REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE ABOU-BEKR BELKAID – TLEMCEN

THÈSE LMD

Présentée à :

FACULTE DES SCIENCES – DEPARTEMENT D'INFORMATIQUE

Pour l'obtention du diplôme de :

DOCTORAT

Spécialité: *Réseaux et Systèmes Distribués*

Par :

BOUZEBIBA Hadjer

Sur le thème

Adaptation des protocoles de communication conçus pour les IoT aux systèmes IoMT

Soutenue publiquement le 15 Octobre 2020 à Tlemcen devant le jury composé de :

Mr FEHAM Mohammed	Professeur	Université de Tlemcen	Président
M^{r} LEHSAINI Mohamed	Professeur	Université de Tlemcen	Directeur de thèse
Mr KHALFI Fethi	MCA	Université de Sidi Bel Abbes	Examinateur
Mr ALI CHERIF Moussa	MCA	Université de Sidi Bel Abbes	Examinateur
Mr BENMAMMAR Badr	Professeur	Université de Tlemcen	Examinateur

Laboratoire Systèmes et Technologies de l'Information et de la Communication (STIC)
BP 119, 13000 Tlemcen - Algérie

Remerciements

Tout d'abord, je remercie *Allah* Tout-Puissant de m'avoir donnée la force et les moyens de terminer mon doctorat, Hamdouli Allah. Ce voyage merveilleux et stimulant n'aurait pas été possible sans les conseils et le soutien de plusieurs personnes. Je voudrais exprimer ma sincère gratitude à toute personne qui a contribué à la réussite de ce travail de thèse. Je leur suis redevable de leur supervision incessante, de leurs précieuses suggestions, de leur soutien et de leur motivation pour bien mener à la réussite de cette thèse.

Tout d'abord, je voudrais exprimer ma gratitude à mes chers parents *Nacera* et *Mohammed*. Je leur suis éternellement reconnaissante pour leur amour, leur soutien, leurs prières, leurs encouragements, leurs sacrifices et leur aide tout au long de ma vie. C'est à eux que je dois tout le succès de ma vie. Je voudrais également exprimer mes sincères remerciements aux membres de ma famille pour leur soutien et leurs encouragements. Ceux-ci ont été le moteur de mes réalisations.

Je dois ma profonde gratitude à mon superviseur, *Mr Mohamed Lehsaini*, pour son soutien et ses conseils continus, qui m'ont orienté dans la bonne direction et ont fait de mon parcours doctoral une expérience intéressante et agréable. Je remercie tout particulièrement, *Mr Sidi Mohammed Senouci*, pour son soutien et ses précieux commentaires.

Je suis très honorée et reconnaissante envers *Mr Feham Mohammed* d'avoir accepté de présider le jury de cette thèse. Je tiens à remercier aussi les membres du jury *Mr Benmammar Badr*, *Mr Khalfi Fethi*, *Mr Ali Cherif Moussa* pour l'honneur qu'ils m'ont fait en acceptant de juger ce travail.

Je souhaite également remercier tous les membres du laboratoire *STIC* au sein duquel ce travail a été réalisé et mes collègues enseignants et doctorants à qui je souhaite l'épanouissement dans leur travail.

Enfin, mes sincères remerciements à tous ceux/celles qui ont contribué, directement ou indirectement, à la réalisation de ce travail.

Merci pour tous vos encouragements !

Dédicaces

À mes parents,
À ma soeur et à mon frère,
À la mémoire de ma grande mère.
À tous ceux que j'aime
Je dédie ce travail.

Table des matières

Liste des figures

Liste des tableaux

Glossaire

6LoWPAN IPv6 over Low power WPAN. 15

ACO Ant Colony Optimization. 45

ADRR Airtime Deficit Round Robin. 102

AID Active IoT Device. 41

AOMDV-IoT An Improved AOMDV Routing Protocol for Internet of Things. 33

AQA-AODV Adaptive QoS-Aware Ad-hoc On-demand Distance Vector. 82

AQM Active Queue Management. 98

ARSSI Average Received Signal Strength Indicator. 69

BLE Bluetooth Low Energy. 7

BMRF Bidirectional Multicast RPL Forwarding protocol. 71

BRPL Backpressure RPL. 69

BRR Budget-based Round Robin. 102

BVD Big Volume of Data. 79, 97

BW Bandwidth. 80

C-RPL Coopérative-RPL. 71

CAOF Context aware Objective Function. 64

CASCR Context Awareness in Sea Computing. 38

CCA Clear Channel Assessment. 16

CECA Context-aware Energy Conserving Algorithm for routing. 38

CH Cluster Head. 35

CLRPL Context Aware and Load Balancing RPL. 64

CMOS Complementary Metal Oxide Semiconductor. 22

CMPR Clustering based Multi-Path Routing algorithm for improving the reliability in WSNs. 82

CoAP Constrained Application Protocol. 2, 13

CrowWhale-ETR Crow Whale-energy trust routing. 48

DAG Directed Acyclic Graph. 50

DAO Destination Advertisement Object. 53

DAO-ACK Destination Advertisement Object ACKnowledgement. 54

DDRR Distributed Deficit Round Robin. 101

DIM Delay Iterative Method. 39

DIO DODAG Information Object. 53

DIS DODAG Information Solicitation. 52

DODAG Destination Oriented DAG. 50, 81

DoS Déni de Service. 72

DSR Dynamic Source Routing Protocol. 34

DT-RPL Diverse Traffic-RPL. 64

DTLS Datagram Transport Layer Security. 14

DWRR Deficit Weighted Round Robin. 98

E-CARP Enhanced version of the Channel-Aware Routing Protocol (CARP). 42

EARA Energy aware Ant Routing Algorithm. 46

ECOR An Energy Aware Coded Opportunistic Routing. 42

EDWRR Equilibrated Deficit Weighted Round Robin. iii, 4, 5, 99, 100, 110, 111, 113, 115

EELSR Energy Efficient Link Stable Routing. 42

EEPR Energy Efficient Probabilistic Routing algorithm. 42

EHARA Effective energy Harvesting Aware Routing Algorithm. 44

EICAntS Efficient IoT Communications based on Ant System. 46

EKR-MRPL Extended Kalman Filter for Mobile RPL. 70

ERGID Emergency Response IoT based on Global Information Decision. 38

ERR Elastic Round Robin. 101

ESMRF Enhanced SMRF. 71

ETSP Cluster HeadEfficient Tree-based Self-organizing Protocol. 35

ETX Expected Transmission Count. 3, 43

EXP/PF Exponential/Proportional Fair. 103

FLS Frame Level Scheduler. 103

FQ Fair-Queuing. 98

FreeBW-RPL BandWidth RPL. 3

FSELC Fully Simplified Exponential Lifetime Cost. 66

GeoRank geometric based behavior of GOAFR. 36

GT-ACR Game Theoretic Approach for Context Based Routing. 38

GTM-RPL Game-Theory based Mobile RPL. 69

GTS Guaranteed Time Slot. 16

H2M Homme-Machine. 10

HCDSR A Hierarchical Clustered based on modified Dynamic Source Routing. 36

ICT Internet Connexion Table. 33

IEEE Institute of Electrical and Electronics Engineers. 2

IEIFTA Improved Efficient and Intelligent Fault-Tolerance Algorithm. 46

IETF Internet Engineering Task Force. 2, 13

IFS Inter Frame Space. 101

ILA Internet Linking Address. 33

IoMT Internet of Multimedia Things. 2, 22

IoT Internet of Things. 1

IPSO Improved Particle Swarm Optimization Algorithm. 46

KP-RPL Kalman positioning RPL. 69

L2AM Lifetime and Latency Aggregatable Metric. 66

LASeR Lightweight authentication and secured routing for NDN IoT in smart cities. 48

LBR LLN Border Router. 51

LDDWRR Least Delay Dynamic Weighted Round Robin. 102

LDGM-IoT Lightweight and Distributed Geographic Multicast Routing Protocol for IoT Applications. 37

LGRR Loan-Grant based Round Robin. 102

LLN Low power and Lossy Network. 1

LOADng Multipath-Enhanced Lightweight On-demand Ad hoc Distance-vector Routing Protocol –Next Generation. 34

