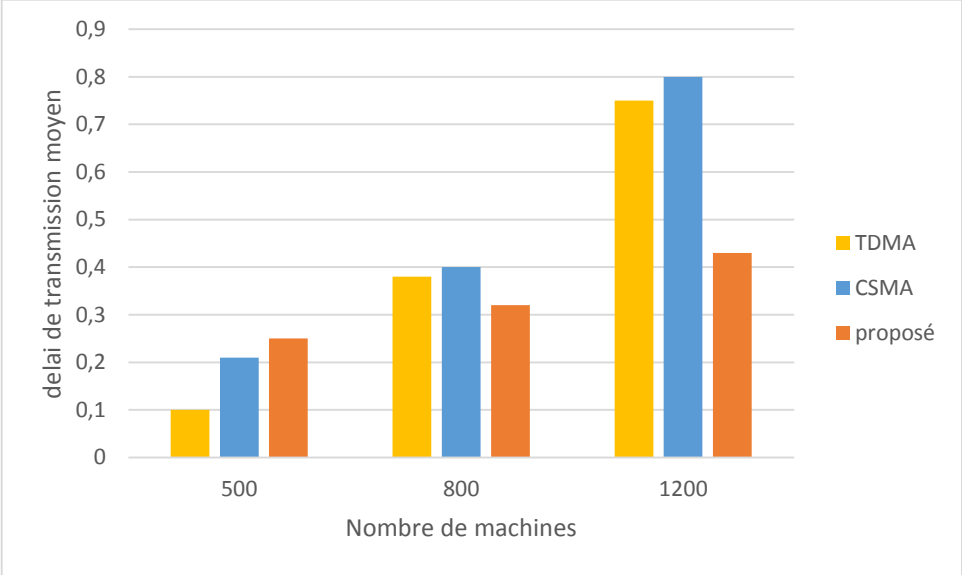


Figure 2.12 *Comparaison du délai de transmission moyen*

c) Utilité

Nous définissons l'utilité comme le rapport de la période de transmission (TOP) par rapport la période de chaque cycle (T_{frame}). On a :

$$U = \frac{Ttop}{\text{Tframe}} \qquad (2.47)$$

Pour illustrer la performance en termes d'utilité, nous comparons aussi notre protocole avec CSMA p-persistant et TDMA.

Figure 2.13 Présente la comparaison de l'utilité du protocole proposé avec les deux autres protocoles. On remarque que l'utilité de notre protocole MAC est supérieure à celle de CSMA p-persistant car le nombre de machines est élevé. Dans ce cas, la collision causée par CSMA p-persistant augmentera aussi ce qui peut considérablement réduire l'utilité. Puisque le protocole hybride utilise le mécanisme TDMA pour la transmission, les dispositifs réussis peuvent transmettre des données sans collision. De plus, l'utilité du protocole proposé est particulièrement plus élevée que celle du TDMA. En effet, notre protocole permet uniquement aux périphériques avec des données à transmettre de participer à la contention. Par conséquent, les créneaux de transmission attribués aux dispositifs réussis peuvent être totalement utilisés. Comparativement, l'attribution des créneaux dans TDMA est fixe et statique pour chaque dispositif sans tenir compte de l'utilisation complète du canal.

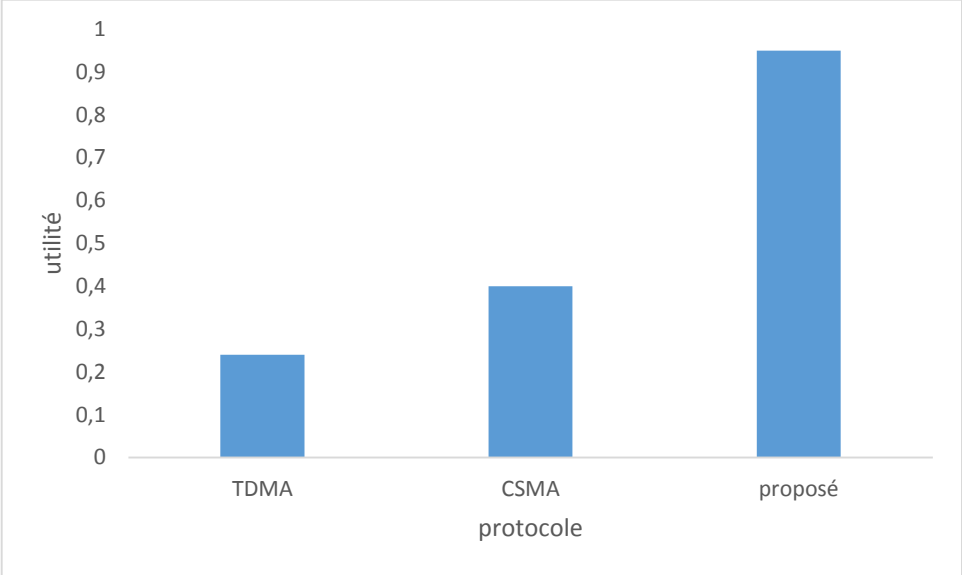


Figure 2.13 *Comparaison d'utilité dans le cas de 1200 appareils*

d) Consommation d'énergie

On considère la consommation d'énergie du réseau M2M pendant un cycle. On assume que la station de base est alimentée par courant et que les appareils sont alimentés par batterie. Ainsi, on se concentre sur la consommation d'énergie des machines. La consommation d'énergie pendant le mode de transmission est notée P_t W ; la consommation d'énergie pendant le mode de réception est notée P_r W ; et la consommation d'énergie pendant le mode inactif est notée P_i W. La consommation d'énergie du réseau M2M dans chaque période est définie comme suit :

Pendant la durée NP, chaque périphérique reçoit un message de notification. Soit E_{NP} l'énergie totale utilisée pour recevoir les messages de notification pendant NP. On a

$$E_{NP} = K\, P_r\, T_{NOF} \tag{2.48}$$

Où K est le nombre total des périphériques dans le réseau M2M et T_{NOF} est la longueur du message de notification.

Pendant la durée COP, il y aura M_{opt} des périphériques qui enverront avec succès le message Tran-REQ à BS. L'énergie totale utilisée pour envoyer ce message est indiquée par E_{COP}, on a

$$E_{COP} = \sum_{m=1}^{Mopt} Em, i \tag{2.49}$$

$$E_{m,i} = \sum_{j=1}^{N_{m,i}^{c}} [idlem, j\ Pi + Collm, j\ Pt] + IdleN_{m,i}^{c} + 1\ Pt + Sm, idesign\ Pt \tag{2.50}$$

Pendant la durée TOP, après avoir reçu le programme de transmission alloué de la station de base, chaque appareil envoie son paquet de données à la station de base à son intervalle de temps programmé T_r. La consommation d'énergie par les dispositifs réussis en transmission pendant un cycle est définie comme suit :

$E_s = M_{opt}\ P_t\ T_r$

Les périphériques qui ont échoué dans la contention restent inactifs et gardent leur module radio éteint pendant TOP. Ainsi, sur un cycle, il consomme l'énergie suivante :

$$E_{in} = (L - M_{opt})\, M_{opt}\, P_i\, T_r \tag{2.51}$$

Où $M_{opt}\, P_i\, T_r$ désigne l'énergie utilisée en mode veille pendant TOP. Par conséquent, l'énergie totale consommée par les appareils pendant TOP est

$$E_{TOP} = E_s + E_{in} \tag{2.52}$$

Par conséquent, la consommation d'énergie totale de tous les appareils pendant un cycle est définie comme suit :

$$E_{frame} = E_{NP} + E_{COP} + E_{TOP} \tag{2.53}$$

En simulation, nous visons à comparer la consommation d'énergie dans un cycle du protocole hybride proposé, CSMA p-persistant et TDMA. Le taux d'arrivée des paquets de chaque appareil est $\lambda = 1$. Pour le protocole hybride proposé, $p_{inl} = 0.01$ et $\alpha = 1$. Figure 2.14 montre la comparaison de la consommation d'énergie entre la méthode hybride proposée, CSMA p-persistant et TDMA. La comparaison indique que le protocole hybride proposé est capable de consommer moins d'énergie que CSMA p-persistant. En effet, le protocole hybride permet aux dispositifs de transmettre uniquement un message de faible longueur pendant la période de contention. La consommation d'énergie pendant la collision peut être considérablement réduite. De plus, lorsque la contention est terminée, la méthode hybride proposée peut contrôler les dispositifs qui ont échoué en contention en mode inactif pour économiser de l'énergie. De plus, le protocole proposé consomme plus d'énergie que celui du schéma TDMA. Autrement dit, dans le protocole proposé, les dispositifs doivent utiliser plus d'énergie pour contester pendant la période de contention ; cependant, cette consommation d'énergie peut conduire à une plus grande utilisation du canal et à un plus faible taux de perte de paquets.

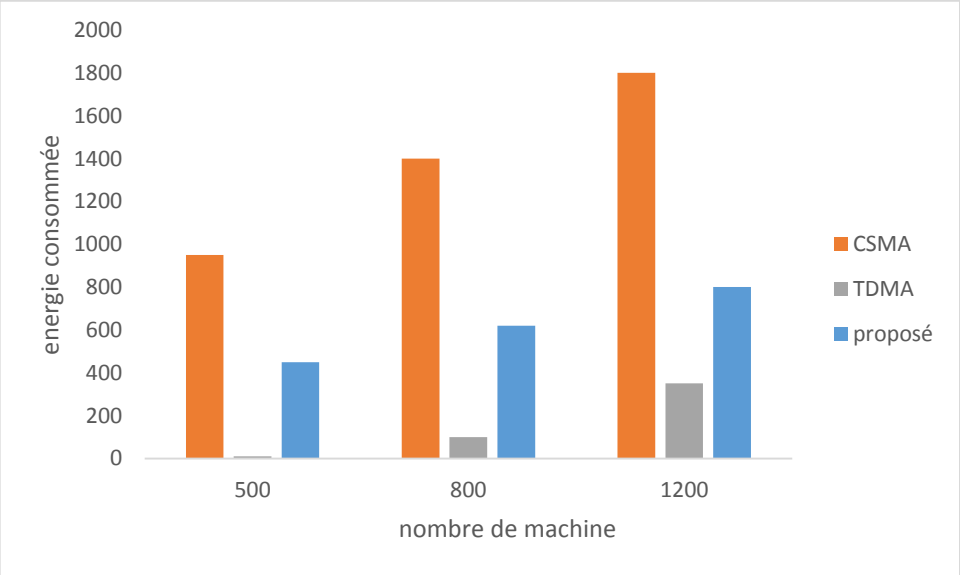


Figure 2.14 *Comparaison de la consommation d'énergie en termes de nombre de machines*

2.11. Conclusion

Dans ce chapitre nous avons proposé un protocole MAC hybride pour les communications M2M. Ce protocole est désigné pour servir plusieurs classes de trafic et répondre à leurs exigences de QoS. Le temps est divisé en cycles et chaque cycle se compose d'une période de contention et une période de transmission. Nous avons formulé un problème d'optimisation pour déterminer la probabilité et la période de contention optimale puis nous avons proposé une solution à ce problème. Nous avons présenté les résultats numériques du problème d'optimisation et déterminé les paramètres de contention optimaux pour maximiser le débit du système. Aussi, une comparaison des performances du protocole MAC hybride proposé avec un protocole à base de contention et un protocole sans contention est effectuée. Nous avons effectué un ensemble d'expérimentation varié selon le nombre des appareils afin de montrer l'efficacité de notre approche. Cela nous a permis de dégager ses avantages et ses inconvénients. Après avoir réalisé ce protocole, nous prévoyons de l'appliquer dans une application réelle comme celle qu'on va développer dans le chapitre suivant.

Chapitre 3 : Surveillance des personnes à mobilité réduite utilisant une canne intelligente

3.1. Introduction

Après avoir réalisé un protocole MAC hybride pour la communication M2M, nous allons maintenant développer une application d'e-santé réelle, ce qui va nous permettre d'appliquer ce protocole.

Plusieurs projets sont proposés dans le domaine de l'e-santé, parmi eux, le projet CANet qui vise à surveiller une personne via des capteurs qui instrumentent une canne de marche communicante. Dans ce cadre s'inscrit le contexte général de notre système.

Vu la montée en puissance des systèmes E-Santé et de la ville intelligente, la nécessité de prendre en charge les capteurs et les actionneurs, pour une automatisation efficace, s'avère être une exigence essentielle pour la maintenance de la communication machine à machine (M2M). Les éléments clés d'un système E-Santé performant sont la consommation d'énergie et le maintien de l'interopérabilité. C'est dans ce contexte que l'on pourrait définir le travail actuel dans le cadre duquel un système dédié aux personnes âgées agissant et surveillant à l'aide de leur canne connectée est mis en œuvre. Notre système consiste en un nœud émetteur positionné sur la canne qui transmet les données relatives à la position et à l'état des personnes âgées à une station de base via la technologie LoRa. Cette dernière utilise ensuite le protocole MQTT pour interagir avec l'environnement quand une chute est survenue. Plusieurs expériences ont été menées pour évaluer la zone couverte par notre réseau LoRa et la consommation d'énergie de notre système. Les résultats indiquent que la superficie moyenne couverte est d'environ 6 km2 et que la consommation électrique de notre système est au moins dix fois inférieure à celle d'un système de transmission basé sur GPRS.

3.2. Les travaux réalisés pour les systèmes de E-Santé

Dans cette section, nous présentons quelques projets e-santé basés sur l'IOT.

En fait, Juha et al. [130] ont mené une étude d'évaluation de la technologie LPWAN via LoRa afin de surveiller la santé et le bien-être à distance à l'intérieur de la maison à l'aide d'appareils de l'Université d'Oulu, en Finlande. En utilisant une gamme de paramètres de couche physique (débits, largeurs de bande et puissances de transfert ...), les résultats obtenus suggèrent qu'avec le facteur d'étalement le plus important (12 et 14 dBm), un seul mode de couverture peut être fourni par une seule station de base. L'analyse de la consommation d'énergie de l'émetteur et du récepteur indique que la quantité d'énergie requise pour transmettre le même volume d'informations est égale à 200 fois.

Les auteurs du document [131] ont abordé la surveillance de l'état de santé basée sur l'IoT à l'aide de l'infrastructure de réseau LoRaWAN. C'était en fonction de la pression artérielle, du glucose et de la température dans les zones rurales où la couverture du réseau cellulaire est manquante. Ils ont évalué leur solution via la couverture et la consommation d'énergie. Cependant, ils n'ont pas dépassé en moyenne 30 km2 lorsque le routeur LoRa est placé à l'extérieur à 12 mètres d'altitude.

Le système de surveillance à distance pour les personnes âgées utilisant IoT des auteurs de [132] traite la position et la motilité de ces personnes de manière discrète et à faible consommation. Ils ont envisagé l'utilisation de deux modules. Le premier est chargé d'identifier la position de l'utilisateur à l'intérieur. Le second détecte en permanence l'activité du corps. Cette conception peut être utilisée pour une analyse complète du comportement et un système de détection des risques. Cependant, il faut encore améliorer la portabilité et la portée du signal.

Les auteurs dans le travail [133] ont été motivés par l'application de l'IoT dans le système de santé clinique, c'est pourquoi ils ont intégré le brouillard informatique dans leur architecture. Ils utilisaient un système pour la surveillance périodique des signes vitaux du corps en temps réel. La réduction de la consommation d'énergie par la minimisation de la charge sur le cloud implique encore la justification d'une faible consommation d'énergie pour la communication, en particulier pour les appareils dotés de batteries de faible capacité.

Dans le travail actuel [134], les auteurs recherchent un design basé sur la LoRa de l'IoT pour le suivi et l'observation du patient souffrant de troubles mentaux. Le système implique un client LoRa qui suit les périphériques étiquetés sur le patient et les ponts LoRa situés dans les hôpitaux et autres lieux publics, en utilisant à la fois les réseaux cellulaires mobiles et Wi-Fi comme moyens de communication. De même, des exécutions sont effectuées dans le cloud pour alléger la charge locale. À cet égard, il n'est pas évident que le coût de consommation causé par l'augmentation de la communication n'aura pas d'effet négatif inattendu.

Les auteurs dans [135] décrivent une architecture orientée pour la maison intelligente en admettant les IoT utilisant la technologie LoRa à longue portée et basse consommation, et la communication objet via la télémétrie Message Queue, qui garantit ensuite l'interopérabilité. Bien qu'ils aient approuvé l'utilisation de leur algorithme pour la domotique en temps réel, la surveillance de multiples et différents capteurs reste une faiblesse.

Dans le tableau suivant, nous trouvons une comparaison de certains travaux mentionnés ci-dessus pour le suivi des soins de santé dans le domaine de l'IoT.

De plus, des études récentes ont été menées afin d'améliorer la canne. The Salam & Trenton, les rédacteurs de papier [126] ont tenté d'utiliser la carte Raspberry PI pour vérifier le matériel d'un système intégré utilisant l'Arduino. Pour garantir que la personne malvoyante atteigne correctement

la destination, Shreyas et les autres auteurs du document [127] ont mis en œuvre un appareil doté d'un Arduino Uno équipé d'un GPS et d'un appareil vocal afin que les malvoyants puissent éviter les obstacles et atteindre leur destination en toute sécurité. Dans [128], Meinhardt et Christin ont essayé de concevoir une canne de marche pour aider les personnes malvoyantes au moyen d'une rotule entraînée par robot. Puja et al. dans le document [129] ont cherché à concevoir une canne de marche économique et intelligent pour aider les malvoyants avec un microcontrôleur, un capteur à ultrasons et un capteur d'eau. La première composante présente la partie contrôle et décision. La deuxième composante est un transducteur qui produit des ondes et reçoit la réflexion de l'écho pour mesurer la distance. La dernière consiste à détecter l'existence d'eau afin de protéger la personne des surfaces glissantes. Nous détaillons dans le tableau 10 les caractéristiques des systèmes de surveillance ainsi leur limites en terme de surveillance et interopérabilité.