LQGR Link Quality based Geographic Routing resilient to location errors. 36

LQI Level Quality Indicator. 16, 59

M-LWDF Modified Largest Weighted Delay First. 103

M2M Machine-to-Machine. 10

MAC Medium Access Control. 16, 98

MARPL Mobility Aware RPL. 70

MCTAR Multi-context trust aware routing. 48

MDWRR Modified Dynamic WRR. 101

MEMS Micro-Electro-Mechanical Systems. 22

MERPL Memory Efficient storing mode in RPL. 65

MLDDRR Multi Level Dynamic Deficit Round Robin. 101

MoP Mode of Operation. 53

MP2P Multipoint-à-Point. 57

MPAR centralized MultiPAth QoS-driven Routing protocol. 44

MQS Maximum Queue Size. 103

MRHOF Minimum Rank with Hysteresis Objective Function. 3, 56

MTU Maximum Transmission Unit. 17

NB-IoT Narrowband Internet of Things. 103

NE Nash Equilibrium. 69

NLEE Node Level Energy Efficiency protocol. 42

NNDWRR Dynamic Weighted Round Robin. 102

NRT non-real time. 111

NSA Node State and Attribute. 58

OCP Objectif Code Point. 55

OF-FL Objective Function Fuzzy Logic. 66

OF0 Objective Function Zero. 55

Opt-RPL Optimized RPL. 66, 81

OSEAP Optimal Secured Energy Aware Protocol. 42

P2MP Point-à-Multipoint. 57

P2P point à point. 57

PAIR Pruned Adaptive IoT Routing. 38

PAOF Parent Aware Objective Function. 67

PC-RPL Power Controlled RPL. 83

PDR Packet Delivery Ratio. 81, 87

PI Packet generation Interval. 118

PLAWRR Prioritized Load Aware Weighted Round Robin. 102

PMIPv6 Proxy mobile IPv6. 50

PMSO bio-inspired Particle MultiSwarm Optimization. 46

QAODV-AC QoS-aware AODV routing-based Admission Control. 82

QCI QdS Class Identifier. 104

QI Queue Insolvency. 102

QoS qualité de service. 2

RCSFs Réseaux de Capteurs Sans Fil. 6

RDC Radio Duty Cycle. 18

REOR Reliable and Energy-Efficient Opportunistic Routing protocol. 42

REPC Residual Energy Probability Choice. 40

RERR Route ERRor packet. 33

RFID Radio Frequency Identification. 1, 6

ROLL Routing Over Low power and Lossy networks. 15

RPL Routing Protocol for Low power and lossy networks. 2, 15, 44

RR Round Robin. 101

RREP Route REply packet. 33

RREQ Route REQuest packet. 33

RSSI Received Signal Strength Indicator. 59

RT real time. 111

SAVEERS Secure Anti-Void Energy-Efficient Routing. 48

SCAOF A Scalable Context-Aware Objective Function. 67

SCOTRES Self-Channel Observation Trust and REputation System. 48

SEE-M2M Scalable Energy Efficient-M2M. 42

SEEOF Smart Energy Efficient Objective Function. 62

SERO-SH-IoT Secure and Efficient Protocol for Route Optimization in PMIPv6 based Smart Home IoT. 48

SHR Secure Hybrid Routing. 48

SMRF Stateless Multicast RPL Forwarding protocol. 71

SMRP Secure Multi-Hop Routing Protocol. 48

SpEED-IoT Spectrum aware Energy Efficient multi-hop multi-channel routing scheme for D2D communication in IoT. 38

SPLIT Secure and scalable RPL routing protocol. 73

SSRA Smart and Self-organised Routing Algorithm. 38

TSRF a Trust-Aware Secure Routing Framework. 48

UAV Unmanned Aerial Vehicle. 22

UDGM Unit Disk Graph Model. 86

UDP User Datagram Protocol. 13

UHD Ultra High Definition. 103

VT-M-LWDF Virtual Token Modified Largest Weighted Delay First. 103

WFQ Weighted Fair Queuing. 98

WG 6LoWPAN Working Group. 15

WRR Weighted Round Robin. 98

WSNs Wireless Sensor Networks. 6

Résumé

Ce travail entre dans le domaine d'internet des objets (IoT), et plus spécifiquement dans l'internet des objets multimédias (IoMT). En comparaison avec l'IoT, les réseaux IoMT exigent un certain niveau de qualité de service (QoS) plus élevé en termes de bande passante, de gigue, de fiabilité, de délai, etc. En effet, nous proposons d'aborder les problèmes d'incapacité des protocoles de communication d'IoT pour satisfaire les contraintes de QoS des applications l'IoMT. A cet effet, en commençant dans une première partie par une optimisation du protocole de routage RPL, qui est l'un des principaux éléments constitutifs des LLNs dans l'IoT, pour l'adapter aux communications multimédias. Dans ce contexte, nous avons proposé dans cette thèse une amélioration de ce protocole appelée *FreeBandWidth RPL* permettant un meilleur transfert de données multimédias dans les réseaux IoMT. Ce protocole est basé sur le calcul de la bande passante tout au long du chemin de routage et sur une fonction d'objectif adaptative pour avoir un meilleur équilibrage de charge entre les différents chemins de routage, particulièrement, lors d'une surcharge de données multimédias. Dans la deuxième partie, nous avons proposé une nouvelle extension équilibrée de l'algorithme d'ordonnancement DWRR, nommée *Equilibrated Deficit Weighted Round Robin (EDWRR)*. EDWRR garantit un taux de perte de paquets réduit dans chaque file d'attente et cela est due essentiellement à la procédure d'interruption de la mise en file d'attente de manière à avoir un taux de perte de paquets équilibré. L'implémentation des deux solutions proposées dans un émulateur a prouvé qu'elles sont plus performantes en comparaison avec les protocoles et les algorithmes d'ordonnancement concurrents.

Mots clés : IoT, IoMT, RPL, LLNs, QoS, Routage, Ordonnancement, DWRR.

Abstract

This work is part of the Internet of Things (IoT), and more specifically in the Internet of Multimedia Objects (IoMT). Compared to IoT, IoMT networks require a higher level of Quality of Service (QoS) in terms of bandwidth, jitter, reliability, data loss, delay, etc. Indeed, we propose to address the incapacity problems of IoT communication protocols to satisfy the QoS constraints of IoMT applications. To this end, starting in the first part with an optimization of the RPL routing protocol, which is one of the main components of LLNs in IoT, to adapt it to multimedia communications. Consequently, we have proposed in this thesis an improvement of this protocol called *FreeBandWidth RPL* allowing a better transfer of multimedia data in IoMT networks. It is based on the calculation of the bandwidth along the routing path and on an adaptive objective function to have a better load balancing between the different routing paths, in particular, during a multimedia data overload. In the second part, we proposed a new balanced extension of the DWRR scheduling algorithm, called *Equilibrated Deficit Weighted Round Robin (EDWRR)*. EDWRR guarantees a reduced packet loss rate in each queue and this is mainly due to the process of interrupting the queuing so as to have a balanced packet loss rate. The implementation of the two solutions proposed in an emulator has proven that they are more efficient in comparison with competing scheduling protocols and algorithms.

Keywords: IoT, IoMT, RPL, LLNs, QoS, routing, scheduling, DWRR.

ملخص

يعد هذا العمل جزءًا من إنترنت الأشياء، وبشكل أكثر تحديدًا في إنترنت الأشياء ذات الوسائط المتعددة. بالمقارنة مع إنترنت الأشياء ، تتطلب شبكات مستوى أعلى من جودة الخدمة من حيث النطاق الترددي والتذبذب والموثوقية وفقدان البيانات والتأخير وما إلى ذلك. في الواقع ، نقترح معالجة مشاكل عدم القدرة على بروتوكولات الاتصال بإنترنت الأشياء لتلبية متطلبات جودة الخدمة للتطبيقات. تحقيقا لهذه الغاية ، بدءا من الجزء الأول مع تحسين بروتوكول توجيه، الذي يعد أحد المكونات الرئيسية لـ LLNs في إنترنت الأشياء ، لتكييفه مع اتصالات الوسائط المتعددة. وبالتالي ، اقترحنا في هذه الأطروحة تحسين هذا البروتوكول المسمى مما يسمح بنقل أفضل لبيانات الوسائط المتعددة في الشبكات. وهو يعتمد على حساب عرض النطاق الترددي على طول مسار التوجيه وعلى وظيفة الهدف التكيفي للحصول على موازنة تحميل أفضل بين مسارات التوجيه المختلفة ، على وجه الخصوص ، أثناء التحميل الزائد لبيانات الوسائط المتعددة. في الجزء الثاني ، اقترحنا امتدادًا جديدًا متوازنًا لخوارزمية جدولة، تسمى عجز الموازنة المرجحة. يضمن انخفاض معدل فقدان الحزمة في كل قائمة انتظار وهذا يرجع بشكل رئيسي إلى عملية مقاطعة قائمة الانتظار للحصول على معدل فقدان حزم متوازن. أثبت تطبيق الحلين المقترحين في المحاكي أنهما أكثر كفاءة مقارنة ببروتوكولات وخوارزميات الجدولة المتنافسة.

الكلمات المفتاحية :IoT، IoMT، QoS، LLN، RPL، DWRR، التوجيه ، الجدولة.

Introduction Générale

Introduction Générale

Contexte de recherche

L'internet des objets, appelé ***en anglais*** *Internet of Things (IoT)*, est envisagé comme un grand défi pour la communauté des chercheurs sur Internet. La vision de l'IoT est de créer un environnement intelligent en utilisant des objets/dispositifs intelligents qui ont des capacités sensorielles et de communication pour générer de manière autonome des données. Ensuite, ces dernières seront transmises via Internet pour une certaine prise de décision. L'IoT comprendra des milliards de dispositifs communicants qui repoussent les frontières du cyber-monde avec des entités physiques, ainsi qu'avec des composants virtuels [8, 30].

Ces objets qui sont dotés d'un ensemble de capteurs sans fil ou d'étiquettes d'identification par radiofréquence (Radio Frequency Identification (RFID)), sont connectés à Internet avec la possibilité de détecter l'état de l'objet et d'utiliser des données en temps réel. En outre, ils accèdent à des données historiques et à des algorithmes développés en provoquant un déclenchement éventuel de ces dispositifs. Ces actions conduisent à des environnements intelligents très puissants, notamment des bâtiments intelligents, soins de santé, villes intelligentes ... etc.

Les exemples d'application dans le domaine IoT sont très nombreux. Nous citons les plus fameux par exemple, les systèmes de surveillance de la santé qui peuvent vérifier l'état du corps d'un patient, le comparer avec les enregistrements dans des bases de données ainsi qu'informer le médecin si nécessaire. Un autre exemple d'un réfrigérateur intelligent qui pourra commander automatiquement de la nourriture pour toute la famille. Ainsi, l'IoT peut également devenir un élément central des systèmes de véhicules intelligents capables d'échanger facilement des informations pour nous rendre en sécurité jusqu'à notre destination.