Tableau 3.1 *Les systèmes d'E-santé*

Système	Zone de surveillance	Capteurs	Communication sans fil	Communication internet	Limitations de surveillance	Limitations d'interopérabilité
Juha et al. [127]	Bâtiment intelligent	Tous les capteurs	LoRa	No	Limitation de distance	Aucune interopérabilité à maintenir via l'API REST
Afef et al. [128]	Ville intelligente	Tous les appareils	LoRa	http	Pas de notification en temps réel (causée par le brouillard)	Interopérabilité inexistante
Mighali et al. [129]	Maison	appareils portables, téléphone intelligent	BLE	REST API	Localisation intérieure	Aucune interopérabilité à maintenir via l'API REST
Kharel et al. [130]	Ville intelligente	Appareils médicaux et capteurs portables.	LoRa, Wi-Fi, BLE, 2G,3G,4G	Fog computing	Pas de notification en temps réel (causée par le brouillard)	Protocole de communication sans fil multiple, l'interopérabilité avec l'environnement n'est pas maintenue
Hayati et al. [131]	Ville intelligente	GPS	LoRa	http	Limitation de service en utilisant un téléphone intelligent	Pas d'interopérabilité avec d'autres objets connectés
Gambi et al. [132]	Maison intelligente, bâtiment intelligent	Tous les capteurs	LoRa	MQTT	Surveillance de la maison intelligente : plusieurs capteurs avec transmission LoRa	

3.3. Architecture du système

Le système avancé d'E-santé, objet de notre conception, est décrit dans la figure 3.1 ci-dessous. Il s'agit d'une canne de marche spécialement conçu pour aider à transmettre des données relatives à l'état des personnes âgées (suivi GPS, détection des chutes, nombre d'étapes) à la station de base (BS) via la technologie LoRa (longue distance, basse consommation). La BS représente une passerelle M2M, car elle permet la communication via MQTT avec un autre objet connecté dans un environnement de ville intelligente.

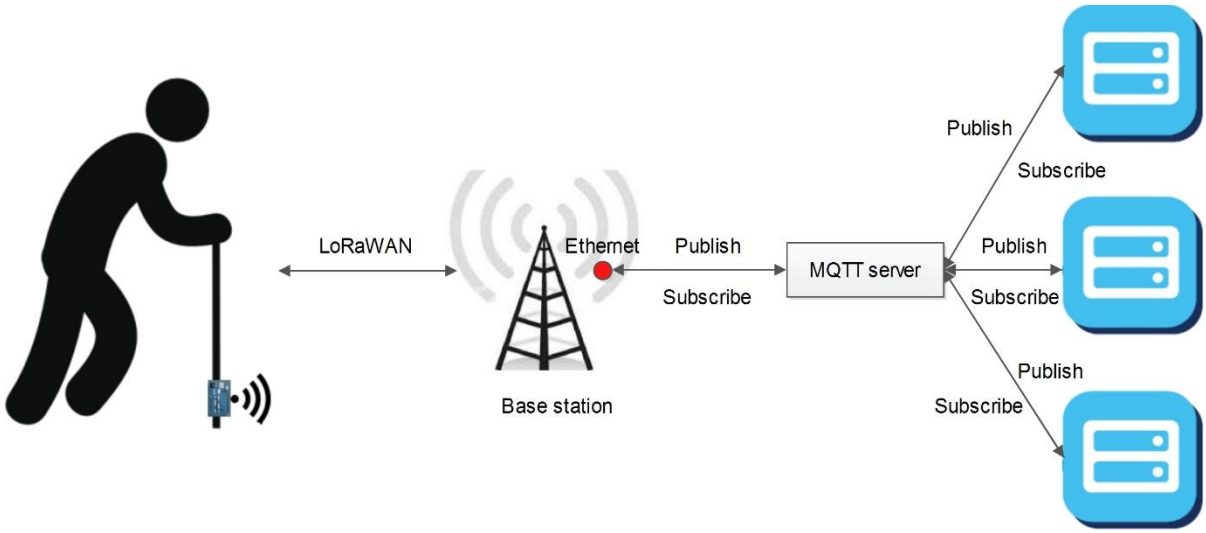


Figure 3.1 *Architecture du système de surveillance*

En fait, le système conçu est conçu de manière à permettre aux utilisateurs de visualiser l'état de la canne via un téléphone mobile afin de surveiller les mouvements des personnes âgées dans un environnement de ville intelligente. Il est utilisable en permettant à la canne de communiquer avec l'environnement en cas de chute imminente.

3.3.1. Le projet CANet

L'idée du projet CANet [136,137] est née au sein de l'équipe de recherche SCSF du laboratoire LATTIS de l'Université de Toulouse 2, il y a maintenant 10 ans. CANet a pour but d'offrir la surveillance et le suivi d'une personne âgée sans être intrusif, c'est-_a-dire sans équiper si possible directement la personne. Pour cette raison, les concepteurs ont cherché à identifier l'élément le plus habituel pour les personnes âgées. En se basant sur des expériences familiales personnelles, ils se sont aperçus que la canne est l'objet le plus utilisé et le plus important pour la personne âgée. Ils ont décidé d'intégrer une multitude de capteurs biométriques qui permet la détection des informations liées à l'environnement et des informations sur l'état de santé de la personne âgée. Parmi ces capteurs, nous trouvons des capteurs de température de la main et de l'extérieur, un capteur

d'humidité, un capteur de rythme cardiaque, un capteur de pression, un système de localisation, un système de communication sans fil… La canne contient également un microphone et un haut-parleur, ce qui permet la communication avec un centre de traitement ou un proche de la personne âgée. Ce projet a permis la fédération de différentes compétences auprès des chercheurs de l'IUT de Blagnac : informatique, électronique, réseaux, protocoles, mécanique, psychologie, expression et communications...

3.3.2. LoRaWAN

LoRaWAN définit le protocole de communication et l'architecture système du réseau, tandis que la couche physique LoRa active la liaison de communication à longue portée. Le protocole et l'architecture de réseau ont le plus d'influence sur la détermination de la durée de vie de la batterie d'un nœud, de la capacité du réseau, de la qualité de service, de la sécurité et de la diversité des applications desservies par le réseau [139].

De nombreux réseaux déployés utilisent une architecture de réseau maillé. Dans un réseau maillé, les nœuds d'extrémité individuels transmettent les informations des autres nœuds pour augmenter la portée de communication et la taille de cellule du réseau. Bien que cela augmente la portée, cela ajoute également à la complexité, à la capacité du réseau et à la durée de vie de la batterie, car les nœuds reçoivent et transmettent des informations en provenance d'autres nœuds, ce qui est probablement sans importance pour eux. L'architecture en étoile longue portée est la solution la plus judicieuse pour préserver la durée de vie de la batterie lorsque la connectivité longue portée peut être atteinte.

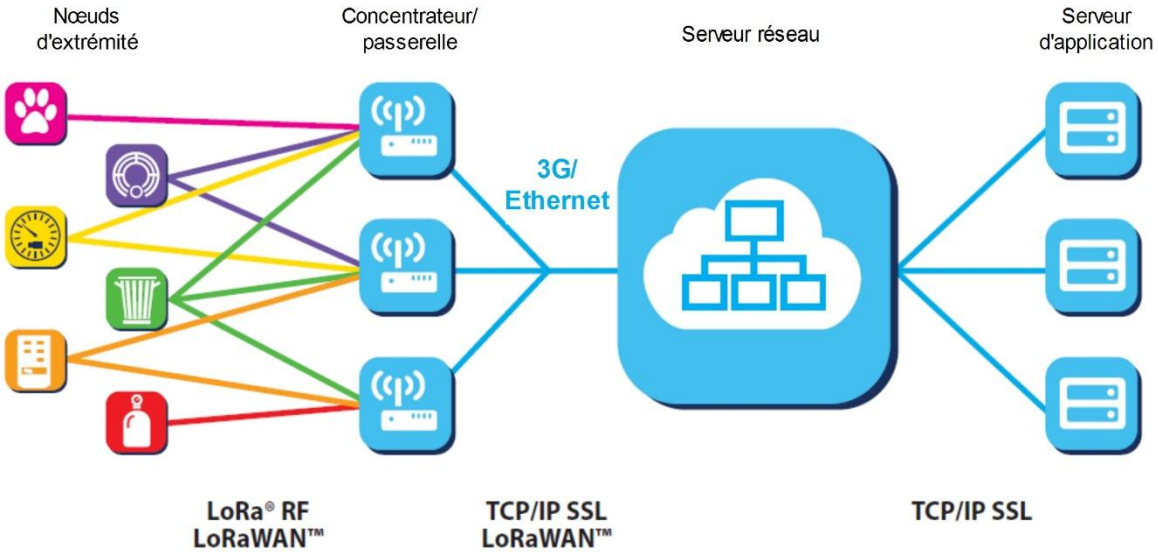


Figure 3.2 *Architecture de LoRaWAN [138]*

Dans un réseau LoRaWAN, les nœuds ne sont pas associés à une passerelle spécifique. Au lieu de cela, les données transmises par un nœud sont généralement reçues par plusieurs passerelles. Chaque passerelle transfère le paquet reçu du nœud d'extrémité au serveur de réseau basé sur un nuage via une liaison terrestre (cellulaire, Ethernet, satellite ou Wi-Fi). L'intelligence et la complexité sont transmises au serveur de réseau, qui gère le réseau, filtre les paquets redondants reçus, effectue des contrôles de sécurité, planifie les accusés de réception via la passerelle optimale et effectue le débit de données adaptatif, etc. Si un nœud est mobile ou en déplacement aucun transfert intercellulaire n'est nécessaire d'une passerelle à l'autre, ce qui est une fonctionnalité essentielle pour permettre aux applications de suivi des actifs, une application cible principale verticale pour l'IoT.

- **Durée de vie de la batterie**

Les nœuds d'un réseau LoRaWAN sont asynchrones et communiquent lorsqu'ils ont des données prêtes à être envoyées, qu'elles soient planifiées ou planifiées. Ce type de protocole est généralement appelé méthode Aloha. Dans un réseau maillé ou avec un réseau synchrone, tel qu'un réseau cellulaire, les nœuds doivent souvent se «réveiller» pour se synchroniser avec le réseau et rechercher les messages. Cette synchronisation consomme beaucoup d'énergie et constitue le principal moteur de réduction de la durée de vie de la batterie. Dans une étude récente et une comparaison effectuée par la GSMA des différentes technologies s'adressant à l'espace LPWAN, LoRaWAN a montré un avantage de 3 à 5 fois supérieur à celui de toutes les autres options technologiques [138].

- **Capacité du réseau**

Afin de rendre viable un réseau en étoile de longue portée, la passerelle doit avoir une très grande capacité de recevoir des messages d'un très grand nombre de nœuds. Une capacité de réseau élevée dans un réseau LoRaWAN [138] est obtenue en utilisant un débit de données adaptatif et en utilisant un émetteur-récepteur multi-canaux multicanaux dans la passerelle, de sorte que des messages simultanés sur plusieurs canaux puissent être reçus. Les facteurs critiques affectant la capacité sont le nombre de canaux simultanés, le débit de données (heure de diffusion), la longueur de la charge utile et la fréquence de transmission des nœuds. LoRa étant une modulation à spectre étalé, les signaux sont pratiquement orthogonaux les uns aux autres lorsque différents facteurs d'étalement sont utilisés. Lorsque le facteur d'étalement change, le débit de données effectif change également. La passerelle profite de cette propriété pour pouvoir recevoir plusieurs débits de données différents sur le même canal au même moment. Si un nœud dispose d'une bonne liaison et est proche d'une passerelle, il n'y a aucune raison pour qu'il utilise toujours le débit de données le plus faible et remplisse le spectre disponible plus longtemps que nécessaire. En augmentant le débit de

données, le temps d'antenne est raccourci, ce qui permet aux autres nœuds de transmettre davantage d'espace potentiel. Le débit de données adaptatif optimise également la durée de vie de la batterie d'un nœud [139]. Pour que le débit de données adaptatif fonctionne, une liaison montante et une liaison descendante symétriques sont nécessaires avec une capacité de liaison descendante suffisante. Ces fonctionnalités permettent à un réseau LoRaWAN d'avoir une très grande capacité et de le rendre évolutif. Un réseau peut être déployé avec un minimum d'infrastructure et, en fonction de la capacité, davantage de passerelles peuvent être ajoutées, ce qui permet d'augmenter les débits de données, de réduire le nombre d'ententes sur d'autres passerelles et de multiplier la capacité par 6-8. D'autres alternatives LPWAN n'ont pas l'évolutivité de LoRaWAN en raison de compromis technologiques qui limitent la capacité de liaison descendante ou rendent la plage de liaison descendante asymétrique à la plage de liaison montante.

3.3.3. MQTT

En tant que protocole de connectivité (M2M) / IoT, le MQTT est conçu pour être applicable au-dessus de la pile de protocoles TCP / IP, conçu pour se présenter comme un protocole de messagerie de publication / abonnement basé sur un courtier extrêmement léger, comme choisi volontairement pour un certain nombre de caractéristiques. , en particulier, les petites empreintes de code (par exemple, les contrôleurs RAM 8 bits, 256 Ko), une bande passante et une alimentation faibles, une connectivité et un temps de latence élevés, une disponibilité variable et des garanties de livraison négociées [140].

Dans cette architecture spécifique, un capteur est considéré comme un éditeur et un serveur MQTT équitable (courtier) doit être récupéré, ce qui permet de collecter les messages envoyés par les éditeurs et d'examiner à quelle cible les messages doivent être renvoyés. De l'autre côté, chaque appareil ayant déjà enregistré ses intérêts de réception sur le serveur continuerait à recevoir des messages jusqu'à ce que l'abonnement soit annulé (Figure 3.3). Grâce à une telle architecture, les éditeurs et les abonnés n'ont pas besoin de reconnaître les caractéristiques qui se caractérisent, ce qui constitue l'un des avantages majeurs de ce protocole. Par exemple, un capteur de température n'a pas besoin de reconnaître l'identité des clients abonnés pour recevoir des données et inversement [141].

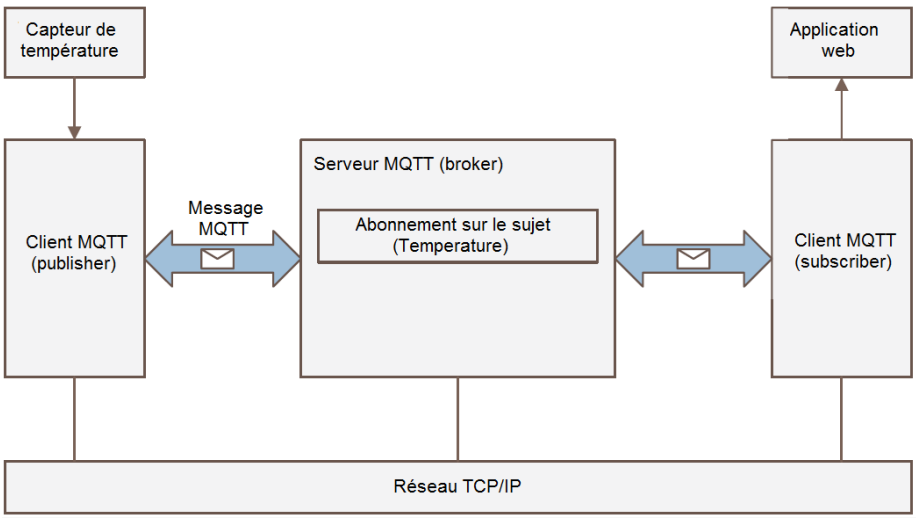


Figure 3.3 *Modèle de protocole MQTT*

- **Le client MQTT**

Il convient de souligner que tout appareil IoT pourrait bien être considéré comme un client MQTT susceptible d'envoyer ou de recevoir des données de télémétrie. Il est à noter qu'un type de client MQTT (également appelé abonné ou éditeur) dépend fortement du rôle qui lui est attribué dans le système, dans la mesure où il peut produire ou collecter des données de télémétrie. Dans les deux cas, un type de client MQTT doit d'abord établir une connexion avec un serveur de messagerie (courtier) via un type de message particulier, comme indiqué dans le chapitre suivant. Pour distinguer les différentes données envoyées par l'éditeur, une chaîne de rubrique est appliquée. Par exemple, un nœud client peut publier des valeurs de température et d'humidité en utilisant une chaîne différente pour chaque valeur (par exemple, température ou humidité). D'un autre côté, si un client MQTT a l'intention d'acquérir de telles données, il doit s'abonner au sujet spécifiquement souhaité [142].

- **Le courtier MQTT (ou bus logiciel)**

Les principales responsabilités attribuées au type de courtier MQTT consistent à gérer et à maintenir la communication entre les clients MQTT, ainsi qu'à distribuer des messages entre eux. En fait, il est capable de gérer simultanément plusieurs milliers de clients MQTT connectés. En outre, il existe également une diversité d'autres tâches et responsabilités gérées par le courtier. En premier lieu, l'authentification et l'autorisation des clients à des fins de sécurité. En outre, en ce qui concerne les communications cryptées entre le courtier et les clients, les cryptages TLS (Transport Layer Security) et SSL (Secure Sockets Layer) sont utilisés, suivant le même protocole de sécurité que celui utilisé par le protocole HTTP. Il est également possible d'implémenter une logique d'authentification ou d'autorisation personnalisée dans le système . En effet, plusieurs courtiers de messagerie semblent être capables de mettre en œuvre le protocole MQTT comme Mosquito [143]

- **Le format du message**

L'en-tête de message associé à chaque message de commande MQTT comprend un en-tête fixe d'une longueur de deux octets, ainsi qu'un en-tête de longueur variable facultatif spécifique au message et une charge utile de message (Tableau 3.2).

Tableau 3.2 *Format de message MQTT*

Bit	7	6	5	4	3	2	1	0
Byte 1	Message type				DUP	QOS		RETAIN
Byte 2	Remaining length							

En ce qui concerne l'octet 1, il contient le type de message, représenté par une valeur non signée sur quatre bits. Il existe 14 types de message spécifiés dans la version 3.1 du protocole MQTT. Parmi ces types de messages, citons : CONNECT (demande de connexion au serveur du client), PUBLISH (publication du message), PUBACK (accusé de réception de la publication), SUBSCRIBE (demande du client), pour n'en nommer que quelques-uns. Une description détaillée des types de message, dans leur intégralité, est disponible dans les spécifications du protocole [144] [145]. À ce niveau, l'indicateur DUP est défini lorsque le client ou le serveur tente de renvoyer un message PUBLISH, PUBREL, SUBSCRIBE ou UNSUBSCRIBE. Ceci s'applique aux messages avec une valeur de QoS supérieure à zéro (0) et une exigence d'accusé de réception. L'indicateur QoS sert à indiquer le niveau de garantie pour la livraison d'un message PUBLISH. Les niveaux de QoS pertinents sont décrits dans le chapitre suivant. Par exemple, si un indicateur RETAIN est défini sur true, un message MQTT normal devient un message conservé. Le courtier s'engage alors à restaurer le dernier message retenu avec la qualité de service correspondante pour un sujet spécifié. En conséquence, chaque client abonné à ce modèle de sujet particulier recevra immédiatement le message conservé (inférieur à 1 ms). Le courtier n'enregistre qu'un seul message conservé par sujet .La longueur restante, quant à elle, représente le nombre d'octets restant dans le message en cours, y compris les données disponibles dans l'en-tête de variable et la charge utile [143].

- **Qualité de service**

MQTT assure la fiabilité en maintenant l'option de trois niveaux de qualité de service (QoS), le niveau minimal étant mis à zéro pour garantir un effort de haut niveau. Le message ne faisant pas l'objet d'un accusé de réception de la part des destinataires, ni d'un message enregistré ni d'une nouvelle livraison par l'expéditeur (figure 3.4), le processus est souvent appelé "feu et oublie", offrant la même garantie que celle fournie par le protocole TCP sous-jacent [146].

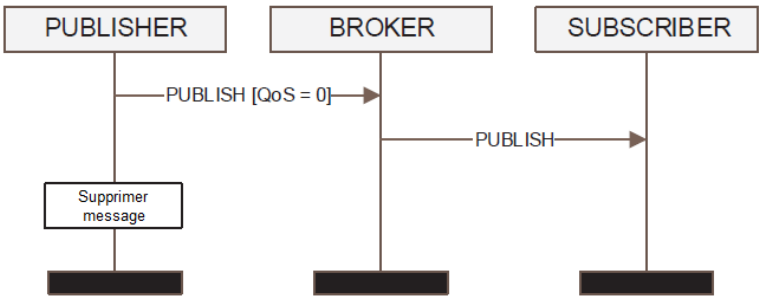


Figure 3.4 *Au plus une fois par livraison (MQTT QoS = 0)*

Lors de la mise en œuvre du niveau de qualité de service 1 (figure 3.5), il est maintenu qu'un message sera remis au destinataire au moins une fois. Cependant, le message peut toujours être remis plus d'une fois, car l'éditeur peut bien l'envoyer et vérifier l'état de livraison au moyen d'un message PUBACK.

En cas de perte du message PUBACK, le courtier s'engage alors à renvoyer le même message à nouveau, jusqu'à ce que le message PUBACK soit reçu.

Le rang de QoS le plus élevé est défini sur 2, ce qui permet de garantir que chaque message n'est reçu qu'une seule fois par la contrepartie. Il marque simultanément le niveau de qualité de service le plus sûr et le plus lent. La garantie est assurée par deux flux aller et retour établis, entre l'expéditeur et le destinataire.

Une fois que le destinataire reçoit un message QoS 2 PUBLISH (figure 3.6), il traite le message de publication en conséquence et le reconnaît à l'expéditeur via un message PUBREC.

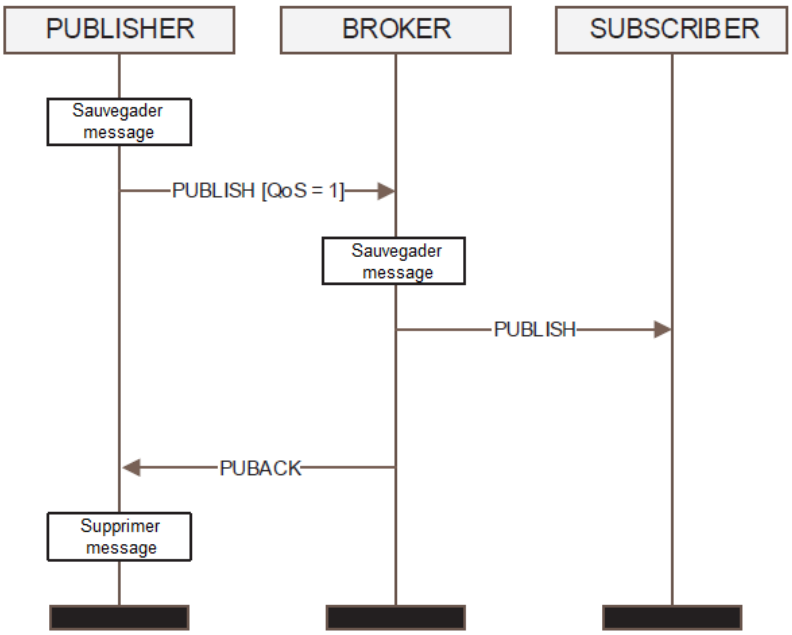


Figure 3.5 *Livraison au moins une fois (MQTT QoS = 1)*

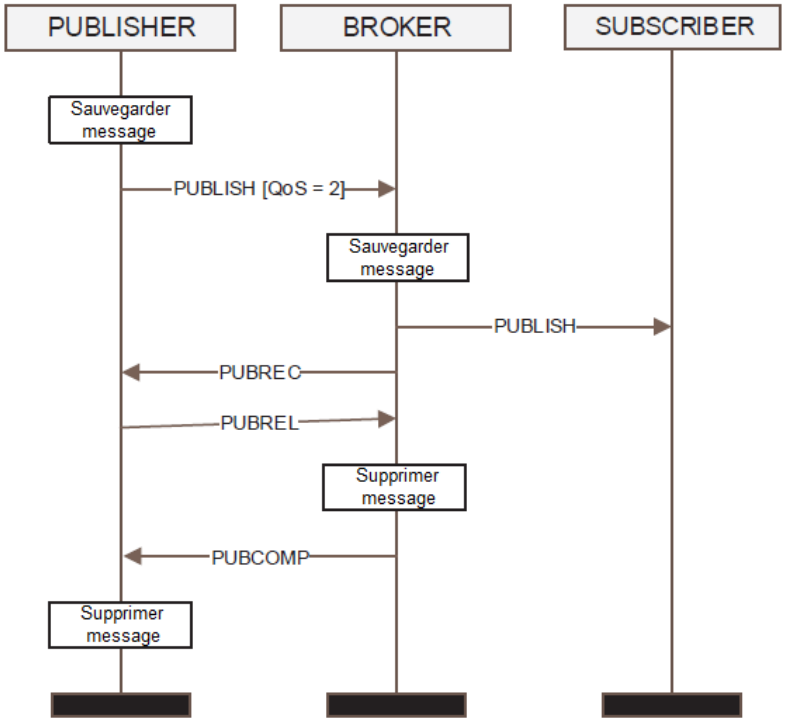


Figure 3.6 *Exactement une fois la livraison (MQTT QOS =2)*

3.4. Matériels et méthodes

3.4.1. Nœud émetteur de la canne

Le nœud émetteur est responsable de la collecte des données relatives à la canne (détection des chutes, comptage des pas, distance parcourue et la position et de l'état de la canne) ainsi que de la transmission de ces données. À cet effet, lsm303dlhc [147], en tant que système intégré, comprend un capteur d'accélération linéaire numérique 3D, un capteur magnétique numérique 3D et un module GPS Adafruit Ultimate, ainsi que le Teensy 3.2. [148] ainsi qu'un module radio RFM95 (module d'émetteur-récepteur RFM95 ISM V1.2) pour les fins de transmission de données. Ces éléments sont entièrement alimentés par une petite batterie LiPo. L'architecture détaillée du noeud est illustrée à la figure 3.7.

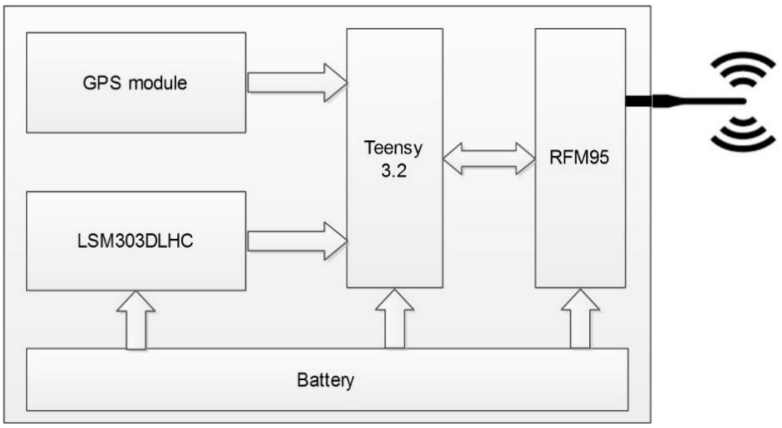


Figure 3.7 *Architecture du nœud émetteur de la canne*

Le LSM303DLHC a une pleine échelle d'accélération linéaire de ± 2g / ± 4g / ± 8g / ± 16g et une pleine échelle de champ magnétique de ± 1,3 / ± 1,9 / ± 2,5 / ± 4,0 / ± 4,7 / ± 5,6 / ± 8,1 gauss. L'intégralité des gammes complètes disponibles est entièrement sélectionnable par l'utilisateur.

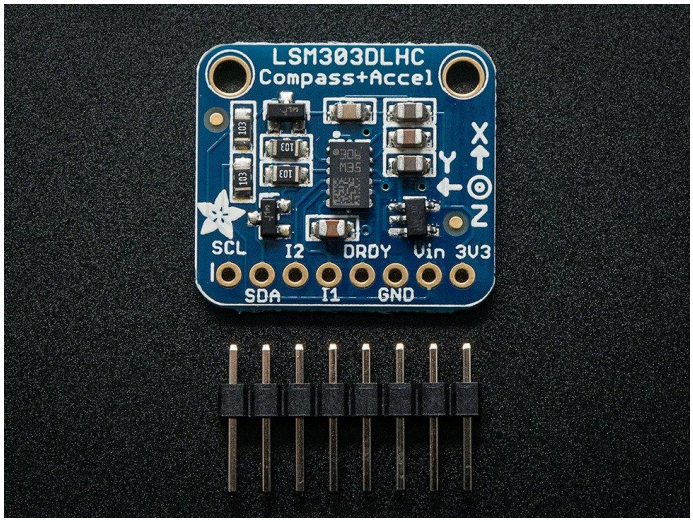


Figure 3.8 *Capteur lsm303dlhc*

Le Teensy 3.2 utilisé présente les caractéristiques suivantes :

- Alimentation : via micro-USB
- Microprocesseur : ARM Cortex M4 72 MHz
- Mémoire flash : 256 ko
- Mémoire SRAM : 64 kB
- Mémoire EEPROM : 2 ko
- 34 broches d'E / S dont 12 PWM
- 21 entrées analogiques 13 bits
- 1 sortie analogique 12 bits
- Support USB avec transfers DMA (Direct Access Memory)
- Bus series, CAN, I2C et SPI
- Interface I2S
- Gestion des interruptions
- Module RTC (nécessite l'ajout d'un quartz 32 768 kHz et d'une pile 3 Vcc pour la sauvegarde de l'heure)
- Entrée capteur tactile
- Régulateur 3,3 Vcc / 100 mA
- Dimensions : 35 x 18 mm

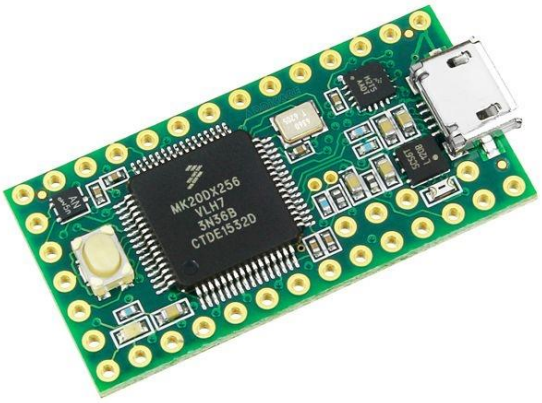


Figure 3.9 *Teensy 3.2*

En ce qui concerne les émetteurs-récepteurs RFM95 / 96/97/98 (W), le modem longue portée LoRaTM assure une communication à spectre étendu ultra-longue portée et une immunité élevée aux perturbations tout en minimisant la consommation de courant. En utilisant la technique de modulation LoRaTM brevetée par Hope RF, RFM95 / 96/97/98 (W) peut atteindre une sensibilité de plus de - 148dBm avec un cristal et une nomenclature des matériaux peu coûteux. La haute sensibilité associée à l'amplificateur de puissance intégré de +20 dBm offre un budget de liaison inégalé dans l'industrie, le rendant optimal pour toute application nécessitant de la portée ou de la robustesse. LoRaTM offre également des avantages importants en termes de blocage et de sélectivité par rapport aux techniques de modulation conventionnelles, résolvant ainsi le compromis de conception traditionnel entre portée, immunité aux perturbations et consommation d'énergie.

Figure 3.10 *Module LoRa RF96*

Le module GPS est construit autour du chipset MTK3339, un module de grande qualité qui peut suivre jusqu'à 22 satellites sur 66 canaux, dispose d'un excellent récepteur haute sensibilité (suivi à -165 dBm!) Et d'un capteur intégré.

Figure 3.11 *Module GPS Adafruit*

3.4.2. Acquisition des données

Cette section décrit les méthodes déployées et développées pour calculer les valeurs des paramètres de la surveillance d'une personne agée.

- **Orientation absolue**

Pour déterminer l'orientation d'un objet, il faut calculer l'angle de rotation sur l'axe des x (Roll), l'angle de rotation sur l'axe des y (Pitch) et l'angle de rotation sur l'axe des z (Yaw) comme le montre la figure 3.12.

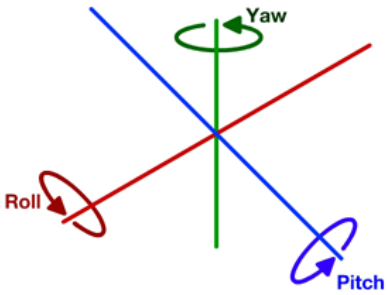


Figure 3.12 *Rotations sur les axes x,y et z*

Pour cela, nous avons utilisé l'accélération liée à la gravité fournit par l'accéléromètre pour calculer le Roll et le Pitch, et la vitesse de rotation pour calculer le Yaw.

Le système de fusion de capteur appliqué est représenté sur la figure 3.13. Le signal de l'accéléromètre calibré est utilisé pour obtenir le Roll et le Pitch par les équations 1 et 2. En revanche, une unité de compensation de l'inclinaison est mise en œuvre, qui utilise un signal de magnétomètre en combinaison avec le Roll et le pitch pour calculer la rotation sur l'axe des Z (Yaw).

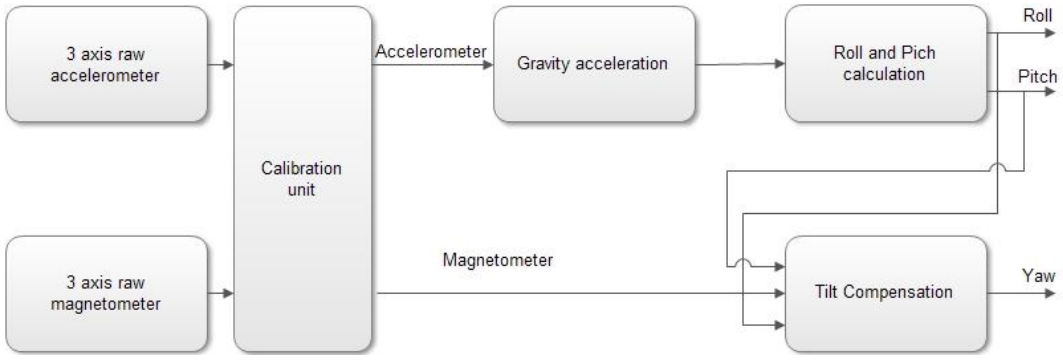


Figure 3.13 *Système de fusion de capteur*

L'accéléromètre donne la mesure basée sur l'accélération linéaire et l'accélération de la pesanteur [149]. Le problème des accéléromètres est qu'ils mesurent à la fois l'accélération linéaire et l'accélération liée à la gravité, qui est dirigée vers le centre de la terre. Etant donné qu'il ne peut pas faire la distinction entre ces deux accélérations, il est nécessaire de séparer accélération de la pesanteur et le mouvement par filtrage.