La prospérité de l'IoT est essentiellement due aux efforts de normalisation pour les nouveaux protocoles, qui ont permis aux réseaux à faible puissance et à pertes (Low power and Lossy Network (LLN)) d'offrir une infrastructure durable pour de nombreuses applications IoT. La communication entre les dispositifs dans un environnement IoT implique des capteurs miniaturisés et des dispositifs portables. En outre, ces dispositifs sont caractérisés par une petite unité de traitement, alimentés par une batterie et quelques kilo-octets de mémoire pour les rendre compacts et portables. En raison de leur caractéristique miniature (contraintes matérielles), ces dispositifs n'ont pas la capacité de fonctionner avec des protocoles lourds conçus pour les dispositifs hérités d'Internet en posant de nombreux défis en termes de mémoire, de puissance de traitement et d'autonomie d'énergie. Par consequent, les protocoles de communication d'IoT conçus à ces fins (routage, allocation des ressources, sécurité et interopérabilité) doivent être légers et en même temps attei-

gnant une efficacité, une évolutivité et une fiabilité des protocoles hérités d'internet et utilisés dans le même but.

À cet effet, la communauté des chercheurs dans ce domaine s'efforce de déployer de nombreux efforts précieux pour répondre aux besoins et aux défis de ce nouveau paradigme (i.e., IoT) [12, 31, 32] en termes de traitement restreint, de mémoire limitée, ainsi d'une capacité énergétique limitée. Par ailleurs, en raison d'une carence de protocoles satisfaisants ces contraintes, un besoin persistant de nouveaux protocoles est apparu en phase avec l'émergence des applications IoT. D'où les organismes de normalisation, Internet Engineering Task Force (IETF) et Institute of Electrical and Electronics Engineers (IEEE), ont anticipé cette nécessité en concevant une pile protocolaire standardisée et dédiée à l'IoT. Ainsi, jusqu'à présent, leurs efforts ont porté leurs fruits sur différents protocoles à travers toutes les couches de la pile protocolaire dédiée au paradigme IoT, tels que le protocole IEEE 802.15.4 dans la couche physique et MAC, le protocole de routage basé sur IPv6 à faible puissance et avec perte (Routing Protocol for Low power and lossy networks (RPL)) dans la couche réseau et le protocole d'application (Constrained Application Protocol (CoAP)).

Motivation de recherche

Bien que le routage est un élément clé dans l'infrastructure IoT et que de nombreux autres paramètres des systèmes IoT tels que la fiabilité et le passage à l'échelle dépendent fortement de cette technologie. À cet effet de nombreux recherches ont investi davantage sur les améliorations des protocoles de routage existants afin de répondre aux exigences des réseaux IoT.

La plupart des recherches actuelles sont limitées aux applications IoT qui sont basées sur les données scalaires des différents dispositifs. Cependant, les activités de recherche et de développement d'aujourd'hui reposent sur des services et des applications multimédias. Du point de vue de la communication, la prise en charge du contenu multimédia dans un tel réseau, comme l'IoT, est très exigeante. De plus, avec l'émergence du nouveau paradigme appelé Internet des objets multimédias (Internet of Multimedia Things (IoMT)), les protocoles dédiés aux applications IoT ont manifesté leur insuffisance dans les environnements multimédias.

Dans ce paradigme IoMT, différents objets multimédias permettent de récupérer et de communiquer un contenu de données multimédia qui leur permettent d'interagir et de coopérer entre eux sur Internet. Par conséquent, de nombreux types de trafic peuvent circuler dans le réseau avec des caractéristiques de qualité de service (QoS) différentes. De plus, les applications multimédias traitant des flux audio/vidéo ont des exigences spécifiques qui sont difficiles à satisfaire. Dans ce cas, le réseau doit être capable de supporter la transmission de grandes rafales de données à un débit élevé. Ces caractéristiques doivent être traitées efficacement tenant compte du matériel exigeant ainsi qu'aux limitations en termes de stockage mémoire, de bande passante, de latence...etc.

Objectifs de recherche et Contributions

Concevoir un protocole de routage efficace pour les applications IoMT, qui répond aux différents exigences des applications multimédias représente un défi majeur. Il existe de nombreuses solutions de routage proposées dans les IoT, notamment le protocole de routage IPv6 pour les réseaux LLNs (RPL pour les LLN) normalisé par le groupe de travail IETF ROLL, et qui est dédié aux dispositifs à ressources limitées comme dans le cas des IoT. Le protocole RPL est censé être l'un des principaux éléments constitutifs des LLN dans la tendance IoT. Cependant, ce protocole a encore besoin d'améliorations supplémentaires, en termes d'équilibrage de charge, de consommation d'énergie...etc. En outre, les paramètres de QoS du réseau IoT sont considérés à partir de différentes vues et dimensions telles que la bande passante, le délai, le taux de perte de paquets et la gigue [33].

En outre, le protocole RPL se caractérise par sa flexibilité permettant d'utiliser une ou plusieurs métriques de routage, ainsi que la manière dont ces métriques peuvent être combinées. Dans la fonction d'objectif "Minimum Rank with Hysteresis Objective Function (MRHOF)", deux métriques peuvent être utilisées soit la métrique "Expected Transmission Count (ETX)" ou la métrique énergie selon la définition de la norme RPL. Chacune de ces métriques possède ses avantages et ses inconvénients, par exemple la métrique ETX consomme beaucoup d'énergie, quand à la métrique d'énergie, elle ne garantit pas la fiabilité de la livraison des paquets entre les noeuds.

L'objectif principal de cette thèse est de développer des protocoles de communication d'IoT adaptés et efficaces dans le paradigme d'IoMT. En conséquence, la présente thèse propose de nouvelles approches qui se subdivisent en deux parties. Dans la première partie, nous avons suggéré une amélioration qui permet de combler les lacunes du protocole RPL déployé dans le réseau IoT ainsi dans l'IoMT. Ainsi, dans la deuxième partie, nous avons descendu vers la couche MAC de la pile protocolaire d'IoT en se focalisant sur les algorithmes d'ordonnancement et leurs rôles principaux lors d'une communication multimédia.

Partie I

Les données multimédias avec QoS ressortent un comportement antagoniste par rapport aux données scalaires dans l'IoT. Ainsi, un protocole de routage traitant un type de données non gourmand, notamment le protocole RPL, devra faire face à de nombreuses difficultés pour acheminer ce type de données. Pour cette raison, nous proposons une version améliorée du protocole RPL pour l'IoMT appelée "BandWidth RPL (FreeBW-RPL)" dans laquelle les données détectées sont essentiellement fournies par des dispositifs multimédias. Le protocole FreeBW-RPL définit une nouvelle fonction d'objectif appelée FreeBW qui effectue le calcul de la bande passante (BD) libre au niveau de la couche réseau. Nous définissons le défi de routage avec QoS comme la quantité de bande passante libre maximale tout au long du chemin de routage afin de mesurer la FreeBW maximale en fournissant les meilleures performances des applications multimédias. Les résultats de simulation ont prouvé que le protocole proposé surpasse les protocoles conventionnels en termes de délai de bout-en-bout, de débit, de taux de paquets délivrés et de consommation d'énergie.

Partie II

Les services multimédias fournis par les applications IoMT sont très exigeants en termes de QoS telles que la bande passante, le délai et le taux de perte de paquets. Il est important de mentionner que si l'une de ces conditions n'est pas satisfaite, les performances des ressources réseau, telles que la mémoire par exemple, seront affectées d'une manière négative. Dans cette optique, lorsqu'il s'agit des données volumineuses, tels que les flux multimédias, le défaut majeur se produit lorsque l'algorithme d'ordonnancement ne gère pas d'une manière efficace les files d'attente selon les exigences de QoS du système multimédia. Ainsi, le taux élevé de perte de paquets peut engendrer des taux de rejet différents en raison de l'iniquité d'allocation des files d'attente.

Nous avons suggéré l'utilisation d'un schéma multi-priorité et multi-file dans lequel l'influence du type de données dans un flux multimédia est considérée. Dans ce schéma, nous avons visé à développer une nouvelle extension équilibrée de l'algorithme d'ordonnancement DWRR, nommée "EDWRR". L'algorithme proposé réduit le taux de perte de paquets dans les files d'attente en interrompant la procédure de mise en file d'attente de manière à obtenir une quantité équilibrée d'espace libre et un taux de perte de paquets équilibré entre les différentes files d'attente. De plus, EDWRR peut distinguer différents services d'applications IoMT en attribuant une classification spécifique à chaque flux de données. Tout en s'adressant au problème des files d'attente surchargées, EDWRR atteint un taux de perte de paquets inférieur avec de meilleures performances que les algorithmes d'ordonnancement FIFO et DWRR en termes de PDR, de délai de bout en bout et de débit.

Organisation de la thèse

Cette thèse est organisée en quatre chapitres :

- Dans le premier chapitre nous introduisons les précurseurs de l'internet des objets notamment les réseaux de capteurs, les RFID et les réseaux LLNs. Ensuite, nous présentons une vue d'ensemble de l'architecture de la pile protocolaire d'IoT en définissant également le paradigme IoMT et ces domaines d'application. Enfin, nous clôturons ce chapitre par des interrogations sur les problèmes d'incapacité des protocoles de communication d'IoT à faire face à de lourdes contraintes causées par les différents QoS du paradigme IoMT.

- Dans le deuxième chapitre, nous passons en revue les protocoles de routage proposés dans l'IoT. Cette étude nous a permis de tirer profit de leurs atouts et de proposer de nouvelles solutions de routage pour ce type de réseaux. Ainsi, nous définissons en détail le protocole de routage RPL avec toutes ces fonctionnalités et nous clôturons ce chapitre par une taxonomie des revues de la littérature des améliorations du protocole RPL.

- Le troisième chapitre présente notre première contribution qui est la proposition d'une nouvelle fonction d'objectif basée sur la quantité de la bande passante libre dans la couche réseau, sous une version améliorée du protocole RPL appelée FreeBW-RPL. De plus, nous avons étudié les performances de la transmission d'un flux multimédia dans les réseaux IoMT en utilisant notre protocole amélioré.