Par exemple, sur l'axe des X, l'accélération liée à la gravité peut être calculée de la manière suivante :

Initialement Xg = 0.

$$Xg = X * alpha + (Xg * (1 - alpha)). \quad (3.1)$$

Avec Alpha = 0.5 (comme le présente [35]) et X la valeur de l'accélération sur l'axe des x fournit par l'accéléromètre.

En utilisant la sortie de l'accéléromètre, la rotation autour de l'axe X (Roll) et autour de l'axe Y (Pitch) peut être calculée. Si Accel_X, Accel_Y et Accel_Z sont des mesures de l'accéléromètre (accélération de la pesanteur) dans les axes X, Y et Z, les équations (17) et (18) montrent comment calculer les angles Roll et Pitch [36]:

$$Pitch = \arctan\left(\frac{\text{Accel\_X}}{(\text{Accel\_X})^2 + (\text{Accel\_Z})^2}\right) \quad (3.2)$$

$$Roll = \arctan\left(\frac{\text{Accel\_Y}}{(\text{Accel\_Y})^2 + (\text{Accel\_Z})^2}\right) \quad (3.3)$$

Si α, β et γ représente respectivement le Roll, Pitch et Yaw, et si mx, my et mz sont les sorties du magnétomètre, alors le Yaw est calculé de la manière suivante :

$$XH = mx \cos(\beta) + my \sin(\beta) \sin(\alpha) + mz \sin(\beta) \cos(\alpha) \quad (3.4)$$

$$YH = my \cos(\alpha) + mz \sin(\alpha) \quad (3.5)$$

$$\gamma = \text{atan2}\left(\frac{-YH}{XH}\right) \quad (3.6)$$

- **Détection de chute**

Le principe de la chute doit être bien appréhendé tout d'abord afin de développer un algorithme de détection de chute efficace.

a) Analyse des données

Quand une personne âgée tombe avec sa canne, la valeur de l'accélération linéaire sur l'axe des Y sera inférieure à -5 et la valeur de l'accélération linéaire sur l'axe des X ou Z sera supérieure à 5 comme montre la figure 3.14.

Les valeurs de seuil minimal ont été obtenues après plusieurs tests. En fait, nous avons mesuré les valeurs de l'accélération en tombant avec la canne.

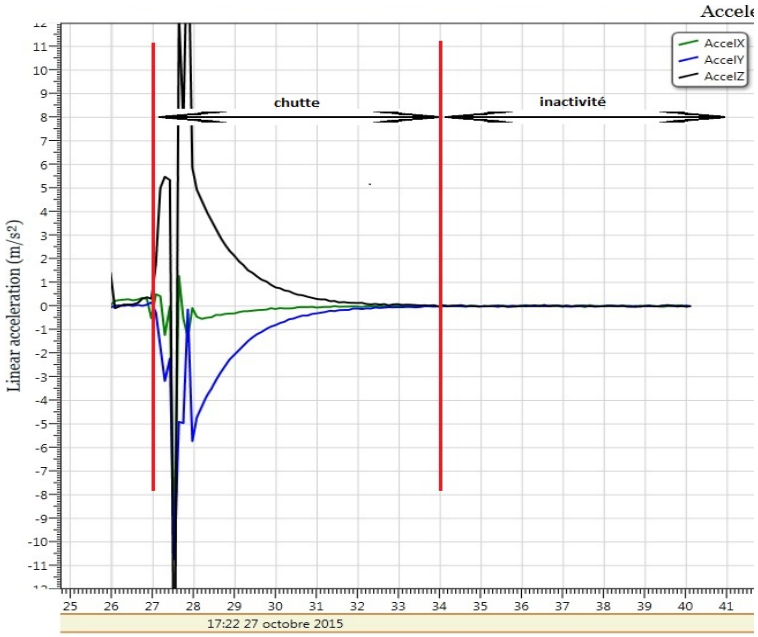


Figure 3.14 *Détection d'une chute par l'analyse de l'accélération linéaire*

De plus, quand la personne âgée tombe avec sa canne, la valeur de l'accélération liée à la gravité sur l'axe des Y tend vers 0 et la valeur absolue de l'accélération liée à la gravité sur l'axe des X ou Z augmente, comme le montre la figure 3.15.

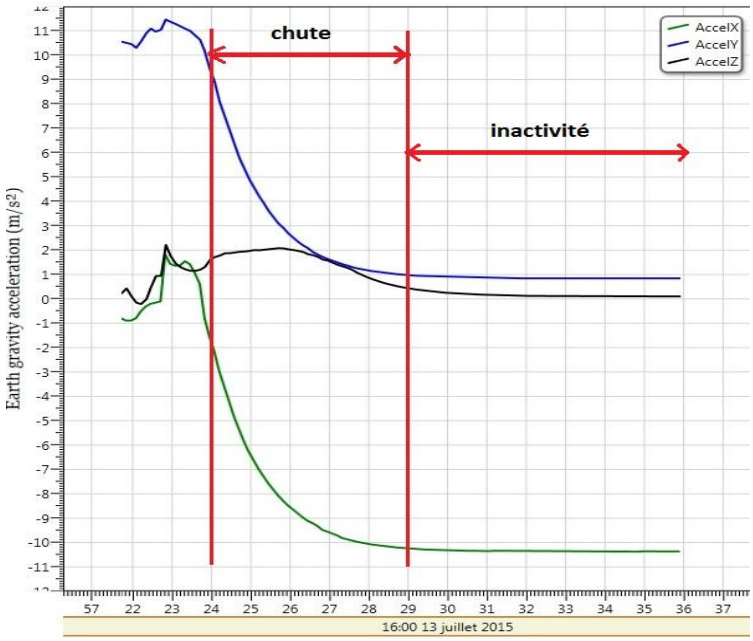


Figure 3.15 *Détection d'une chute à travers l'accélération liée à la gravité*

Après une analyse des données des capteurs, nous pouvons identifier qu'une chute typique pour un utilisateur de canne se compose d'un processus en trois étapes : (i) la chute, (ii) la position horizontale, (iii) l'inactivité.

Pendant la phase de chute, l'utilisateur perd l'équilibre et tombe vers le sol dans un mouvement accéléré. Il a été supposé et vérifié que la canne va suivre un processus de chute libre similaire, même si l'utilisateur perd le contrôle de la canne. Nous modélisons cette chute et nous calculons le seuil minimal de l'accélération lorsqu'une personne âgée tombe. Nous avons identifié par de nombreuses expérimentations que le seuil minimal est égal à 5 ms².

Après la phase de chute, on retrouve la phase identifiable par l'inclinaison de la canne. La position de cette dernière devient quasi horizontale, l'accélération linéaire sur l'axe des Y est quasi égal à 0.

L'étape d'inactivité est évidemment l'étape la plus facile à modéliser et à détecter, nous avons choisi une durée de 30 secondes durant laquelle la canne ne doit pas pratiquement pas bouger pour confirmer la chute effective. Sinon, cela veut dire que la personne vient de reprendre sa canne pour continuer de marcher, la chute est donc moins grave, ou il s'agit simplement d'une perte de contrôle de la canne par la personne.

b) Algorithme

L'algorithme de détection de chute que nous avons implémenté est représenté dans la figure 3.16.

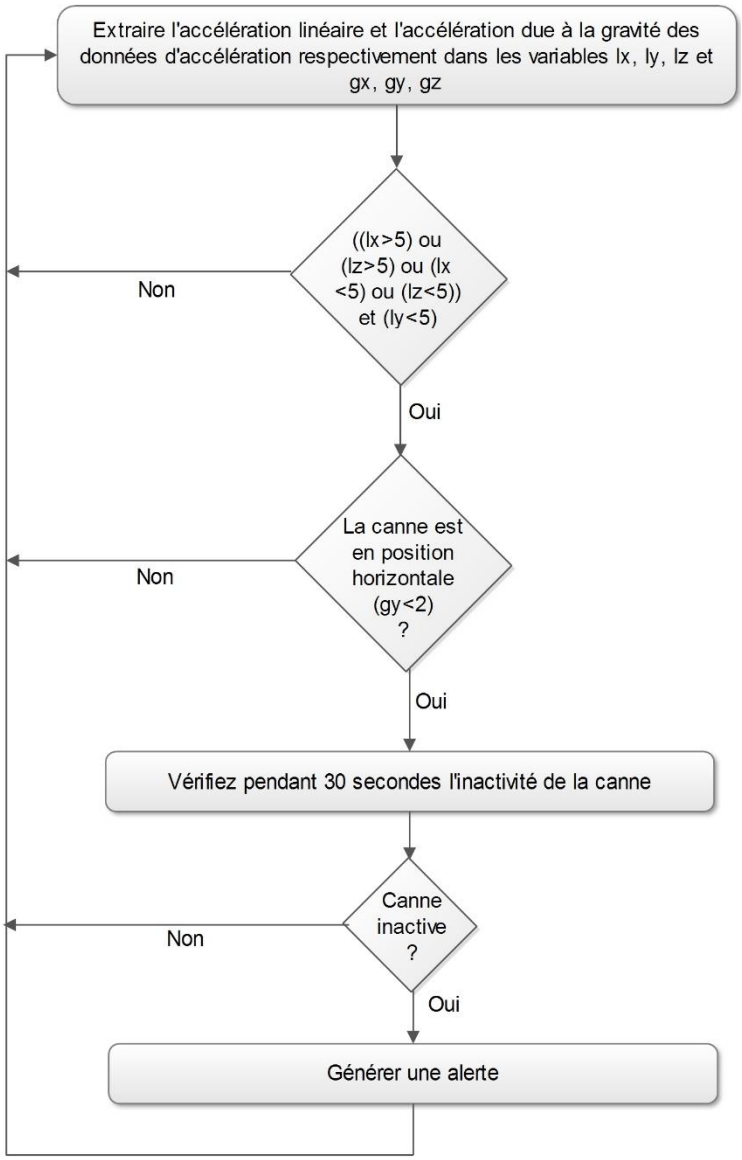


Figure 3.16 *Algorithme de détection de chute.*

- **Nombre de pas**

Le mécanisme de marche doit être lui aussi bien analysé afin de développer un algorithme de détection de nombres de pas efficace.

a) Analyse des données

Nous pouvons utiliser l'accélération linéaire pour déterminer si la personne est en train de marcher en utilisant sa canne de marche par l'observation du changement de l'accélération linéaire sur l'axe X, Y et Z comme le montre la figure 3.17.

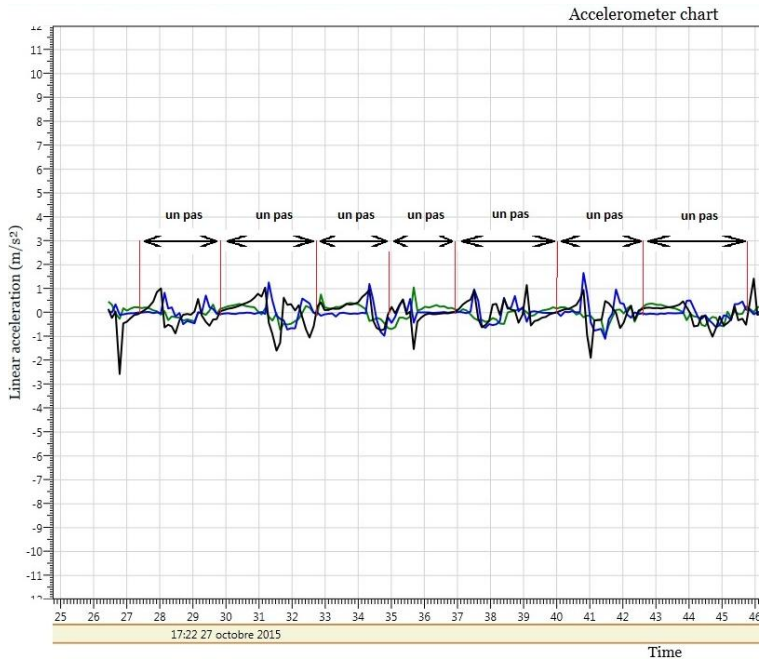


Figure 3.17 *Détection d'un pas à travers l'accélération linéaire*

Lorsque une personne âgée marche avec sa canne, la valeur de l'accélération liée à la gravité sur l'axe des y reste supérieur à 9 m/s² comme montre la figure 3.18.

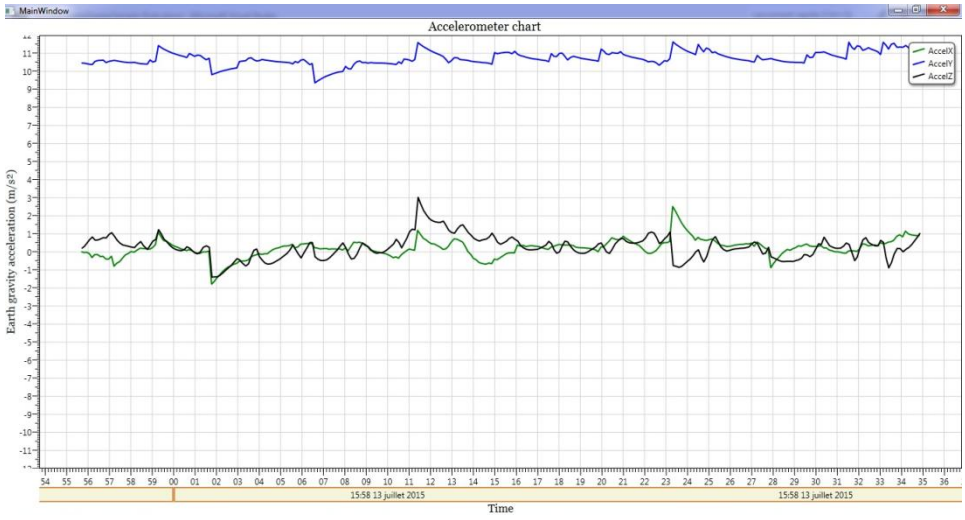


Figure 3.18 *Détection d'un pas à travers l'accélération liée à la gravité*

Après une analyse des données des capteurs, nous pouvons dégager qu'un pas pour un utilisateur de canne se compose d'un processus en deux étapes : (i) accélération sur l'axe des z et l'axe des y, (ii) position verticale.

Pendant la 1ère phase, pour aider à marcher, la canne monte vers le haut et se déplacer en avant, ce qui engendre une accélération sur l'axe des z et l'axe des y, le seuil minimal de cette accélération est de 0.5 ms2. Ce seuil a été évalué par plusieurs tests de marche avec la canne. La figure 3.17 montre que l'accélération linéaire sur l'axe des z augmente avant l'accélération linéaire sur l'axe des y avec une période qui ne dépasse pas le 0,3 secondes.

Pendant la marche, la canne reste en position verticale avec une petit inclinaison qui ne dépasse pas 20 degrés et le seuil minimal de l'accélération liée à la gravité sur l'axe des y est 9 ms^2.

b) Algorithme :

Après avoir analysé les variations de l'accélération linéaire et l'accélération liée à la gravité nous avons implémenté un algorithme de détection d'un pas automatique :

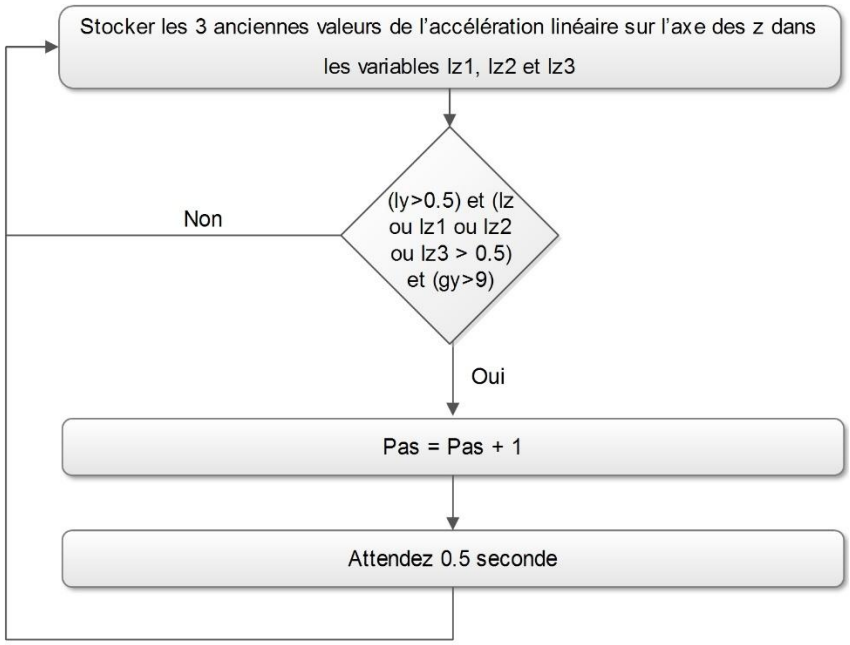


Figure 3.19 *Algorithme de détection d'un pas*

Avec ly est l'accélération linéaire sur l'axe des y et gy l'accélération liée à la gravité sur l'axe des y. La période minimale entre deux pas d'une personne âgée est égale à 0.5 seconde. Pour cela, nous avons ajouté une variable compteur pour ne pas confondre un pas à une autre activité.