- Le quatrième chapitre expose une nouvelle solution au problème de la probabilité croissante de perte de données multimédia sous une extension de l'algorithme d'ordonnancement DWRR nommée "EDWRR". Fondamentalement, l'algorithme d'ordonnancement EDWRR est obtenu en introduisant un mécanisme d'équilibrage dans l'algorithme d'ordonnancement DWRR avec un taux de perte de paquets équilibré entre les différentes files d'attente dédiées aux différents types de données, à savoir, les données scalaires et multimédias.

Finalement, nous concluons ce manuscrit en rappelant les principales contributions tout au long de ce travail de thèse. Ainsi, nous ouvrons quelques futures orientations de travail potentielles.

Chapitre 1

IoT & IoMT : Généralités et Concepts

Chapitre 1

IoT & IoMT : Généralités et Concepts

1.1 Introduction

L'IoT et l'IoMT ont récemment connu une période de croissance rapide dans le monde des nouvelles technologies et des applications à la mode fournissant de nombreux services multimédias.

Dans ce chapitre, nous discutons les différents concepts essentiels pour faciliter la compréhension des problèmes de recherche dans l'IoT et l'IoMT. Tout d'abord, nous présentons une vision de l'internet des objets et à travers toutes les couches de la pile protocolaire d'IoT, nous étudions les différents protocoles de normalisation conçus pour les réseaux LLN. En outre, une définition de l'IoT en tant que terme avec ses applications potentielles est également présentée avec une plus grande attention accordée aux tendances à venir de ces applications et à leurs influences. Ensuite, nous fournissons une définition détaillée du système IoT ainsi ses installations de communication. Puis, nous entamons le domaine des IoMT en tant que nouvelle technologie, ainsi que ses applications potentielles en mettant l'accent sur la non adaptation de quelques protocoles de communication d'IoT pour l'IoMT.

1.2 Vue historique sur les précurseurs de l'Internet des Objets

Les concepts prometteurs de l'IoT reposent sur deux décennies de progrès technologiques et de travaux dans divers domaines. Dans ce chapitre, nous revenons sur les précurseurs de l'IoT : les Réseaux de Capteurs Sans Fil (RCSFs) et les réseaux d'objets RFID.

1.2.1 Réseaux de capteurs sans fil

Les réseaux de capteurs sans fil (***en anglais*** Wireless Sensor Networks (WSNs)) représentent une part très importante de l'IoT. Un RCSF [34] est un réseau de noeuds de capteurs communiquant via un canal sans fil en fournissant des données précieuses sur un

environnement cible ainsi qu'ils peuvent interagir avec leur environnement via des actionneurs. Les capteurs sont caractérisés par leur petite taille ainsi que leur faible coût, qui leur facilitent d'être intégrés dans l'environnement en offrant un moyen non intrusif qui nous facilite la vie. Typiquement, les noeuds capteurs (aussi appelés motes) sont des systèmes embarqués dotés de ressources limitées notamment : communications à faible consommation d'énergie, à faible portée, à faible bande passante, petite mémoire ainsi qu'une petite batterie ou un dispositif de récupération d'énergie. En outre, les puces radios des noeuds capteurs telles que 802.15.4 ou Bluetooth Low Energy (BLE) sont limitées en termes de la puissance émise et de portée de transmission comparées à la technologie populaire WiFi 802.11. Ces caractéristiques ont fait l'objet de ces dispositifs d'être déployés en masse (sur une grande surface) avec un minimum d'intervention humaine.

Au sein d'une seule plateforme de base d'un noeud de capteurs, il peut exister de nombreux types de capteurs (température, lumière, humidité, caméras, accéléromètres...etc.) ou actionneurs (climatisation, commande de porte, alarmes...etc.) comme illustre la Figure 1.1. Un exemple classique d'un réseau de capteurs est la surveillance d'un environnement, où les noeuds de capteurs sont répartis sur la zone d'intérêt en y mesurant certaines propriétés comme la température.

Les RCSFs sont utilisés dans divers scénarios d'applications [35], par exemple dans le domaine médical [36], les maisons et les villes intelligentes, la surveillance environnementale, les systèmes de transport intelligents, la surveillance des installations militaires et industrielles...etc [37,38]. L'évolution des réseaux de capteurs leur a permis de s'éloigner des normes propriétaires notamment une connectivité native entre RCSF et Internet [39]. Cependant, l'intégration des RCSFs dans l'IoT fait une tendance actuelle, cela due à son rôle crucial dans l'IoT. Afin de mieux suivre l'état des objets, par exemple leur emplacement, leur température, leurs mouvements...etc., les RCSFs peuvent ainsi coopérer avec les systèmes *RFID*.

1.2.2 Radio Frequency Identification (RFID)

La première inspiration de l'internet des objets a été par des membres de la communauté de développement *RFID*, qui ont mentionné qu'un objet étiqueté peut fournir des informations comme il peut être parcouru par son adresse Internet ou une entrée de base de données correspondant à une *RFID* particulière [40]. Depuis cela, les recherches ont évolué en plusieurs activités sur la liaison de dizaines de milliers de réseaux de capteurs en utilisant la convergence de technologie, comme la technologie *RFID*, afin de suivre à tout moment chaque élément physique sur un tel environnement.

RFID est un terme générique qui décrit un ensemble d'objets ou de personnes diffusant son identité (sous la forme d'un numéro de série unique) à l'aide d'ondes radio. Il est classé dans la grande catégorie des technologies d'identification automatique.

Les objets étiquetés dans un réseau d'objets *RFID* sont dépendants d'autres objets afin d'être détectés et connectés au réseau global. Une étiquette *RFID* consiste en une micro-puce attachée à une antenne radio. La taille des données qui peuvent être stockées sur cette puce *RFID* vaut jusqu'à 2 kilo-octets. Par exemple, des informations sur un produit ou un envoi (date de fabrication, destination et date de péremption).

La technologie *RFID* a une importance capitale dans l'Internet des Objets. Au niveau logiciel, la technologie *RFID* et les RCSFs nécessitent une collaboration étroite pour l'in-

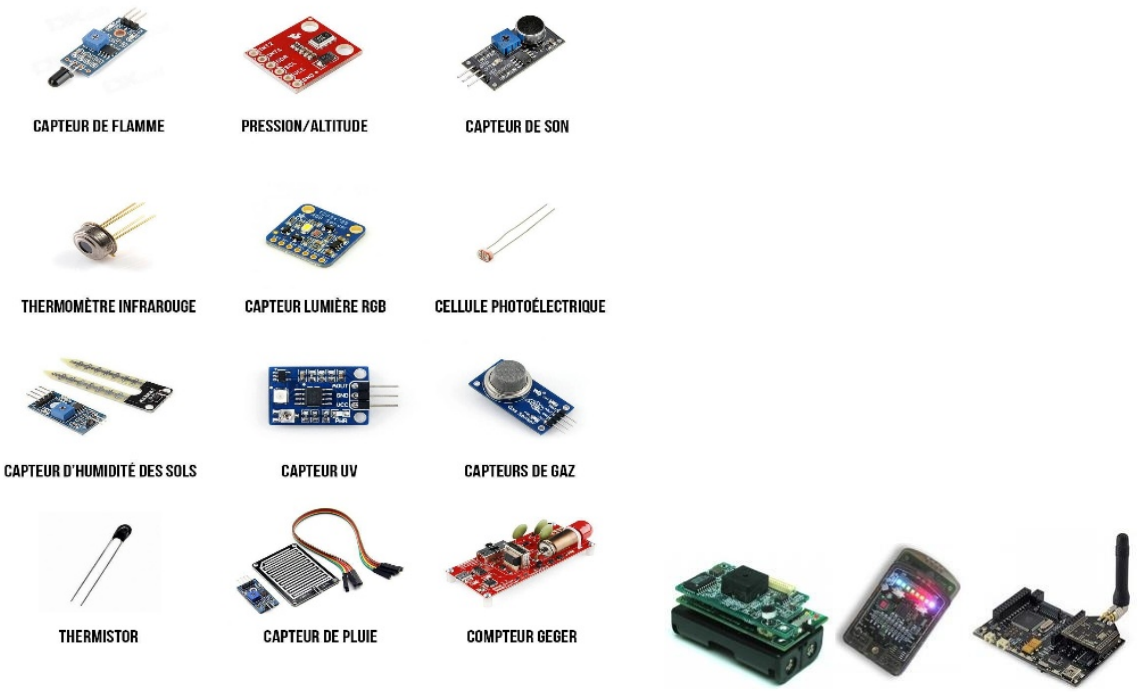


FIGURE 1.1 – Une série de capteurs mesurant des variables physiques [1, 2]

tégration au niveau du système. Cependant, la technologie *RFID* et les RCSFs possèdent différents formats de stockage, différents formats d'accès à l'information et différents mécanismes de contrôle et de sécurité. Par conséquent, à cause de différents formats de données et de différentes directions d'application, la technologie *RFID* et les RCSFs possèdent de différentes méthodes de traitement des données pour le filtrage, l'agrégation et d'autres traitements de données. Bien que la technologie *RFID* est largement utilisée, elle est exposée à de nombreux problèmes à résoudre, notamment : codage uniforme, conflits de collision, protection de la confidentialité, gestion de la confiance dans l'IoT, problèmes de sécurité et solutions techniques dans les RCSFs [41].

Les Figures 1.2 représentent les différentes utilisations de la technologie *RFID*.