- **Distance parcourue**

La distance parcourue est relative au mouvement de la canne sur l'axe des z. En fait, lorsque la personne marche avec sa canne, l'accélération sur l'axe des z augmente puis elle diminue puis elle retourne à 0. Ceci est identique au raisonnement pour le calcul du nombre de pas.

En général, pour calculer une distance à partir de l'accélération, il faut utiliser la formule suivante :

Si en prend a = accélération constante pendant une période t alors :

Vitesse v(t) = a*t + v0 ; avec v0 = vitesse initiale ;

Distance parcourue :

$$s(t) = ½ \times a \times t^2 + v0 \times t \qquad (3.7)$$

Dans notre cas t = 100 ms, et nous avons calculé la vitesse et la distance parcourue chaque fois qu'un pas est détecté, l'algorithme de calcul de la distance parcourue fonctionne de la manière suivante :

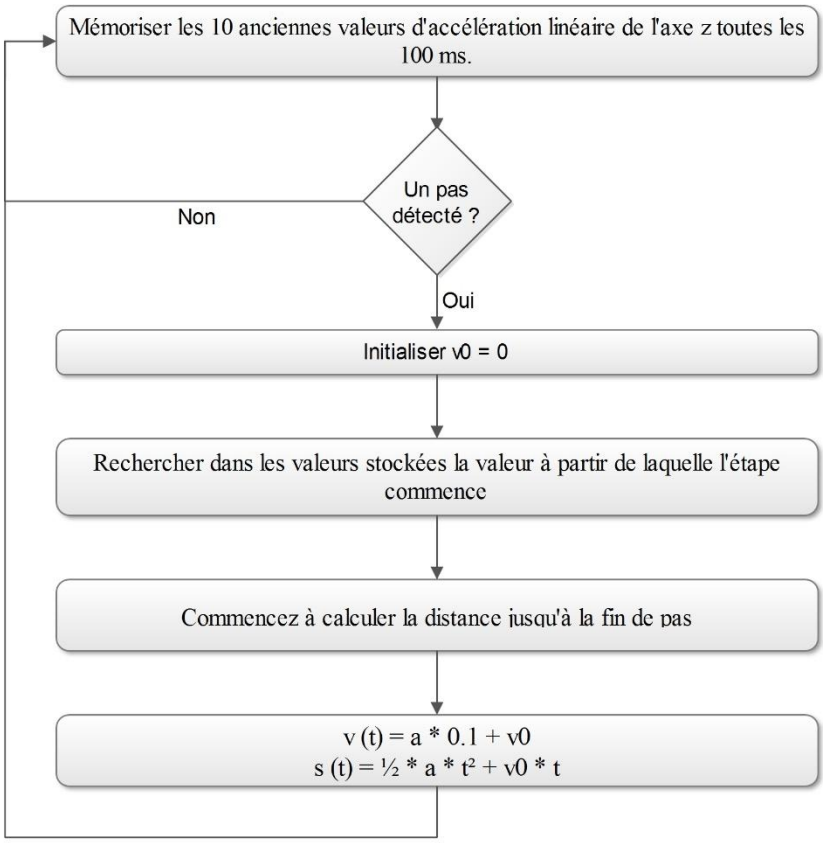


Figure 3.20 *Algorithme de calcul de la distance parcourue.*

Concernant les données GPS pertinentes, le système ne cesse de demander la position nouvellement occupée. Une fois indisponible (par exemple, un emplacement intérieur), la canne enverrait la position GPS la plus récemment enregistrée, ainsi que les données de date et d'heure associées. Nous envisageons également de mettre en place un système spécial de localisation en intérieur utilisant l'UWB, en complément du GPS [146].

3.4.3. Communication entre canne et station de base

L'émetteur positionné sur la canne s'engage à envoyer des données à la station de base au moyen de LoRa, susceptible d'envoyer un message à la canne portant une demande de données. La transmission radio, comme le suppose notre étude de cas, applique une bande de fréquences du type ISM (industriel, scientifique et médical) à 866 MHz. En réalité, les bandes ISM [150] sont des bandes de fréquences susceptibles d'être appliquées dans un petit espace à des fins industrielles, scientifiques, médicales, domestiques ou similaires.

En fait, pour toute personne utilisant une radio pour communiquer sur une distance donnée, quel que soit le type de communication utilisé, la capacité de communication reste généralement une préoccupation primordiale, ce qui nous incite à faire une nouvelle tentative pour tenter de trouver une facteur ou source fiable susceptible de nous aider à améliorer la plage de capacités.

L'équation appliquée pour décrire le comportement de cette onde dans un environnement «espace libre» est celle conçue par H.T. Friis [151], a également tamponné l'équation de transmission de Friis, définie comme suit:

$$P_R = P_T G_T G_R (\frac{1}{d})^2 \times \left(\frac{\lambda}{4\pi}\right)^2 \quad (3.8)$$

Où

PR = puissance reçue (watts)

PT = puissance transmise (watts)

GT = gain d'antenne d'émission (scalaire)

GR = gain de l'antenne de réception (scalaire)

ƛ = longueur d'onde

d = distance séparant l'émetteur et le récepteur

n = exposant pour les conditions environnementales (n = 2 définit «espace libre»).

Tableau 3.3 *Valeur de "n" [152]*

Environnement	Valeur n
Espace libre	2
Épicerie	1.8
Magasin de détail	2.2
Bureau (murs durs)	3
Bureau (murs souples)	2.6
Télédéverrouillage	4

Dans sa forme de base, l'équation indique que l'intensité de l'onde radioélectrique électromagnétique reçue à un endroit donné est fonction de: (a) l'intensité du signal transmis d'origine, (b) les performances des antennes au niveau de l'émetteur et du récepteur, (c) la longueur d'onde correspondant à la fréquence de fonctionnement, et (d) la distance séparant l'émetteur et le récepteur.

L'équation de Friis telle qu'elle est formulée en décibels se révèle être :

$$P_R(dB) = -20\,log\left(\frac{\lambda}{4\pi}\right) - 10n\,log(d) + P_T + G_T + G_R \quad (3.9)$$

La perte de chemin telle que rendue sous forme scalaire (où GT = GR = 1) ressemble à ceci :

$$L_{PATH} = \frac{P_R}{P_T} = \left[\frac{\lambda}{4\pi}\right]^{2\left[\frac{1}{d}\right]^n} \text{ (3) [28]} \quad (3.10)$$

La perte de trajet sous forme de décibels (où GT = GR = 1) est décrite comme suit :

$$L_{PATH}(dB) = P_R - P_T = 20\,log(\frac{\lambda}{4\pi}) - 10n\,log\left(\frac{1}{d}\right) \quad (3.11)$$

L'équation générique du tableur du calculateur de distance, telle que résolue pour la distance d, prend la forme suivante :

$$d = \frac{\lambda}{4\pi 10^{\frac{a_r}{20}}} \quad (3.12)$$

Avec: a_r = Perte de chemin + marge de fondu

En se basant sur l'équation 24, nous pouvons bien conclure que le facteur important affectant la plage de transmission s'avère être la longueur d'onde.

LoRa définit le facteur d'étalement du spectre (SF) par la formule suivante: SF = log2 (Rc / Rs), Rc étant le débit du message transmis (Chirp) et Rs, le débit du symbole à transmettre. L'augmentation du facteur de propagation permet de couvrir une plus grande distance entre l'équipement et la passerelle au détriment de la bande passante disponible.

Les largeurs de bande possibles à configurer pour un canal sont de 125, 250 et 500 kHz pour la bande des 868 MHz, ce qui permet d'atteindre un débit maximal de 27 kbit / s avec une largeur de bande de 500 kHz et un facteur de propagation de 7.

Le module RF95 a quatre configurations qui sont :

- Bande passante = 125 kHz, Cr (taux de correction d'erreur) = 4/5, Sf (facteur de propagation) = 128puce / symbole
- bw = 500 kHz, Cr = 4/5, Sf = 128puce / symbole
- bw = 31,25 kHz, Cr = 4/8, Sf = 512puce/ symbole
- Bw = 125 kHz, Cr = 4/8, Sf = 4096puce/symbole

Nous avons décidé d'utiliser la configuration numéro 4, car elle présente le facteur d'étalement le plus élevé et un petit BW.

Après avoir ajusté la valeur de configuration, nous déterminons les quatre nœuds associés au protocole de transmission, à savoir le mode normal, le mode veille, le mode descendant et le mode demande, comme indiqué ci-dessous.

- Le mode normal: il est activé tout au long du processus de mouvement de la canne, c'est-à-dire lorsqu'elle se déplace. Dans ce cas, le nœud émetteur s'engage à envoyer une trame à la station de base régulièrement, à savoir toutes les dix minutes ; les données encapsulées dans la trame sont détaillées dans le tableau 3.4.
- Le mode veille: ce mode est appliqué chaque fois que la canne ne bouge pas (par exemple la nuit). Dans ce cas, le nœud émetteur envoie une trame à la station de base toutes les heures. Si la canne reprend son état de mouvement à nouveau, le mode normal est activé. Le mode de requête: durant lequel la station de base propose d'envoyer une trame de requête au nœud positionné de la canne. Les données encapsulées dans la trame sont détaillées dans le tableau 3.5.

- Le mode de chute: cet état est activé ou atteint chaque fois qu'une chute est détectée. Dans ce cas, le nœud émetteur s'engage à envoyer une trame régulière à la station de base (toutes les 100 ms) pour visualiser l'état de la canne en 3D, pour une reconnaissance plus explicite de l'état de la canne. Les données encapsulées dans la trame sont décrites dans le tableau 3.6.

Tableau 3.4 *Mode normal*

Nom	Description	taille (byte)
CaneId.	Identifiant unique de la canne	16
Status	Status de la canne	1
Longitude	GPS longuitude	16
Latitude	GPS latitude	16
Distance	Distance parcourue	16
Steps	Nombre de pas	16
Fall	Détection de chute	1

Tableau 3.5 *Mode requête*

Nom	Description	Taille (byte)
CaneId.	Identifiant unique de la canne	16
Request	Code de la requette	32

Tableau 3.6 *Mode chute*

Name	Description	Size (byte)
CaneId.	Identifiant unique de la canne	16
Longitude	GPS longuitude	16
Latitude	GPS latitude	16
Roll	Rotation sur l'axe des X	16
Pitch	Rotation sur l'axe des Y	16
Yaw	Rotation sur l'axe des Z	16

3.4.4. Station de base

En ce qui concerne la station de base, elle consiste en une carte Raspberry Pi 2 [153] équipée d'un module radio Chistera Pi [154] développé par Snootlab à double interface radio (866 et 433 MHz). les spécifications techniques de Chistera-Pi :

- Emetteur-Récepteur (G)FSK Longue portée 868 Mhz : RFM95W compatible LoRa
- Emetteur-Récepteur FSK courte portée 434 Mhz : RFM22
- Deux connecteurs d'antenne : UFL et SMA

- Taille : celle de la carte HAT du Raspberry Pi
- Emetteurs/récepteurs connectés au GPIO
- Zone de prototypage disponible pour l'utilisateur
- Ports GPIO du Raspberry Pi accessible + sortie des 26 premiers sur pastilles à souder

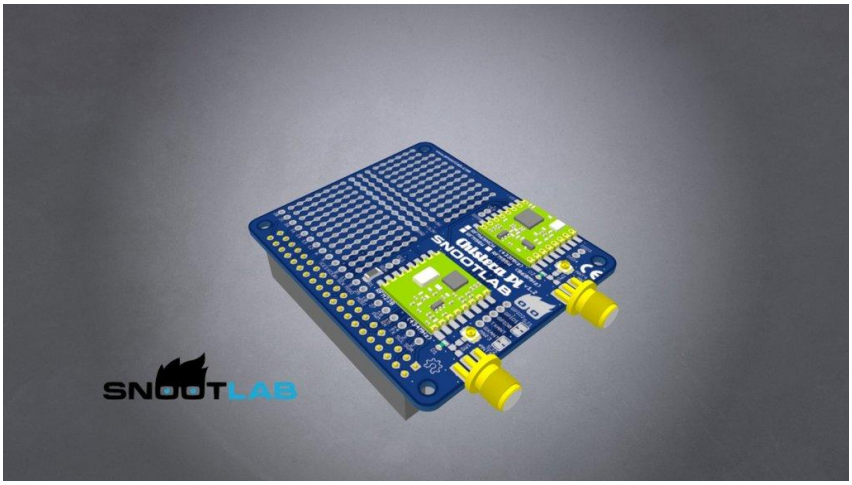


Figure 3.21 *Module radio ChiesteraPI*

Les spécifications techniques de Raspberry pi 2:

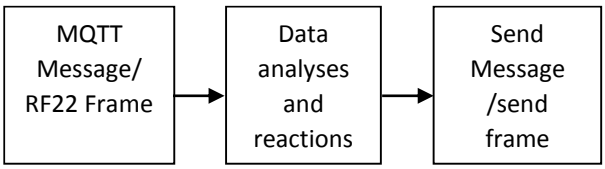
- Ram : 1 Go.
- Nombre de processeur : 4.
- Processeur : ARMv7 (~6x plus puissant)
- Cadence du processeur : 900 Mhz.
- Supporte Windows 10 : Oui.
- Stockage : Carte MicroSD.
- Ports : 4 USB 2.0.
- Puissance : 600 mA (3,5 W)

Figure 3.22 *Carte Raspberry PI*

En conséquence, une carte Raspberry PI a été équipée d'une carte d'interface radio Chistera Pi. À cet égard, un langage de programmation Python est appliqué pour développer un script particulier permettant de conserver les fonctionnalités de la station de base. En ce qui concerne le serveur, les AWS (Amazon Web Services) ont été appliqués pour englober le courtier MQTT Mosquitto [155] et l'application Java relative aux données de sauvegarde.

3.4.5. Déroulement protocolaire de la station de base

Un modèle mathématique consiste en la description du système à l'aide de concepts mathématiques et linguistiques. À cet égard, un modèle de dérision semblerait quelque peu utile pour expliquer le système et étudier les effets associés aux différents composants. Cette modélisation est également utile pour certaines prédictions concernant le comportement approprié. En ce qui concerne notre contexte particulier, une description sera faite concernant le comportement pertinent de la station de base lors de la réception de messages via le MQTT ou de données via le RFM95.



Le système complet comprend les ensembles de I, O, F, Fc, Sc, détaillés comme suit.

S = {I, O, F, Fc, Sc}

I: ensemble d'entrées.

O: ensemble de sorties.

F: ensemble de fonctions.

Fc: ensemble de cas d'échec.

Sc: Ensemble de cas de réussite.

Contribution:

• Message reçu avec MQTT

• cadre reçu en utilisant RFM95

Sortie:

• cadre RFM95

• message MQTT

Les fonctions:

• S'abonner à un sujet

• vérifier l'existence d'une trame RF95

• La prise de décision

• Cadre d'envoi utilisant le module RFM95

• Envoi d'un message MQTT à l'aide d'un courtier MQTT

Cas d'échec:

• Impossible de se connecter au courtier MQTT

• Impossible d'obtenir le cadre RFM95

Impossible d'envoyer le cadre RFM95

Cas de réussite:

• RFM95 a été envoyé avec succès

• Le message MQTT est envoyé avec succès

En se basant sur le schéma décrit ci-dessus, nous pourrions bien en déduire que la station de base est chargée à la fois d'assurer l'interopérabilité et l'automatisation du système de surveillance.

3.4.6. Communication via MQTT

Dans cette section, la conception du message IoT est décrite sur la base du protocole MQTT, comme indiqué pour la mise en œuvre dans notre scénario M-Health.
Le tableau 5 ci-dessous met en évidence le message IoT applicable au fonctionnement du protocole MQTT. Les messages IoT concernent les informations relatives à la canne, les demandes d'informations ainsi que les alertes de détection de chute. Pour chaque type de message, l'en-tête associé à MQTT est fourni, ainsi que l'identification des thèmes de publication et d'abonnement pertinents, ainsi que la définition de l'abonné ayant pris des mesures à la suite de la réception du message.

Comme indiqué dans le tableau 3.7, une détermination du système de gestion de sujets pour la communication MQTT est définie pour le niveau de sécurité et de fiabilité le plus optimal à atteindre. À noter que le symbole "#" désigne tout caractère de chaîne et que le sujet est conçu pour comporter trois parties principales, à savoir:

La nomenclature CANET désigne notre système de surveillance;

Le Appcode, qui représente le code attribué à chaque application différente;

De plus, le CaneID, qui représente l'identifiant de la canne mobile dérivé de la trame RF95, à des fins de fiabilité accrue des données.

Tableau 3.7 *Système de gestion de sujets*

Message MQTT	Sujet MQTT	Publisher	Subscriber
Informations	CANet/sendappcode/CaneId	Station de base	Client MQTT
Requette	CANet/recappcode/#	Client MQTT	Station de base
Detection de chute	CANet/fallappcode/#	Station de base	Client MQTT

Le processus de communication entrepris via le MQTT est expliqué en détail à la figure 3.23 ci-dessous. En conséquence, la canne continue à calculer le paramètre toutes les 100 ms pour déterminer le mode de fonctionnement exact (normal, en baisse ou en veille). Pendant chaque période de déchéance des modes, la canne s'engage à envoyer une trame à la station de base et, en fonction des données associées à la canne (chute, déplacement, etc.), la station de base décide dans quel sujet elle doit publier, comme indiqué sur le tableau précédent. En conséquence, le client MQTT doit être abonné au sujet correspondant pour pouvoir recevoir le message et effectuer les interactions pertinentes nécessaires.