FIGURE 1.2 – Déploiement de la technologie RFID [3–5]

1.3 Internet des Objets (IoT)

Plusieurs définitions ont été données à l'IoT vu qu'il est assez difficile de capturer l'essentiel de l'IoT dans une seule définition unique. Historiquement, Kevin Ashton (directeur exécutif de MIT Auto-ID Labs) a été le pionnier du terme Internet des objets (**en anglais** Internet of Things (IoT)) pour la première fois en 1999 [42] en mentionnant : "*l'Internet des objets a le potentiel de changer le monde, tout comme Internet l'a fait. Peut-être encore plus*". Ensuite, le centre MIT Auto-ID a présenté sa vision de l'IoT en 2001 [43]. Ce paradigme s'est incroyablement développé en incluant toujours plus de nouvelles technologies, d'objets innovants allant de celui des microcontrôleurs, de la nanotechnologie, des capteurs et actionneurs sans fil à de véritables infrastructures complexes de plus grande ampleur qui fera l'objet d'une vie intelligente.

En plaçant le monde virtuel (i.e. Internet) et le monde physique (i.e. les objets) ensemble sémantiquement signifie un réseau mondial d'objets interconnectés adressables de manière unique, basé sur des protocoles de communication standard [44]. L'IoT fait référence à une connectivité stricte entre le monde numérique et le monde physique [8].

De nombreux chercheurs ont défini l'IoT de différentes manières. Dans ce qui suit, nous présentons les principales définitions de ce paradigme :

Selon les auteurs dans [45], "les objets ont des identités et des personnalités virtuelles opérant dans des espaces intelligents en utilisant des interfaces intelligentes pour se connecter et communiquer dans l'environnement social.

- Selon un groupe de projets de recherche européens [31] sur l'IoT, *"les objets sont des participants actifs dans les processus commerciaux, informationnels et sociaux où ils peuvent interagir entre eux et avec l'environnement en échangeant des données et des informations détectées sur l'environnement ; tout en réagissant de manière autonome aux événements du monde réel/physique et l'influencer en exécutant des processus qui déclenchent des actions et créent des services avec/sans intervention humaine*".

- Dans [46], les auteurs ont défini l'IoT comme "*une infrastructure de réseau mondial dynamique avec des capacités d'auto-configuration basées sur des protocoles de communication standards et interopérables où les 'objets' physiques et virtuels ont des identités, des attributs physiques et des personnalités virtuelles en utilisant des interfaces intelligentes qui sont parfaitement intégrées au réseau d'information*".

- Une autre définition largement acceptée est suggérée par [47] : "*l'IoT permet aux personnes et aux objets d'être connectés à tout moment et en tout lieu en utilisant idéalement n'importe quel chemin/réseau et tout service*".

En plus de ces définitions, il en existe encore plusieurs études qui ont défini l'IoT dans différents contextes notamment dans [48] : "L'intégration des appareils minuscules appelés 'objets intelligents' (Smart Object (SO)), généralement alimentés par des batteries équipés d'un microcontrôleur (MCU) et d'émetteurs-récepteurs. Les services offerts par ces objets intelligents sont appelés services intelligents (SS) [49, 50]".

Les mêmes points du concept de l'IoT ont été également observés dans la définition dans [51], qui peuvent être résumés comme suit. L'IoT est :

- Une infrastructure qui existe à l'échelle mondiale,

- Composé d'agents IoT appelés "Objets",
- Interconnectés pour que les données puissent être partagées et
- Possède un potentiel d'impact technologique et societal grâce à des applications et des services avancés.

L'idée fondamentale du concept d'IoT est de rajouter de la communication aux objets physiques qui nous entourent, afin de les rendre dynamiques, collaboratifs et plus efficaces. Cette communication peut se faire entre objet-objet ou bien objet-personne ayant des objectifs divers qui se résument tous dans un seul but qui est, rendre l'environnement plus intelligent (voir Figure 1.3). Ces objets sont identifiés d'une manière unique ainsi qu'ils permettent d'échanger, collecter, stocker des informations, rendre accessible aux êtres humains les informations collectées et d'interagir naturellement entre eux. Toutes ces fonctions ont permis à ces objets de prendre des décisions de manière autonome, permettant un nouvel ensemble d'applications et de services.

FIGURE 1.3 – Extension d'internet aux objets du quotidien [6]

Un exemple de ce contexte [52], une plante à côté d'une fenêtre peut tweeter à quel point elle se sent confortable (en détectant la température et l'humidité). Comme elle peut donner un ordre aux rideaux de la fenêtre de se fermer partiellement quand il fait très chaud. Il y a une décennie, cela semblait irréaliste ou très coûteux et difficile à mettre en oeuvre. Cependant, il devient maintenant réaliste avec la disponibilité des matériels pour les objets intelligents, des logiciels libres et open-source développés spécialement pour faciliter la manipulation des objets dans un environnement d'IoT.

La Figure 1.4 visualise la définition globale de l'IoT ainsi que ses interactions entre ses différents composants. Divers acteurs de l'IoT, par exemple des particuliers, des entreprises ou le gouvernement, interagissent avec des agents IoT appelés "Objets" ou des applications et des services via des interfaces "Homme-Machine (H2M)". Les objets et les applications produisent des données qui sont partagées via le réseau interconnecté en fournissant un échange appelé interaction "Machine-to-Machine (M2M)". Les applications et

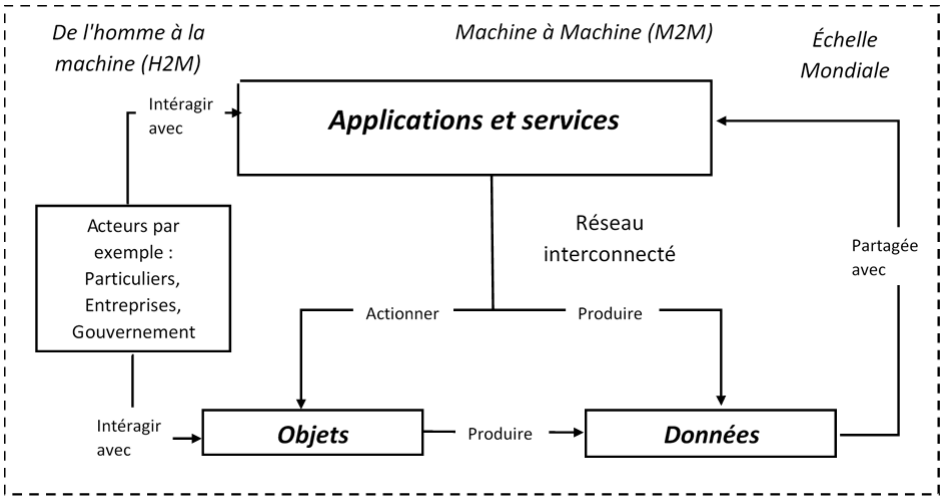


FIGURE 1.4 – Visualisation de la définition d'IoT [7]

les services, éventuellement dans plusieurs domaines d'applications, agissent sur les données pour faire actionner les objets ou bien pour produire plus de données. Ces derniers peuvent contenir des informations qui mènent à divers impacts sociétaux positifs, tels qu'une grande productivité avec l'automatisation intelligente de longues tâches. Toutes ces interactions peuvent se produire à une l'échelle mondiale.

Les noeuds de capteurs dans l'environnement IoT sont souvent appelés des dispositifs à ressources limitées (réseaux à contraintes). Ce sont de petits appareils avec une capacité de stockage et de traitement limitée qui utilisent des batteries déployés à grande échelle. En outre, ces derniers sont distribués largement, ce qui implique des problématiques de fiabilité, de performance, de sécurité et de confidentialité.

1.4 Domaines d'applications d'IoT

De nombreux types de services peuvent être imaginés avec l'arrivée de ces objets intelligents, car les informations qu'elles collectent permettraient aux gens de connaître l'état exact de l'environnement surveillé. Par conséquent, les domaines d'applications dans l'IoT peuvent être reconnus dans une vaste gamme et les défis augmentent de jour en jour. La Figure 1.5 répertorie diverses applications de l'IoT dans différents domaines.

Dans les environnements intelligents, la technologie IoT offre plusieurs avantages en facilitant la vie du quotidien. Par exemple, les lumières et le chauffage s'éteignent automatiquement lorsque le bâtiment est vide en offrant une économie d'énergie ainsi qu'une sécurité des zones précises est assurée la nuit. Également, dans une maison intelligente, on peut retrouver un réfrigérateur intelligent qui pourra commander automatiquement de la nourriture pour toute la famille. Dans les logistiques intelligentes, l'IoT permet une technologie de traitement de l'information en temps réel qui prend en charge la surveillance des produits, des matières premières...etc. En outre, l'IoT ouvre de nouveaux moyens dans le domaine de la santé permettant notamment une vie assistée aux personnes âgées ou malades. Par exemple, un système de surveillance de la santé peut vérifier l'état de notre corps, le comparer avec nos enregistrements dans des bases de données et informer un médecin si nécessaire. L'Internet des objets peut également devenir un élément cen-