Pour que la fréquence de transmission de données soit minimisée et que le système de notification de demande soit activé, le mode de notification de demande a été mis en œuvre. Une fois le smartphone connecté, l'utilisateur peut envoyer une demande d'informations à la canne; celle-ci répond immédiatement, comme illustré à la figure 3.24.

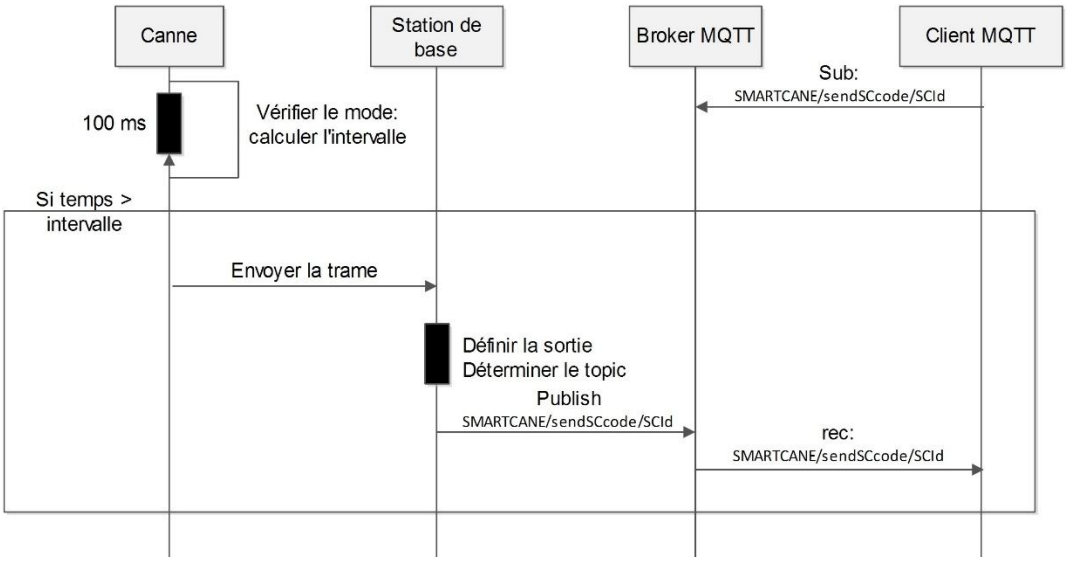


Figure 3.23 *Communication canne avec les objets connectés*

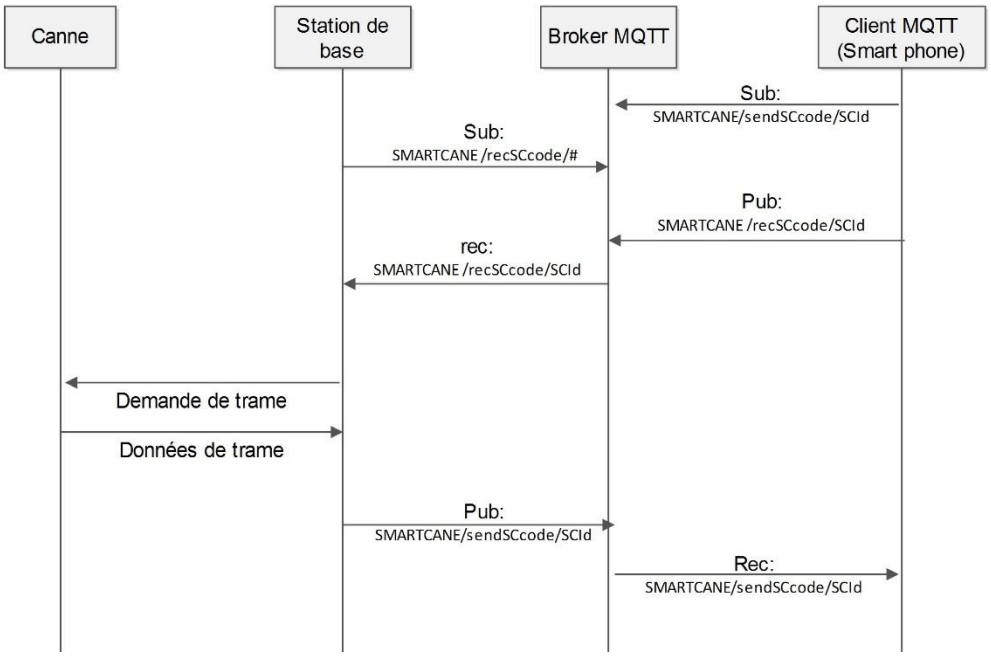


Figure 3.24 *Communication objet avec la canne*

Dans ce scénario, le client MQTT publie un message dans la rubrique "CANet / recappcode / caneid" demandant la mise à jour des informations associées à la canne pour l'activation des modes normal, veille ou descente. Ensuite, la station de base, abonnée à la rubrique "CANet / recappcode / #", recevra le message et exécutera un processus de demande d'informations disséqué sur la canne à l'aide de caneid, tel qu'il est extrait de la rubrique. Il consiste à envoyer une trame de requête telle qu'elle a été extraite du destinataire, puis à obtenir une autre trame à renvoyer au sujet spécifié.

3.5. Tests et résultats

3.5.1. Plateforme expérimentale de détection de chute

Une plateforme de chute sécurisée a été mise en place pour l'expérience. Elle est constituée d'un coussin moelleux pour que la personne tombe dessus sans dommage, et une surface plus dure pour la canne. La position et l'orientation du coussin sont ajustées pour tenir compte de différents types de chutes.

Tableau 3.8 *Le taux de détection de chute (20 essais) pour les types de chute différente*

Personne	1	2	3	4
En avant	100%	100%	100%	100%
En arrière	90%	100%	100%	100%
A côté	100%	100%	95%	100%

- En avant : simule une chute de face lié par exemple à un trébuchement
- En arrière : simule une chute sur le dos, par exemple en raison d'un glissement

- A côté : simule une chute vers le côté en raison d'une perte d'équilibre par exemple.

Les résultats énumérés dans le tableau 3.8 montrent un taux de détection près de 100% pour les trois types de chutes effectuées par les quatre personnes. La différence de poids et la hauteur entre les personnes semblent avoir peu d'effet sur les résultats finaux.

Tableau 3.9 *Taux de faux positifs pour diverses activités (20 essais).*

Personne	1	2	3	4
Marche lente	0%	0%	0%	0%
Marche rapide	0%	0%	0%	0%
Balancement de la canne	0%	0%	0%	0%
s'asseoir et se tenir	5%	0%	0%	5%
Poser sur les genoux	0%	5%	0%	0%

- Marche lente : marche avec la canne à un rythme inférieur à un pas par seconde.
- Marche rapide : marche avec la canne à un rythme autour de deux pas par seconde.
- S'asseoir et se tenir : se mettre debout avec l'aide de la canne à partir d'une position assise.
- Balancement de la canne : balancement de la canne en va-et-vient à une fréquence de 1 Hz avec un angle inférieur à 30 degrés par rapport à l'axe vertical.
- Poser sur les genoux : Ramasser la canne orienté verticalement et la posant à plat sur les genoux en position assise.

Les résultats énumérés dans le tableau 3.9 montrent que l'algorithme est robuste en termes de taux de faux positifs.

3.5.2. Nombre des pas

Tableau 3.10 *Nombre de pas mesuré par l'algorithme pour 10 pas prise par les quatre personnes.*

Personne	1	2	3	4
Marche lente	10	11	10	9
Marche rapide	8	9	8	10

Le tableau 3.10 montre qu'avec une marche lente, le nombre de pas détecté est presque le même que le nombre de pas réalisés par les personnes. Par contre, avec une marche rapide, le système détecte moins de pas. Ceci est sans doute à cause de la période qui sépare deux pas (0.5 secondes) utilisés dans l'algorithme de détection de pas. Pour corriger cela on peut éliminer cette période mais il faut trouver une autre méthode pour séparer deux pas successive.

Tableau 3.11 *Taux de faux positifs pour diverses activités (20 essais).*

Personne	1	2	3	4
Chute	0%	0%	0%	0%
Balancement de la canne	5%	0%	0%	10%
s'asseoir et se tenir	5%	0%	0%	5%
Poser sur les genoux	0%	5%	0%	0%

Le tableau 3.11 montre que l'algorithme de détection de pas est robuste puisque le taux de faux positifs est presque égal à 0% pour des diverses activités.

3.5.3. Distance parcourue

Tableau 3.12 *La distance mesurée par l'algorithme pour 10 mètre de marche.*

Personne	1	2	3	4
Distance mesurée	12.5	8.5	9.2	12.4

Le tableau 3.12 montre que l'algorithme n'est pas très efficace et que la différence de poids et la hauteur entre les personnes semblent avoir un effet sur les résultats finaux. Ceci est à cause de la perte des données transmises, et à cause de l'utilisation de l'axe de z seulement dans l'algorithme. Il faut donc trouver une méthode pour calculer la distance parcourue par rapport l'axe des z et l'axe des x.

3.5.4. Communication entre canne et environnement

Pour que la fiabilité de la messagerie soit maintenue, trois niveaux de QoS sont pris en charge via le MQTT. En ce qui concerne le niveau de qualité de service le plus élevé, davantage d'échanges de paquets s'imposent. En effet, plus le niveau de service QoS est élevé, plus il sera efficace si aucune perte de message ne constitue l'objectif principal ou l'exigence. La perte de messages et le délai de bout en bout sur le réseau sans fil ont été examinés, ainsi que les affichages de corrélation pertinents, en termes de charge utile et de niveaux de qualité de service. Le délai de bout en bout enregistré pour prévaloir entre la station de base et un client MQTT correspondant aux trois niveaux de QoS relatifs aux charges de transmission est testé pour un cas de taille de message inférieur à 20 Ko.

Tableau 3.13 *Test de 3 niveaux de QoS*

QOS	Message loss (100 messages)	Delay (millisecond)
QOS 0	3%	0.4
QOS 1	0%	0.5
QOS 3	0%	0.8

Les résultats présentés dans le tableau 3.13 indiquent bien que l'écart de retard persistant entre QOS 0 et QOS 1 n'est que de 0,1 seconde, alors que l'efficacité de la transmission s'avère nettement meilleure en ce qui concerne la QOS 1 (enregistrement d'aucune perte de message). Pour cette raison, nous avons envisagé d'appliquer le niveau 1 de QoS.

En ce qui concerne le niveau de consommation d'électricité de la canne à sucre, il est mesuré sur une base de 12 heures, soulignant que la consommation d'énergie ainsi que les taux de temps ont augmenté linéairement. En effet, pour T = 5 min, il apparaît clairement que la quantité d'électricité consommée s'avère supérieure à celle consommée à T = 10 min. De plus, et au fil du temps, il a été découvert que la connexion était le témoin de certaines perturbations. Par conséquent, pour les débits de puissance enregistrés et la stabilité du système, on est tenté de considérer que la sélection générale de T = 10 min s'avère plus appropriée. Calculé en termes de T = 10 min, le taux horaire de consommation d'électricité semble être de 0,76 J, soit 24 heures, soit 18,24 J contre 179 J pour un système de transmission basé sur le GPRS.

Pour évaluer la plage de transmission, nous avons calculé le pourcentage de perte de paquet correspondant aux quatre configurations, comme expliqué précédemment :

• Config1: Bw = 500 kHz, Cr = 4/5, Sf = 128puce / symbole

• Config2: Bw = 125 kHz, Cr = 4/5, Sf = 128puce / symbole

• Config3: Bw = 31,25 kHz, Cr = 4/8, Sf = 512chips / symbole

• Config4: Bw = 125 kHz, Cr = 4/8, Sf = 4096chips / symbole

La figure 3.25 montre que la meilleure configuration pour une communication à longue portée est config1, qui présente la valeur maximale du facteur d'étalement et une faible bande passante.

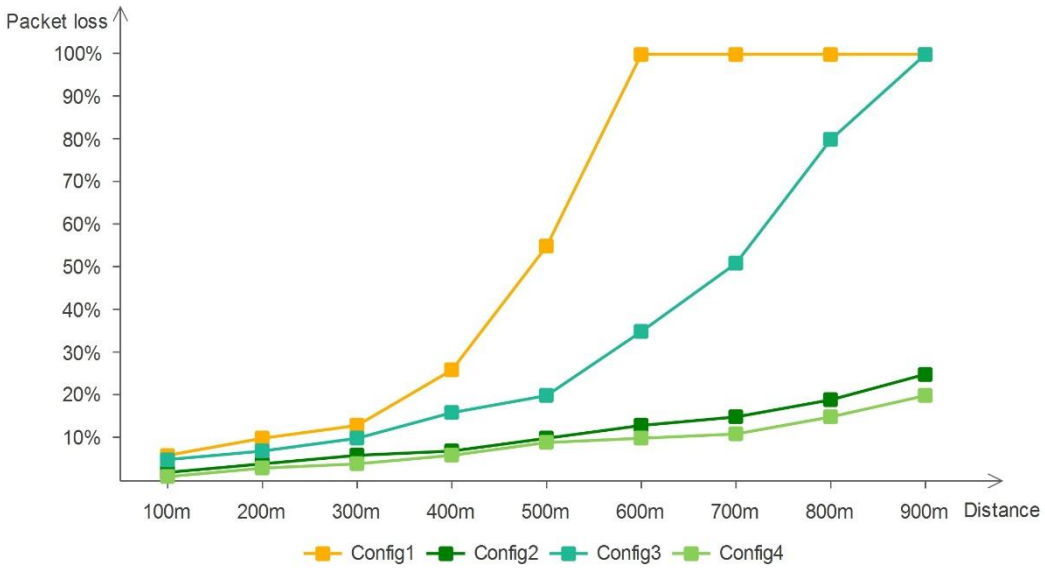


Figure 3.25 *Perte de paquets en fonction de la distance pour chaque configuration*

La figure 3.26 décrit le nombre moyen de pertes de paquets pour chaque système en fonction de la distance d'utilisation moyenne. Notre système est bien positionné par rapport aux résultats d'acheminement des autres examens. En effet, pour une distance moyenne significative, il en résultait une perte de paquets réduite par rapport aux autres. De plus, les valeurs maximales enregistrées valident ce résultat car la perte n'est pas importante. De plus, selon la courbe de la figure 10, la perte de paquets n'est pas importante pour de petites distances, même pour de grandes distances. Par conséquent, malgré la longue distance, le nombre moyen de pertes de paquets de notre solution est inférieur à celui des autres solutions.

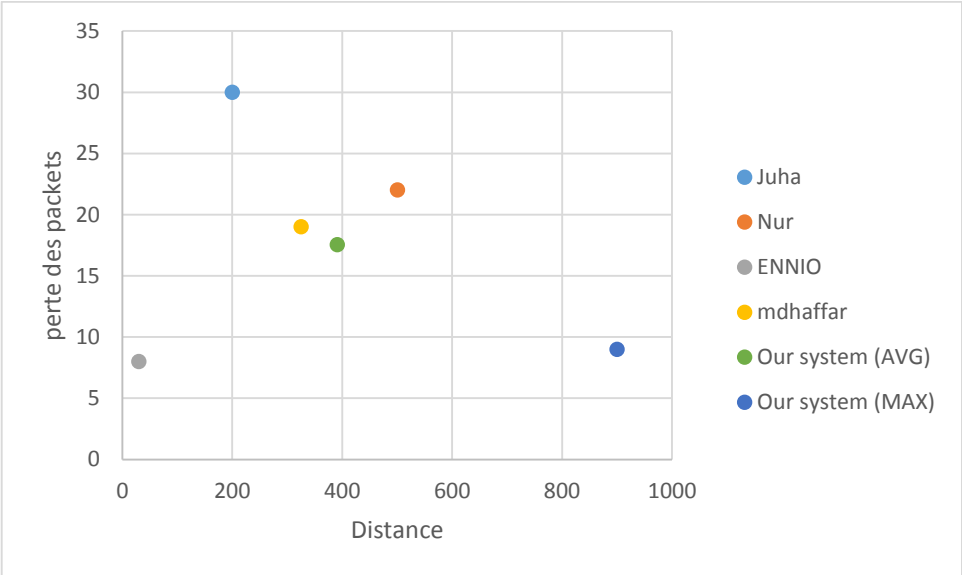


Figure 3.26 *Les pertes des paquets en fonction de distance pour chaque système*

3.4. Conclusion

Dans ce chapitre, une nouvelle architecture pour la surveillance des personnes âgées a été proposée, qui utilise LoRa pour les communications longue portée et faible consommation, ainsi que le protocole MQTT pour assurer l'interopérabilité. En premier lieu, la canne transmet des données relatives à son état (position GPS, détection des chutes et comptage des pas) à la station de base via LoRa. En second lieu, la station de base transmet ces données via MQTT à un sujet spécifique. Nous avons équipé la canne d'un nœud d'émetteur composé d'une carte 3.2 et d'un capteur magnétique LSM303DLHC avec module GPS, et d'un émetteur-récepteur LoRa connecté à une BS (Raspberry Pi avec Chiestera Pi), servant à envoyer des messages à différents objets via les protocoles MQTT. Le résultat indique bien que notre système est robuste et efficace et qu'il pourrait être utilisé dans une ville intelligente.