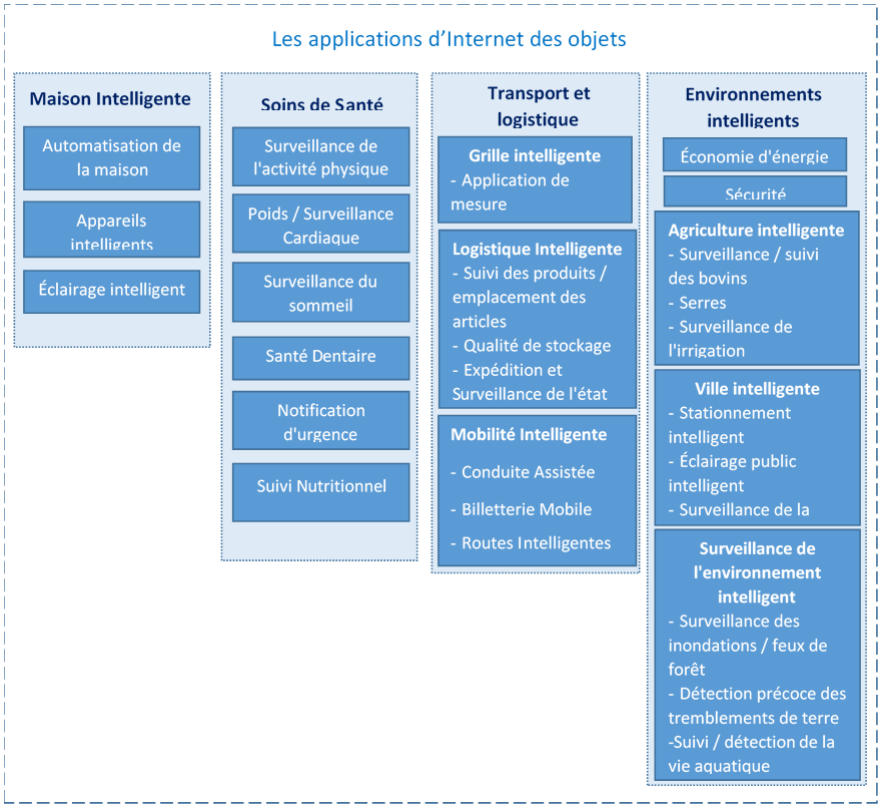


FIGURE 1.5 – Les différents applications d'IoT [8–15]

tral des systèmes de véhicules intelligents capables d'échanger facilement des informations pour nous rendre en sécurité jusqu'à notre destination ; notamment une conduite assistée en suivant des routes d'une manière intelligente.

1.5 Pile protocolaire d'IoT

Avec l'ère de l'IoT, les protocoles conventionnels (notamment ceux de la pile TCP/IP) ne peuvent pas répondre aux contraintes du nouveau paradigme IoT. Par conséquent, les organismes de normalisation IETF et IEEE ont anticipé cette nécessité et ont introduit une nouvelle pile protocolaire qui facilite le déploiement efficace des LLN dans le contexte de l'IoT. Les travaux de normalisation de l'IETF sur l'IoT ont également conduit à la mise en place des protocoles de communication légers adaptés aux objets connectés. Ces protocoles sont principalement hiérarchisés dans une pile protocolaire dédiée spécialement à l'IoT qui est composé de six couches [16] à savoir : application, transport, adaptation, MAC et physique.

Afin de mettre en oeuvre l'écosystème d'IoT, il est nécessaire d'utiliser le système d'exploitation Contiki avec sa pile protocolaire. La Figure 1.6 représente les différentes couches de l'architecture IoT ainsi que les différents protocoles utilisés. Un ensemble de ces protocoles sont mis en place sur chaque noeud du réseau afin de permettre le bon fonctionnement de l'IoT.

Dans les sous-sections suivantes, nous expliquons brièvement les différentes couches de la pile en mettant l'accent sur chacun de leurs composants en particulier : ContikiMAC et

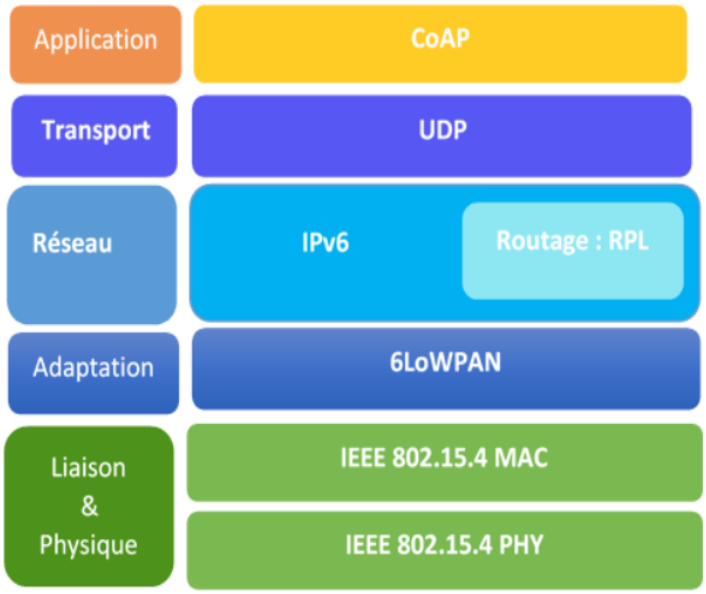


FIGURE 1.6 – La pile protocolaire standardisée de l'IoT [12, 16, 17]

IEEE 802.15.4 (radio sans fil), IPv6 (connectivité réseau) avec 6LoWPAN, RPL (routage), UDP et CoAP.

1.5.1 La couche Application

La couche application est responsable de la gestion des interactions directes avec les utilisateurs finaux. Parmi les fonctions les plus importantes de cette couche sont le traitement des données provenant des différents utilisateurs et la fourniture des services en temps réel. Ainsi que toute décision de contrôle, de sécurité ou bien de gestion des applications est prise par la couche application en fournissant une gestion globale du système IoT.

Plusieurs protocoles de la couche application apparaissent comme susceptibles de répondre à certains besoins particuliers des applications IoT. Parmi ces protocoles, CoAP est le protocole contraint de la couche application normalisé pour l'IoT [53]. Le protocole CoAP [53] est un protocole de transfert Web, conçu par le groupe de travail CORE (COnstrained RESTful Environments) de l'IETF afin de répondre aux capacités des noeuds à ressources limitées. CoAP peut être intégré sur des noeuds très contraints car les messages sont caractérisés par un en-tête court de 4 octets. De plus, CoAP est une version allégée d'HTTP adaptée aux équipements à faible ressources, ainsi qu'il est assez similaire à HTTP en termes de modèle client/serveur.

Le protocole CoAP définit des messages de demande et de réponse afin de demander et de fournir des services d'application pour les dispositifs contraints. La différence principale entre HTTP et CoAP réside lors de l'échange des messages, i.e. les messages HTTP sont échangés simultanément entre le client et le serveur, tandis que les échanges CoAP sont asynchrones sur User Datagram Protocol (UDP). Cette différence reflète positivement sur l'économie d'énergie. Pour des raisons d'identification, les messages CoAP sont équipés d'un ID. Ces derniers se composent de quatre types de messages différents où chacun a

un rôle spécifique, à savoir, confirmable, non confirmable, accusé de réception et réinitialisable. Les messages qui nécessitent une fiabilité sont configurés comme des messages confirmables avec des messages d'accusé de réception, par contre ceux qui ne nécessitent pas de fiabilité sont appelées non confirmables. Parmi les applications qui peuvent bénéficier du protocole CoAP sont les réseaux contraints et les LLNs, en particulier les applications M2M [54, 55].

1.5.2 La couche Transport

Le protocole UDP [56] est le protocole de transport normalisé pour l'architecture de l'IoT. La plupart des applications IoT sont mieux adaptées aux protocoles UDP car il est difficile d'utiliser sur des dispositifs à ressources limitées, notamment les dispositifs d'IoT, une mise en oeuvre complexe comme celle du TCP. Le protocole UDP est beaucoup plus rapide que le protocole TCP avec un taux de messages de contrôle réduit. Cependant le seul inconvénient du protocole UDP qu'il est un protocole sans connexion, i.e. il ne garantit pas la livraison synchrone des datagrammes (pas de contrôle de congestion ou de respect de l'ordre des paquets). Par conséquent, il est nécessaire de le combiner avec le protocole de la couche application afin d'améliorer sa fiabilité. En particulier, le protocole CoAP qui implémente des mécanismes optionnels afin de détecter la perte de messages et de les retransmettre si nécessaire afin de pallier l'absence de garantie d'UDP [57]. Ainsi le protocole sous-jacent hébergeant le protocole UDP doit respecter la séquence précise de livraison des datagrammes. En outre, le protocole UDP prend éventuellement en charge "Datagram Transport Layer Security (DTLS)" [58] afin d'assurer la confidentialité des communications et de fournir une sécurité de haut niveau.

1.5.3 La couche Réseau

a) Le protocole IPV6

La couche réseau est responsable de la transmission des données vers les couches supérieures. Compte tenu du nombre potentiellement élevé des noeuds dans les réseaux IoT (le grand nombre d'objets IoT), l'espace d'adressage IPv4 n'est plus envisageable. En effet l'espace d'adressage IPv6 [59], avec ses 2^{128} adresses possibles, apparaît d'être une solution d'adressage viable dans l'IoT [8]. La version 6 du protocole IP (IPv6) est une extension de la taille de l'adresse de 32 bits à 128, permettant jusqu'à $3{,}4*10^{38}$ adresses uniques.

IPv6 offre également une très bonne option pour accéder aux ressources de manière unique et à distance [60]. De plus, IPv6 fournit des services de découverte de voisins et de configuration automatique d'adresse. En outre, IPv6 envoie son paquet via la couche MAC (Medium Access Control) conformément à une politique de routage.

b) RPL (Protocole de routage IPV6 pour les réseaux de faible puissance et avec perte)

Comme la couche réseau prend en charge l'adressage IPv6, elle définit aussi le routage global des paquets de données. La fonction principale des protocoles de routage dans un réseau est de trouver et d'établir des routes entre des entités souhaitant communiquer.

Après la construction des chemins entre les noeuds du réseau, le protocole de routage acheminera les paquets de données depuis un noeud source vers un noeud de destination.

L'organisme de normalisation IETF a créé le groupe de travail "routage sur réseaux à faible puissance et à pertes (***en anglais*** Routing Over Low power and Lossy networks (ROLL))" [61] afin de concevoir un protocole de routage IPv6 dédié aux réseaux LLNs appelé "RPL" [62]. RPL a été spécialement conçu afin de prendre en charge les exigences des réseaux LLNs qui nécessitent des caractéristiques spéciaux telles que : énergie limitée, capacité de traitement limitée et topologie hautement dynamique. En vue du lien pragmatique remarquable entre les LLNs et l'IoT, les LLNs sous-tendent l'infrastructure de l'IoT. Il en résulte que le protocole de routage RPL est rapidement devenu le protocole de routage de facto pour l'IoT.