Conclusion générale

Les communications M2M doivent jouer un rôle important dans la réalisation de l'IOT. Cependant, jusqu'à présent, les communications M2M n'ont pas de protocole MAC simple, efficace et robuste. Nous proposons un protocole MAC hybride évolutif pour les communications M2M. En plus, Nous proposons un nouveau système de surveillance des personnes âgées utilisant leur canne de marche interopérable.

Nous avons commencé par décrire le contexte de l'internet des objets IOT et plus particulièrement l'interopérabilité et ses défis.

Plusieurs travaux existants ont présenté et proposé des solutions pour le problème de l'accès au canal avec de nombreuses méthodes.

Nous proposons un modèle mathématique et des scénarios de simulation pour le réseau qui est composé par une station de base et des machines qui communiquent avec elle. Notre objectif est de maximiser le débit du système.

Les résultats obtenus nous ont offert un débit faisable par rapport à un protocole à base de contention (CSMA p-persistant) et un protocole sans contention (TDMA) ainsi qu'une efficacité énergétique et un délai de transmission plus performant.

Nous avons pu concevoir et simuler un protocole qui combine à la fois les avantages des protocoles avec contention et sans contention.

Afin d'implémenter le protocole MAC proposé, une nouvelle architecture de surveillance des personnes âgées est proposée, qui utilise le modèle LoRa pour une communication à longue portée et à faible puissance, et le protocole MQTT pour l'interopérabilité à maintenir.

En tant que future proposition de travail, nous envisageons d'établir une interaction assez complexe entre un large éventail d'objets connectés, en permettant aux transmissions de messages d'être maintenues via une variété de protocoles, autres que le MQTT, tels que HTTP et XMPP, pour atteindre un niveau d'interopérabilité encore plus élevé. Même si le système de surveillance, tel qu'il est perçu dans le présent travail, est limité à un seul cas de canne avec une seule station de base, nous avons encore l'intention d'étendre encore la portée de transmission de données pour impliquer une multiplicité de cannes et de stations de base. Le but est d'élargir sans limite la portée du processus de surveillance des personnes âgées pour atteindre autant de portée que possible (Smart City). Nous avons l'intention aussi de tester notre système a l'EHPAD de castres avec un grand nombre de personnes âgées dans des conditions réelles pour mieux évaluer les performances de

l’algorithme de détection de chute. Enfin nous trouvons que c’est impératif d’appliquer notre protocole MAC hybride avec LoRaWAN sur le système d’e-santé.

Publications

Papiers journaux :

1. **Abdelfetteh LACHTAR,** Thierry VAL, Abdennaceur KACHOURI: « 3DCane: a monitoring system for the elderly using a connected walking stick » dans IJCSIS, USA, Vol. 14 N. 8, août 2016.
2. Walid ELLILI, **Abdelfetteh LACHTAR**, Mounir SAMET: « Obstacle Avoidance with Regard to a Mobile Robot's Case » dans IJCSIS, USA, Vol. 14 N. 8, août 2016
3. **Abdelfetteh** LA**CHTAR,** Thierry VAL, Abdennaceur KACHOURI "Elderly monitoring system in a smart city environment using LoRa and MQTT" IET Wireless Sensor Systems, DOI: 10.1049/iet-wss.2019.0121

Papier soumis :

1. **Abdelfetteh** LA**CHTAR,** Marwa Lachtar, Awatef Ben Fradj, Abdennaceur KACHOURI " Throughput-optimized hybrid MAC protocol for heterogeneous M2M networks" IET Wireless Sensor Systems

Conférences :

1. Walid Ellili, **Abdelfetteh Lachtar**, Mounir Samet : « A new trajectory optimization approach for safe mobile robot navigation: a comparative study (Khepera II mobile robot) » ISADA 2016.
2. **Abdelfetteh LACHTAR,** Thierry VAL, Abdennaceur KACHOURI : "Real-time monitoring of elderly using their connected walking stick" SM2C 2017.
3. **Abdelfetteh LACHTAR,** Marwa Lachtar, Abdennaceur KACHOURI:" A Hybrid MAC protocol for heterogeneous M2M net-works", ISDA 2019.

Références

[1] 'World Health Organization: Global report on falls prevention in older age', http://www.who.int/ageing/publications/ Falls_prevention7March.pdf, accessed 25 December 2017

[2] N. Ahmed, H, Rahman, and Md.I. Hussain, 'A comparison of 802.11ah and 802.15.4 for IoT', ICT Express, Vol.2, No. 3, Sep. 2016, pp. 100-102.

[3] Catarinucci, L., De Donno, D., Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M.L., Tarricone, L., 'An IoT-Aware Architecture for Smart Healthcare Systems', (2015) IEEE Internet of Things Journal, 2 (6), art. no. 7070665, pp. 515-526.

[4] Yong Lin, Xingjia Lu, Fang Fang, and Jianbo Fan, 'Personal Health Care Monitoring and Emergency Response Mechanisms', First Int. Symp. on Future Information and Communication Technologies for Ubiquitous HealthCare, Jinhua , 1-3 July 2013, pp. 1-5.

[5] A. Lombardi, M. Ferri, G. Rescio, M. Grassi, and P. Malcovati, 'Wearable Wireless Accelerometer with Embedded Fall-Detection Logic for Multi-Sensor Ambient Assisted Living Applications', IEEE Sensors, Christchurch, 25-28 Oct. 2009, pp. 1967-1970.

[6] L. Meinel, M. Findeisen, M. Heß, A. Apitzsch, and G. Hirtz, 'Automated Real-Time Surveillance for Ambient Assisted Living Using an Omnidirectional Camera', IEEE Int. Conf. on Consumer Electronics (ICCE), Las Vegas, NV, 10-13 Jan. 2014, pp. 396 – 399.

[7] J. A. Uribe, J. F. Duitama, and N. G. Gómez, 'Personalized Message Emission in a Mobile Application for Supporting Therapeutic Adherence', 13th Int. Conf. on e-Health Networking Applications and Services (Healthcom), Columbia, MO, 13-15 June 2011, pp. 15-20.

[8] Mahda Noura1, Mohammed Atiquzzaman and Martin Gaedke, "Interoperability in Internet of Things: Taxonomies and Open Challenges", dans Mobile Networks and Applications · July 2018 DOI: 10.1007/s11036-018-1089-9

[9] Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswamia, M. 'Internet of Things (IoT): A vision, architectural elements, and future directions'. Future Gener. Comput. Syst. 2013, 29, 1645–1660.

[10] Evans, D, 'The Internet of Things: How the Next Evolution of the Internet is Changing Everything', Cisco Internet Business Solutions Group: San Jose, CA, USA, 2011.

[11] LoRa Alliance, 'White Paper: A Technical Overview of Lora and Lorawan', the LoRa Alliance: San Ramon, CA, USA, 2015.

[12] Bandyopadhyay, S, Bhattacharyya, 'Lightweight Internet protocols for web enablement of sensors using constrained gateway devices', International Conference on Networking and Communications (ICNC), vol., no., pp.334,340, 28-31 Jan. 2013.

[13] Colitti, Walter, Kris Steenhaut, and Niccolò De Caro. 'Integrating wireless sensor networks with the web', Extending the Internet to Low power and Lossy Networks (IP+ SN 2011)

[14] M. A. Hail and S. Fischer, 'Iot for aal: An architecture via informationcentric networking', in 2015 IEEE Globecom Workshops (GC Wkshps), Dec 2015, pp. 1–6.

[15] E. Gambi, L. Montanini, L. Raffaeli, S. Spinsante, and L. Lambrinos, 'Interoperability in iot infrastructures for enhanced living environments', in Proceedings of the 4th International BlackSea Conference on Communications and Networking. IEEE, 2016.

[16] Rongxing Lu, Xu Li, Xiaohui Liang, and Xuemin (Sherman) Shen, "GRS: The Green, Reliability, and Security of Emerging Machine to Machine Communications", IEEE Communications Magazine May 2011

[17] Jian Zhang, Lianhai Shan, Honglin Hu and Yang Yang, "Mobile cellular networks and wireless sensor networks: Toward convergence", IEEE Communications Magazine (Volume: 50, Issue: 3, March 2012)

[18] Min Chen , Jiafu Wan and Fang Li "Machine-to-Machine Communications: Architectures, Standards and Applications", KSII Transactions on Internet and Information Systems · January 2012

[19] Pascual J,Sanjua´n O,CuevaJM,PelayoBC,A´lvarez M and Gonza´ lez A., "Modeling architecture for collaborative virtual objects based on services", Journal of Network and Computer Applications 2011;34(5):1634–47.

[20] Dr. Ovidiu Vermesan and Dr. Peter Friess, "Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems", River Publishers, 2013 - 364 pages.

Networks Journal, Elsevier, Vol. 79C N. doi.org/10.1016/j.adhoc.2018.0, octobre 2018

[21] Hakiri Akram, Berthou Pascal, Gokhale Aniruddha, Abdellatif Slim, 'Publish/subscribe-enabled software defined networking for efficient and scalable IoT communications', IEEE Communications Magazine · September 2015, DOI: 10.1109/MCOM.2015.7263372

[22] D. Pianini and G. Salvaneschi, 'IoT Architectural Framework: Connection and Integration Framework for IoT Systems' First workshop on Architectures, Languages and Paradigms for IoT EPTCS 264, 2018, pp. 1–17, doi:10.4204/EPTCS.264.1

[23] Naveen, Soumyalatha ,' Study of IoT: Understanding IoT Architecture, Applications, Issues and Challenges', International Journal of Advanced Networking & Applications (IJANA), ISSN: 0975-0282

[24] I.F. Akyildiz and I.H. Kasimoglu, "Wireless sensor and actor networks : research challenges", Ad hoc networks 2 (2004)

[25] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", Communications Magazine, IEEE 40 (2002), no. 8, 102_114. 11, 13

[26] Christian Buckl, Stephan Sommer, Andreas Scholz, Alois Knoll, Alfons Kemper, Jörg Heuer, and Anton Schmitt, "Services to the _eld : An approach for resource constrained sensor/actor networks", Advanced Information Networking and Applications Workshops, 2009. WAINA'09. International Conference on, IEEE, 2009, pp. 476_481. 12, 16, 28, 44, 62, 66, 67, 83, 102

[27] C.Y. Chong and S.P. Kumar, "Sensor networks : Evolution, opportunities, and challenges", Proceedings of the IEEE 91 (2003), no. 8, 1247_1256. 11, 14

[28] Luca Mainetti, Luigi Patrono, and Antonio Vilei, "Evolution of wireless sensor networks towards the internet of things : A survey", Software, Telecommunications and Computer Networks (SoftCOM), 2011 19th International Conference on, IEEE, 2011, pp. 1_6. 12, 23, 37, 62, 100

[29] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey", Computer Networks 52 (2008), no. 12, 2292_2330. 11, 13, 14, 16, 37, 38, 59

[30] Yusuf Perwej, Kashiful Haq, Firoj Parwej," The Internet of Things (IoT) and its Application Domains", International Journal of Computer Applications (0975 – 8887) Volume 182 – No. 49, April 2019

[31] Revu Krishnamohan "Applications of IoT: A Study" Technical Report · April 2017 DOI: 10.13140/RG.2.2.27960.60169

[32] De, S., & et al, "Concepts and Solutions for Entity-based Discovery of IoT Resources and Managing their Dynamic Associations", IoT-A Deliverable D4.3, 2012.

[33] Perera, C., Zaslavsky, A., Christen, P., Compton, M., & Georgakopoulos, D., "Context-aware sensor search, selection and ranking model for internet of things middleware", Mobile Data Management (MDM), 2013 IEEE 14th International Conference on (pp. 314–322).Vol.1.

[34] Abangar, H., Barnaghi, P., Moessner, K., Tafazolli, R., Nnaemego, A., & Balaskandan, K., "A Service Oriented Middleware Architecture for Wireless Sensor Networks", Proceedings of Future Network and Mobile Summit 2010.

[35] Vincenzo Della Mea. What is e-health (2): The death of telemedicine? Journal of Medical Internet Research, 3(2):e22, 2001.

[36]G. Eysenbach. What is e-health? Journal of Medical Internet Research, 3(2):e20, 2001.

[37] Terrance J.Dishongh and Michael McGrath. Wireless sensor networks for health- care application. Artech House, 1 edition, 2009.

[38] M. Park, "IEEE 802.11ah: sub-1-GHz license-exempt operation for the internet of things," in IEEE Communications Magazine, vol.53, no.9, pp.145-151, September 2015

[39] J. Decuir, "Bluetooth 4.0: Low Energy", Presentation slides, 2010,

[40] C. Gomez, J. Oller, and J. Paradells, "Overview and evaluation of Bluetooth low energy: An emerging low-power wireless technology," Sensors, vol. 12, no. 9, pp. 11734-11753, 2012

[41] ZigBee Standards Organization, "ZigBee Specification," Document 053474r17, Jan 2008, 604 pp.,

[42] M. Hasan, E. Hossain, D. Niyato, "Random access for machine-to-machine communication in LTE-advanced networks: issues and approaches," in IEEE Communications Magazine, vol. 51, no. 6, pp. 86-93, June 2013,

[43] Sigfox, "Make things come alive in a secure way," tech. rep., Sigfox, 2 2017. Accessed: 2018-10-2.

[44] G. Ferré and E. P. Simon, "An introduction to Sigfox and LoRa PHY and MAC layers." working paper or preprint, Apr. 2018.

[45] LoRa Alliance, "LoRaWAN specification," 2015

[46] Guillaume Ferré, Eric Simon. An introduction to Sigfox and LoRa PHY and MAC layers. 2018. ffhal-01774080f

[47] Anthony JUTON, « Réseaux très basse consommation, longue portée, bas débit, l'exemple de LoRaWAN « , 3EI, numéro 96 avril 2019

[48] V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, "A survey on application layer protocols for the internet of things," Transaction on IoT and Cloud Computing, vol. 3, no. 1, pp. 11-17, 2015

[49] M. Singh, M. Rajan, V. Shivraj, and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)," in Fifth International Conference on Communication Systems and Network Technologies (CSNT 2015), April 2015, pp. 746-751

[50] OASIS, "OASIS Advanced Message Queuing Protocol (AMQP) Version 1.0," 2012

[51] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)," IETF RFC 7252, Jun. 2014

[52] P. Saint-Andre, "Extensible messaging and presence protocol (XMPP): Core," IETF RFC 6120, 2011

[53] Object Management Group, "Data Distribution Service V1.4," April 2015,

[54]Bandyopadhyay, S. and Bhattacharyya, A., "Lightweight Internet protocols for web enablement of sensors using constrained gateway devices", International Conference on Networking and Communications (ICNC), vol., no., pp.334,340, 28-31 Jan. 2013.

[55]Colitti, Walter, Kris Steenhaut, and Niccolò De Caro. "Integrating wireless sensor networks with the web", Sensor Networks Conference 2011.

[56] G. Wu, et. al. "M2M: From Mobile to Embedded Internet", IEEE Communications Magazine (Volume: 49, Issue: 4, April 2011).

[57] C. Kahn and H. Viswanathan, "Connectionless Access for Mobile Cellular Networks", IEEE Communications Magazine, Comm. Standards Supplement, pp. 26-31, Sept. 2015.

[58] Boswarthick, David, Omar Elloumi, and Olivier Hersent, "M2M communications: a systems approach", John Wiley & Sons, 14 mars 2012 - 280 pages.

[59] Ajinkya Rajandekar and Biplab Sikdar Fellow, "A Survey of MAC Layer Issues and Protocols for Machine-to-Machine Communications", IEEE Internet of Things Journal (Volume: 2, Issue: 2, April 2015).

[60] BISO/IEC 2382-1:1993 Information Technology – Vocabulary – Part 1: Fundamental terms. International Organization for Standardization (ISO). [Online]. Available: http://www.iso.org/ iso/

[61] Kiljander J, D'Elia A, Morandi F, Hyttinen P, Takalo-Mattila J, Ylisaukko-Oja A, Soininen JP, Cinotti TS (2014) Semantic interoperability architecture for pervasive computing and internet of
things. IEEE Access 2:856–873

[62] Pantsar-Syväniemi S, Purhonen A, Ovaska E, Kuusijärvi J, Evesti A (2012) Situation-based and self-adaptive applications for the smart environment. J. Ambient Intell. Smart Environ. 4(6):491–516

[63] Hahm O, Baccelli E, Petersen H, Tsiftes N (2016) Operating Systems for Low-End Devices in the Internet of Things: A Survey. IEEE Internet Things J. 3(5):720–734

[64] Bello O, Zeadally S, BadraM(2016) Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT). Ad Hoc Networks 0:1–11

[65]. W3C, BW3C Semantic Integration & Interoperability Using RDF and OWL.^ [Online]. Available: https://www.w3.org/2001/sw/BestPractices/OEP/SemInt/. [Accessed: 25-Jul-2017]

[66] Shiao M (2015) Internet of things standardisation and architectures - workshop report

[67] E. and others Levis, Philip and Madden, Sam and Polastre, Joseph and Szewczyk, Robert andWhitehouse, Kamin andWoo, Alec and Gay, David and Hill, Jason andWelsh,Matt and Brewer, BTinyOS: An operating system for sensor networks,^ Ambient Intell, vol 35, pp 115–148, 2005

[68] Thomas KW, Vilajosana X, Kerkez B, Chraim F, Weekly K, Wang Q,Glaser S, Pister (2012) OpenWSN: a standards-based low-power wireless development environment. Trans. Emerg. Telecommun. Technol. 23(5):480–493

[69] BPonte - M2MBridge Framework for REST developers.^ [Online].Available: http://www.eclipse.org/proposals/technology.ponte/. [Accessed: 24-Oct-2016]

[70] Zhu Q, Wang R, Chen Q, Liu Y, Qin W (2010) IOT gateway: bridgingwireless sensor networks into internet of things. 2010 IEEE/IFIP Int Conf Embed Ubiquitous Comput pp 347–352

[71] Fantacci R, Pecorella T, Viti R, Carlini C (2014) Short paper: overcoming IoT fragmentation through standard gateway architecture. 2014 IEEE World Forum Internet Things, WF-IoT 2014, pp 181–182

[72] Pereira C, Rocha P, Santiago F, Sousa J (2016) IoT interoperability for actuating applications through standardised M2M communications. In World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2016 IEEE 17th International Symposium on A, pp 1–6

[73] Aloi G, Caliciuri G, Fortino G, Gravina R, Pace P, Russo W, Savaglio C (2016) Enabling IoT interoperability through opportunistic smartphone-based mobile gateways. J Netw Comput Appl no July pp 1–11

[74] Hoebeke J, De Poorter E, Bouckaert S, Moerman I, Demeester P (2011) Managed ecosystems of networked objects. Wirel. Pers. Commun. 58(1):125–143 Mobile Netw Appl

[75] Ishaq I, Hoebeke J, Moerman I, Demeester P (2012) Internet of things virtual networks: bringing network virtualization to constrained devices. 2012 IEEE Int Conf Cyber Phys Soc Comput

[76] BuIP TCP/IP stack. [Online]. Available: http://users.ece.utexas.edu/~mcdermot/arch/projects_fall_09/Team_04/project/uip-1.0/doc/html/main.html

[77] Han G, Ma M (2007) Connecting sensor networks with IP using a configurable tiny TCP/IP protocol stack. In Information, Communications & Signal Processing, 2007 6th International Conference on, pp 1–5

[78] Dunkels A (2001) Design and Implementation of the lwIP TCP/IP Stack. Swedish Inst. Comput. Sci. 2:77

[79] Zuniga M, Krishnamachari B (2003) Integrating future large-scale wireless sensor networks with the internet. USC Comput Sci Tech Rep

[80] Thubert P (2012) Objective function zero for the routing protocol for low-power and lossy networks (RPL)

[81] Chasaki D, Mansour C (2015) Security challenges in the internet of things. Int. J. Space-Based Situated Comput. 5(3):141

[82] Kreutz D, Ramos F (2015) Software-Defined Networking: A Comprehensive Survey. Proc. IEEE 103(1):14–76

[83] Systems C, France SA, Thubert P, Palattella MR, Engel T (2015) 6TiSCH centralized scheduling: when SDN meet IoT. In Standards for Communications and Networking (CSCN), 2015 IEEE Conference on, pp 42–47

[84] Flauzac O, Alez CG (2015) SDN based architecture for IoT and improvement of the security

[85]. Prazeres M, C'assio, Serrano (2016) SOFT-IoT: self-organizing FOG of things. In Advanced Information Networking and Applications Workshops (WAINA), 2016 30th International Conference on, pp 803–808

[86] Ai Y, PengM, Zhang K (2017) Edge cloud computing technologies for internet of things: A primer. Digit Commun Networks

[87] Gyrard A, Serrano M, Patel P (2017) Building interoperable and cross-domain semantic web of things applications. Manag Web Things pp 305–324

[88] Erl T (2005) Service-oriented architecture (SOA): concepts, technology, and design. Prentice Hall

[89] Guinard D, Trifa V, Karnouskos S, Spiess P, Savio D (2010) Interacting with the SOA-based internet of things: Discovery, query, selection, and on-demand provisioning of web services. IEEE Trans. Serv. Comput. 3(3):223–235

[90] Vinoski S (2003) Integration with Web Services. IEEE Internet Comput. 7(6):75–77

[91] Vega-barbas M, Casado-mansiua D, Valero MA, Lpez-de-ipina D, Bravo J, Florez F (2012) Smart spaces and smart objects interoperability architecture (S3OiA) CPS. In

InnovativeMobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on, pp 725–730

[92] Scioscia F, RutaM(2009) Building a semantic web of things: issues and perspectives in information compression. ICSC 2009 – 2009 IEEE Int Conf Semant Comput pp 589–594

[93] Jara AF, Antonio J, Olivieri AC, Bocchi Y, Jung M, Kastner W, Skarmeta (2014) SemanticWeb of Things: an analysis of the application semantics for the IoT moving towards the IoT convergence. International Journal of Web and Grid Services 10:244–272

[94] Sheth SS, Amit, Henson, Cory, Sahoo (2008) Semantic sensor web. IEEE Internet Comput, vol 12(4)

[95] Terziyan D, Vagan, Kaykova, Olena, Zhovtobryukh (2010) UbiRoad: semantic middleware for context-aware smart road environments. In Internet and web applications and services (iciw), 2010 fifth international conference on, vol 35 pp 295–302

[96] Gyrard A, Serrano M (2016) Connected smart cities: interoperability with SEG 3.0 for the internet of things. In Advanced Information Networking and Applications Workshops (WAINA), 2016 30th International Conference on, no 2 pp 796–802

[97]. Bauer M, Martinbauerneclabeu E, Meissner S (2011) Service modelling for the internet of things. In Computer Science and Information Systems (FedCSIS), 2011 Federated Conference on, pp 949–955

[98] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function", IEEE J. Sel. Areas Commun., vol. 18, no. 3, pp. 535–547,2000.

[99] O. Tickoo and B. Sikdar, "Modeling queueing and channel access delay in unsaturated IEEE 802.11 random access MAC-based wireless networks", IEEE/ACM Trans. Netw., vol. 16, no. 4, pp. 878–891, 2008.

[100] F. De Rango, A. Perrotta, and S. Ombres, "An energy evaluation of ETDMA vs IEEE 802.11 in wireless ad hoc networks", Proc. Int. Symp. Perf. Eval. Comput. Telecommun. Syst. (SPECTS), pp. 273–279, 2010.

[101] A. Viterbi, "CDMA: Principles of Spread Spectrum Communications", Reading, MA, USA: Addison-Wesley, 1995.

[102] C. Zhu and M. S. Corson, "A five-phase reservation protocol (FPRP) for mobile ad hoc networks", Wireless Netw., vol. 7, no. 4, pp. 371–384,2001.

[103] L. Bao and J. Garcia-Luna-Aceves, "A new approach to channel access scheduling for ad hoc networks", Proc. ACM 7th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom), pp.210–221, 2001.

[104] I. Rhee, A. Warrier, M. Aia, J. Min, and M. L. Sichitiu, "Z-MAC: A hybrid MAC for wireless sensor networks", IEEE/ACM Trans. Netw., vol. 16, no. 3, pp. 511–524, 2008.

[105] R. Zhang, R. Ruby, J. Pan, L. Cai, and X. Shen, "A hybrid reservation/ contention-based MAC for video streaming over wireless networks", IEEE J. Sel. Areas Commun., vol. 28, no. 3, pp. 389–398, 2010.

[106] M. Salajegheh, H. Soroush, and A. Kalis, "HYMAC: Hybrid TDMA/FDMA medium access control protocol for wireless sensor networks", in Proc. 18th IEEE Int. Symp. Personal Indoor Mobile Radio Commun. (PIMRC), pp. 1–5, 2007.

[107] M. Hasan, et al., "Random Access for Machine-to-Machine Communication in LTE-Advanced Networks: Issues and Approaches", IEEE Communications Magazine (Volume: 51, Issue: 6, June 2013).

[108] M. Timmers, et al., "A Distributed Multichannel MAC Protocol for Multihop Cognitive Radio Networks", IEEE Transactions on Vehicular Technology (Volume: 59, Issue: 1, Jan. 2010).

[109] N. K. Pratas et. al.,"Code expanded random access for machine-type communications", 2012 IEEE Globecom Workshops.

[110] C. Y. Hsu, C. H. Yen, and C. T. Chou, "An adaptive multichannel protocol for large-scale machine-to-machine (M2M) networks," in Proc. 9th IEEE Int. Wireless Commun. Mobile Comput. Conf. (IWCMC), pp. 1223–1228, 2013.

[111] Y. Liu, C. Yuen, J. Chen, and X. Cao, "A scalable hybrid MAC protocol for massive M2M networks," in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), pp. 250–255, 2013.

[112] Y. Liu, C. Yuen, X. Cao, N. U. Hassan, and J. Chen, "Design of a scalable hybrid MAC protocol for heterogeneous M2M networks," IEEE Internet Things J., vol.1, no.1, pp. 99–111, 2014.

[113] Y. Liu, S.-L. Xie, R. Yu, Y. Zhang, and C. Yuen, "An efficient MAC protocol with selective grouping and cooperative sensing in cognitive radio networks," IEEE Trans. Veh. Technol., vol. 62, no. 8, pp. 3928–3941,Oct. 2013.

[114] R. Yu, C. Zhang, X. Zhang, L. Zhou, and K. Yang, "Hybrid spectrum access in cognitive radio based smart grid communications networks", IEEE Systems Journal (Volume: 8, Issue: 2, June 2014).

[115] R. Bruno, M. Conti, and E. Gregori, "Optimal capacity of p-persistent CSMA protocols", IEEECommun. Lett., vol. 7, no. 3, pp. 139–141,Mar. 2003.

[116] F. Azquez-Gallego, J. Alonso-Zarate, I. Balboteo, and L. Alonso, "DPCF-M: A medium access control protocol for dense machine-to machine area networks with dynamic

gateways", in Proc. IEEE 14th Workshop Signal Process. Adv. Wireless Commun.(SPAWC), pp. 490– 494, 2013.

[117] G. Wang, X. Zhong, S. Mei, and J. Wang, "An adaptive medium access control mechanism for cellular based machine-to-machine (M2M) communication", in Proc. IEEE Int. Conf. Wireless Inf. Technol. Syst. (ICWITS), pp. 1–4, 2010

[118] N. K. Pratas, H. Thomsen, C. Stefanovic, and P. Popovski, "Codeexpanded random access for machine-type communications", in Proc. IEEE Global Telecommun. Conf. Workshop (GLOBECOM), pp. 1681– 1686, 2012.

[119] C. W. Park, D. Hwang, and T. J. Lee, "Enhancement of IEEE 802.11ah MAC for M2M Communications", IEEE Commun. Lett. vol. 18, no. 7, pp. 1151–1154, Jul. 2014.

[120] H. Wu, C. Zhu, R. J. La, X. Liu, and Y. Zhang, "Fast adaptive S-ALOHA scheme for event-driven machine-to-machine communications", in Proc. IEEE Veh. Technol. Conf. (VTC Fall), pp. 1–5, 2012.

[121] Y. Chen and W. Wang, "Machine-to-machine communication in LTE-A", in Proc. IEEE Veh. Technol. Conf. (VTC Fall), pp. 1–4, 2010.

[122] A. Lo, Y. W. Law, M. Jacobsson, and M. Kucharzak, "Enhanced LTE-advanced random-access mechanism for massive machine-to-machine (M2M) communications", in Proc. WWRF, pp. 1–5, 2011.

[123] A. Aijaz and A. H. Aghvami, "A PRMA-based MAC protocol for cognitive machine-to-machine communications", in Proc. IEEE Int. Conf. Commun. (ICC), pp. 2753–2758, 2013.

[124] D. Tarchi, R. Fantacci, and D. Marabissi, "Proposal of a cognitive based MAC protocol for M2M environments", in Proc. 24th IEEE Int. Symp. Personal Indoor Mobile Radio Commun. (PIMRC), pp. 1609– 1613, 2013

[125] S. Boyd and L. Vandenberghe, "Convex Optimization", Cambridge, U.K.: Cambridge Univ. Press, 2004.

[126] Hajjar, S., & Spears, T. (2019). Hardware Microprogramming Education Using Raspberry PI and Arduino Technologies. International Journal of Intelligent Information Systems, 8(2), 47.

[127] Ramaiah, N. S. (2019). IoT Based Route Assistance for Visually Challenged. Elsevier, SSRN.

[128] Branig, M., & Engel, C. (2019, June). SmartCane: an active cane to support blind people through virtual mobility training. In Proceedings of the 12th ACM International Conference on PErvasive Technologies Related to Assistive Environments (pp. 327-328). ACM.

[129] Saha, P., Tuba, M. A., Ahmed, K. A., & Ashrafuzzaman, M. (2019, March). Development of an Inexpensive Proficient Smart Walking Stick for Visually Impaired Peoples. In International Conference on E-Business and Telecommunications (pp. 48-56). Springer, Cham.

[130] Petäjäjärvi, J., Mikhaylov, K., Yasmin, R., Hämäläinen, M., & Iinatti, J. (2017). Evaluation of LoRa LPWAN technology for indoor remote health and wellbeing monitoring. International Journal of Wireless Information Networks, 24(2), 153-165.

[131] Mdhaffar, A., Chaari, T., Larbi, K., Jmaiel, M., & Freisleben, B. (2017, July). IoT-based health monitoring via LoRaWAN. In IEEE EUROCON 17th International Conference on Smart Technologies (pp. 519-524). IEEE.

[132] Mighali, V., Patrono, L., Stefanizzi, M. L., Rodrigues, J. J., & Solic, P. (2017, July). A smart remote elderly monitoring system based on IoT technologies. In Ninth International Conference on Ubiquitous and Future Networks (ICUFN) (pp. 43-48). IEEE.

[133] Kharel, J., Reda, H. T., & Shin, S. Y. (2017). An architecture for smart health monitoring system based. Journal of Communications, 12(4).

[134] Hayati, N., & Suryanegara, M. (2017, October). The IoT LoRa system design for tracking and monitoring patient with mental disorder. IEEE International Conference on Communication, Networks and Satellite (Comnetsat) (pp. 135-139). IEEE.

[135] Gambi, E., Montanini, L., Pigini, D., Ciattaglia, G., & Spinsante, S. (2018). A home automation architecture based on LoRa technology and Message Queue Telemetry Transfer protocol. International Journal of Distributed Sensor Networks, 14(10), 1550147718806837.

[136] G. Eysenbach. What is e-health? Journal of Medical Internet Research, 3(2):e20,2001

[137] Elizabeth Bougeois, Nicolas Van den Bossche, Adrien and Cazenave, Laurence Redon, Adriana Soveja, Thierry Val, and Thierry Villemur. Le projet CANet : une activité pluridisciplinaire liant recherche et pédagogie (regular paper), 2012.

[138] A technical overview of LoRa® and LoRaWAN™ Technical Marketing Workgroup 1.0, November 2015

[139] Jetmir Haxhibeqiri I, Eli De Poorter , Ingrid Moerman and Jeroen Hoebeke, A Survey of LoRaWAN for IoT: From Technology to Application, Sensors 2018, 18, 3995; doi:10.3390/s18113995

[140] V. Gazis et al., "A survey of technologies for the internet of things," in International Wireless Communications and Mobile Computing Conference, August 2015, pp. 1090-1095.

[141] D. Thangavel, X. Ma, A. Valera, H. Tan, and C.K. Tan, "Performance evaluation of MQTT and CoAP via a common middleware," Intelligent Sensors, Sensor Networks and Information Processing, April 2014.

[142] V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso- Zarate, "A survey on application layer protocols for the internet of things," Transaction on IoT and Cloud Computing, vol 1., January 2015.

[143] Eclipse Mosquitto. (2016, Feb. 12). [Online]. Available: http://mosquitto.org

[144] International Business Machines Corporation (IBM), "MQTT V3.1 Protocol Specification," August 2010.

[145] A. Banks, R. Gupta, "MQTT Version 3.1.1," Octobar 2014.

[146] E.P. Frigieri, D. Mazzer, and L. Parreira, "M2M protocols for constrained environments in the context of IoT: A comparison of approaches" in International Telecommunications Symposium.

[147] 'Ultra-compact high-performance eCompass module: 3D accelerometer and 3D magnetometer', STMicroelectronics.

[148] 'Freescale Semiconductor, Data Sheet: Technical Data', Document Number: K20P64M72SF1 Rev. 3, 11/2012

[149] P. Badura, E. Pietka, and S. Franiel, "Acceleration trajectory analysis in remote gait monitoring," in Engineering in Medicine and Biology Society (EMBC), 2014 36th Annual International Conference of the IEEE, pp. 4615–4618August 2014.

[150] Matthew Loy, Raju Karingattil, Louis Williams, ISM-Band and Short Range Device Regulatory Compliance Overview, SWRA048–May 2005.

[151] Texas Instruments®, Application Report SWRA046A, "ISM-Band and Short Range Device Antennas", March 2005

[152] Spread Spectrum Scene, "Indoor Radio Propagation SSS Online and Pegasus Technologies" (http://www.sssmag. com/indoor.html), December 1998.

[153] 'Introducing the Raspberry Pi 2 - Model B', https://learn.adafruit.com/introducing-the-raspberry-pi-2-model-b, accessed 2 April 2017

[154] 'chistera-pi', https://snootlab.com/shields-snootlab/1152-chistera-pi-12-lora-accessoires-fr.html, accessed 3 April 2017

[155] 'Eclipse Mosquitto', http://mosquitto.org, Accessed 25 mars 2017.