Le protocole RPL est considéré comme un protocole de routage à vecteur de distance proactif car il pilote des tables de routage en les mettant à jour fréquemment selon deux modes différents, à savoir, le mode avec stockage (storing) et sans stockage (non-storing). Plus de détails sur le protocole RPL sont présentés dans le chapitre 2.

1.5.4 La couche Adaptation (6LoWPAN)

La couche adaptation IPv6 over Low power WPAN (6LoWPAN) comme son nom l'indique a été créée principalement pour une adaptation d'IPv6 sur le standard IEEE 802.15.4. Cette couche est située entre la couche réseau IPv6 et la couche MAC.

Le groupe de travail "6LoWPAN Working Group (WG)" créé par l'IETF a proposé une couche adaptation 6LoWPAN (IPv6 sur les réseaux personnels sans fil à faible puissance) [63–65], afin de surmonter l'obstacle de limitation des ressources des noeuds, permettant ainsi une adaptation de toutes les capacités du protocole IPv6 sur la norme IEEE 802.15.4.

L'objectif principal de cette couche est d'optimiser la transmission des paquets IPv6 au-dessus des réseaux IEEE 802.15.4. Afin de prendre en charge les gros paquets IPv6 sur des trames MAC/PHY 802.15.4, 6LoWPAN fournit des techniques de fragmentation, d'encapsulation et de compression d'en-tête paquets IPv6. Les principaux services du 6LoWPAN pour prendre en charge le fonctionnement transparent d'IPv6 sont détaillés comme suit :

- **Fragmentation** : Afin d'optimiser la transmission des paquets IPv6 au-dessus des réseaux IEEE 802.15.4, 6LoWPAN fragmente les paquets IPv6 en plusieurs trames MAC plus petites afin de prendre en charge l'exigence MTU minimale d'IPv6. Ainsi, 6LoWPAN joue un rôle essentiel afin de garantir le bon assemblage des paquets fragmentés sur plusieurs sauts.

- **Compression** : La couche adaptation fournit une compression d'en-tête pour réduire la surcharge de transmission [66]. En raison de la bande passante limitée (127 octets) fournie par le protocole IEEE 802.15.4, le standard IETF a proposé une normalisation RFC 6282 [65] afin d'adapter que 60 à 80 octets d'une charge utile UDP. Cette technique permet de minimiser et redimensionner les octets supplémentaires en compressant l'en-tête des paquets IPv6 de 40 octets en aussi peu que 4 octets [67].

L'attractivité de 6LoWPAN réside dans l'activation d'IPv6 avec un taux d'overhead réduit [67] en termes de : taille de code (12-22K), exigences de RAM (4K) et taille d'en-

tête (2-11 octets). Cependant, 6LoWPAN avait besoin d'un mécanisme complémentaire pour permettre la livraison de bout en bout de paquets IPv6, i.e. un protocole de routage. Par la suite l'IETF a créé le groupe de travail ROLL WG qui a de même créé le protocole de routage RPL.

1.5.5 La couche MAC et Physique

a) Couche liaison de données (MAC)

Le contrôle d'accès au médium (***en anglais*** Medium Access Control (MAC)) de la couche liaison de données est chargé de la gestion de contrôle d'accès au support physique (canal de transmission), ainsi que la transmission des trames de données via le médium. En outre, la couche MAC permet les fonctions suivantes : gestion des balises (mode asynchrone (sans balises) et synchrone (avec envoi de balises)), gestion des intervalles de temps garantis Guaranteed Time Slot (GTS), validation de trame, livraison de trame reconnue. La transmission des trames de données dans des réseaux contraints engendre des événements de gaspillage d'énergie tels que : les collisions, l'écoute oisive, messages de contrôle du protocole...etc.

b) Couche physique

La couche physique est responsable principalement de la transmission et de la réception réelle des données sur le support physique (radio) sous forme de signaux électromagnétiques. En plus, elle fournit plusieurs services notamment : la sélection de fréquence pour le canal choisi (selon les spécifications), l'activation et la désactivation de l'émetteur-récepteur radio, détection d'énergie du canal actuel, l'estimation de l'indicateur de qualité de la liaison (Level Quality Indicator (LQI)) pour les trames reçues et l'exécution de l'évaluation claire du canal (Clear Channel Assessment (CCA)) afin de détecter les canaux occupés avec accès multiples.

Aperçu sur l'IEEE 802.15.4

IEEE 802.15 WPAN Task Group a proposé les protocoles MAC IEEE 802.15.4 et IEEE 802.15.4 physique à très faible consommation d'énergie pour les deux couches basses de la pile protocolaire : couche liaison MAC et couche physique respectivement. IEEE 802.15.4 est une normalisation du standard IEEE pour la communication sans fil dans un environnement contraint (faible coût, faible puissance, faible débit, courte portée et faible consommation énergétique) avec des ressources limitées (mémoire, énergie, bande passante) [68].

Le protocole IEEE 802.15.4 vise principalement une transmission de données d'une manière fiable, un coût extrêmement faible et une consommation énergétique raisonnable. Il s'agit d'un protocole radio normalisé pour un réseau à faible consommation, faible débit, faible coût, ad-hoc et auto-organisé pour les applications de réseautage domestique [69]. Afin de minimiser la consommation d'énergie, le protocole IEEE 802.15.4 divise le temps en cycles de travail, i.e. il alterne les périodes d'activités (transmission et réception de données) avec les périodes de sommeil en éteignant la radio (médium de transmission). De plus, IEEE 802.15.4 emploie trois gammes de fréquences différentes selon les réglementations dans différents pays dans le monde.

La technologie IEEE 802.15.4 définit l'unité de transmission maximale (Maximum Transmission Unit (MTU)) à 127 octets, tandis qu'IPv6 nécessite une transmission de paquets avec un MTU de 1280 octets [70]. D'où intervient le rôle de la couche d'adaptation 6LoWPAN, qui prend en charge la fragmentation et le réassemblage IPv6 afin de faire transmettre des paquets IPv6 sur les réseaux de capteurs sans fil utilisant la technologie de communication IEEE 802.15.4. Ainsi, l'émergence des architectures telles que IEEE 802.15.4, IPv6 et 6LoWPAN deviennent dominantes dans la pile de communication d'IoT.

1.6 Système d'exploitation d'IoT -Contiki-

Contiki [71] est un système d'exploitation open-source, léger, hautement portable (porté sur un grand nombre de plate-formes), développé en langage C, conçu spécifiquement pour les dispositifs à faible coût et à faible consommation de ressource notamment les réseaux de capteurs et l'IoT. Contiki est divisé en deux parties : un noyau piloté par des événements et les programmes chargés. Le noyau comprend le noyau contiki, des bibliothèques, un chargeur de programmes et d'un ensemble de processus ainsi que la pile de communication. Les programmes chargés sont les applications implémentées.

Contiki fournit des bibliothèques pour l'allocation de mémoire, la manipulation des listes et les abstractions de communication. Il prend en charge trois piles de communication : uIP, TCP/IP et Rime (des piles légères pour les microcontrôleurs basse consommation), et fournit un large éventail de protocoles de communication notamment les protocoles standards de faible puissance tels que ICMPv6, ContikiMAC, 6LoWPAN, RPL et CoAP. Contiki utilise un mécanisme de programmation simple correspondant aux normes C appelé protothread qui est un mécanisme à faible surcharge pour la programmation simultanée [72]. En outre, Contiki fonctionne sous une large gamme de dispositifs sans fil de basse consommation tels que micaz, sky, seed-eye, msb430, cc2530dk, z1, win32, sensinode, wismote. . .etc. Ainsi, il intègre des fonctionnalités d'économie d'énergie en incluant une bibliothèque de gestion de l'énergie [73] qui mesure le temps passé à exécuter par divers composants des noeuds capteurs. En plus de toutes ces fonctionnalités, Contiki fournit des mécanismes qui aident à la programmation des applications d'objets intelligents. Il fournit également un système d'exécution de profil de puissance énergétique au niveau du réseau appelé Powertrace [74] qui utilise le suivi d'état pour estimer et mesurer la consommation d'énergie de chaque noeud avec une précision qui peut atteindre jusqu'à 94%. La figure 1.7 montre le schéma principal de l'architecture du système Contiki.

1.6.1 Installations de communication (uIPV6/Rime)

Les protocoles de communication représentent l'atout le plus abondant et le plus varié de Contiki. Dans ce contexte, Contiki comprend deux piles réseaux différentes [74] : la pile IPv6 basse consommation certifiée uIPv6 [75] et la pile de communication Rime Sensornet [76]. La Figure 1.7 illustre un modèle global qu'on a pu résumer depuis les deux études [75,76], représentant les deux couches de la pile de communication Contiki. La pile uIPV6 fournit la mise en réseau IPv4 et IPv6 tandis que la deuxième pile Rime représente un ensemble de protocoles légers conçus pour les réseaux sans fil à faible puissance. Les trois couches inférieures sont communes aux deux piles uIPV6 et Rime. L'ancienne pile Rime offre des services multipoint à point (M2P) alors que la nouvelle pile uIPV6 offre

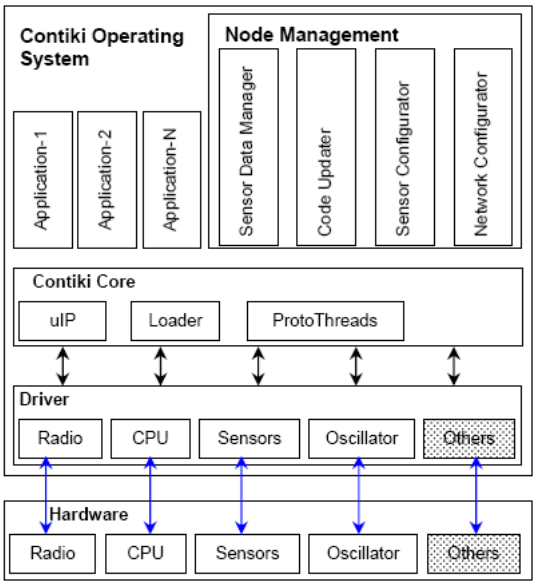


FIGURE 1.7 – Architecture du système d'exploitation Contiki [18]

des services M2P, point à multipoint (P2M) et point à point (P2P). Les deux piles offrent des communications point à point à un seul saut en plus des services de diffusion.

La pile "Rime" est prise en charge par Contiki lorsque la bande passante est critique ou que la pile de mise en réseau uIPv6 est dépassée. Elle prenant en charge des opérations simples telles que l'envoi d'un message à tous les voisins ou des opérations plus complexes comme l'inondation du réseau, le multi-saut sans adresse et la collecte des données semi-fiable [77]. En outre, la pile "Rime" offre un routage multi-sauts de n'importe quel point vers un noeud racine, i.e. Rime ne spécifie pas comment les paquets sont acheminés de la source à la destination tandis que la pile uIPv6 peut être connectée à Internet IPv6 en offrant des fonctionnalités de routage complètes entre tous les noeuds. Par ailleurs, les couches MAC, Radio Duty Cycling (RDC) et physique sont communes aux deux piles en respectant les spécifications IEEE 802.15.4. Au niveau de la couche physique, des pilotes spécifiques pour les différentes radios utilisées dans les noeuds sont inclus dans Contiki dans le répertoire core/dev et certaines parties des pilotes sont spécifiques à un processeur donné se trouvent dans le sous-répertoire approprié du répertoire core/cpu. Les couches MAC et RDC seront décrites en détails dans la sous-section suivante.

Dans notre thèse, on a travaillé sous les deux couches Rime et uIPv6 en fournissant deux contributions différentes qui sont présentées en détails dans les chapitres 3 et 4.

1.6.2 Caractéristiques d'économie d'énergie dans Contiki

Le système d'exploitation Contiki offre en dessous de la couche MAC différents mécanismes d'économie d'énergie appelés aussi cycles d'utilisation radio (***en anglais*** Radio Duty Cycle (RDC)) comme illustre la Figure 1.8. Certains de ces mécanismes maximisent l'utilisation de l'énergie en désactivant la radio autant que possible notamment la technique ContikiMAC [78], tandis que d'autres restent en écoute en laissant la radio ouverte en permanence comme le sicslowMAC. Ces techniques consistent soit à sélectionner les noeuds actifs parmi tous les noeuds déployés dans le réseau ou bien à éteindre (respec-

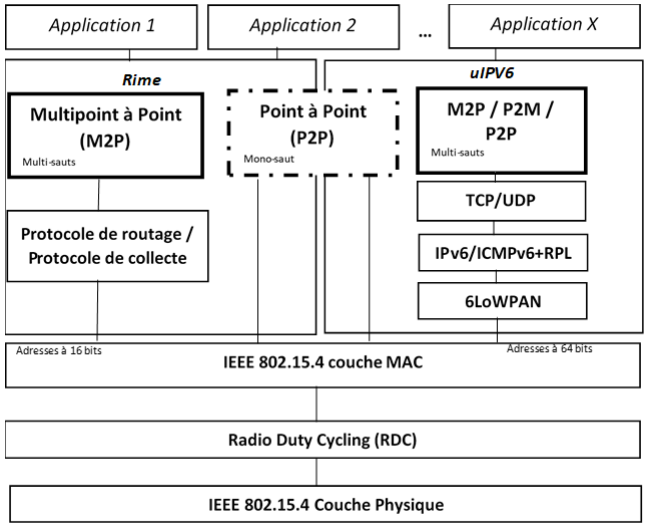


FIGURE 1.8 – Vue globale de la pile de communication dans Contiki

tivement allumer) la radio des noeuds actifs lorsqu'aucune communication n'est requise. Ces techniques sont fortement liées au protocole d'accès au médium [78].

Les périodes de temps pendant lesquelles les noeuds sont actifs ou inactifs doivent être adaptées selon des exigences spécifiées par l'application. En effet, l'une des sources de grand gaspillage d'énergie sur un noeud provient de l'écoute inactive, ce qui signifie que la radio est allumée mais le noeud ne reçoit/transmet aucune donnée [79].

Contiki offre divers pilotes RDC : nullRDCMAC, sicslowMAC, X-MAC, contikiMAC. Nous donnons un aperçu sur ces mécanismes comme suit :

- **NullRDCMAC**
  NullRDC n'éteint jamais la radio et vérifie 128 fois par seconde (à chaque tick d'horloge) les paquets entrants, i.e. il ne prend pas en compte l'économie d'énergie car il n'effectue aucun cycle d'utilisation radio (RDC) et maintient la radio toujours allumée à tout moment [80]. Il fonctionne comme une couche traversante qui ne transmet qu'un paquet et conserve les résultats d'une telle transmission (succès ou collision). NullRDC a deux tâches principales : (i) il utilise des fonctions d'encadrement pour créer un en-tête et (ii) il vérifie simplement si le paquet a été reçu ou qu'une collision s'est produite.

- **SicslowMAC**
  Un autre pilote de Contiki qui ne tient pas en compte l'économie d'énergie est le SicslowMAC. SicslowMAC est un protocole simple qui crée les trames IEEE802.15.4 et les transmet au noeud suivant, sans jamais éteindre la radio (similaire à NullRDC) d'où SicslowMAC correspond à la RDC où la batterie a une durée d'utilisation minimale. Le SicslowMAC prend également en charge l'analyse d'une trame reçue pour le traitement dans les couches supérieures (6LoWPAN) [78].

- **Cx-MAC/X-MAC**
  X-Mac [81] est un mécanisme qui n'éteint pas sa radio après la transmission des

paquets. Bien qu'il n'offre pas la même efficacité énergétique que ContikiMac mais il a des exigences de synchronisation moins strictes.

Lorsqu'un expéditeur veut envoyer un paquet, il l'envoie à plusieurs reprises en laissant un intervalle de temps aléatoire pour permettre à d'autres expéditeurs candidats de tenter leur chance d'envoi. Une fois le récepteur prévu se réveille, il répond par un ACK tout en restant réveillé. Ensuite lors de la réception de cet accusé, l'expéditeur envoie sa trame. Afin de valider la réception, le récepteur stocke la trame et envoie un ACK ensuite il se rend en veille.

La seule différence significative entre ContikiMac et X-MAC est l'intervalle entre les retransmissions : un récepteur X-MAC ne peut pas passer en mode endormi aussi rapidement comme celui qu'un récepteur ContikiMac ayant des règles de "sommeil rapide". Par conséquent, l'intervalle entre les répétitions des paquets diffusés peut être plus long, ce qui favorise ContikiMac par une économie d'énergie lors d'une diffusion intense. Plusieurs travaux ont été focalisés sur une comparaison entre ces mécanismes notamment [78, 80, 82, 83] en déduisant que X-MAC a un overhead plus élevé et un taux de livraison proche de celui de NullRDC, ainsi qu'il a un délai inférieur à ContikiMAC, ce qui peut le rendre utile dans le cas où le délai représente une contrainte à satisfaire.

Cx-MAC est une implémentation modifiée et simplifiée du protocole X-MAC d'origine [81], optimisé pour Contiki. Cx-MAC utilise un préambule court pour réduire le temps d'envoi de l'expéditeur. Ce préambule permet aux récepteurs d'interrompre l'envoi du préambule même au milieu de la transmission de ce dernier [84]. Dans Cx-MAC, les informations d'adresses cibles sont intégrées dans le préambule afin que les récepteurs non cibles qui sont en écoute puissent être immédiatement remis en veille.

- **ContikiMAC**
  ContikiMAC est le protocole RDC par défaut dans Contiki. Il s'initie par l'expéditeur i.e. l'expéditeur est responsable de réveiller le récepteur. Il est asynchrone (ne se synchronise pas avec une horloge globale) [52]. Dans ContikiMAC, quatres états de cycle d'utilisation radio sont pris en compte : émission, réception, écoute inactive et sommeil.

  ContikiMAC est similaire à d'autres protocoles d'écoute à faible puissance en possédant un mécanisme de réveil plus avancé [78], qui représente des réveils périodiques pour écouter les transmissions de paquets des voisins. Lorsqu'un expéditeur envoie un paquet en unicast, cette opération continue de se répéter jusqu'à ce qu'il reçoive un ACK depuis le récepteur. Par la suite, l'expéditeur enregistre l'heure de réveil du récepteur pour les prochaines transmissions [85]. De plus, lors d'une diffusion d'un message par un expéditeur, il l'enverra pendant toute une période de réveil et tous les noeuds doivent se réveiller pendant un certain temps de cette période afin de pouvoir recevoir ce message [52]. Pendant l'état de réveil, si le paquet est détecté, le récepteur sera en état "ON" pour la réception de paquets ; ensuite il reconnaît l'expéditeur. Il utilise des synchronisations précises entre les transmissions de données. De plus, il utilise une optimisation rapide du mode sommeil qui permet de détecter rapidement les réveils faussement positifs pour un fonctionnement économe en énergie.

ContikiMAC est actuellement le protocole RDC le plus économe en énergie de Contiki combiné avec CSMA en tant que protocole MAC [78].

1.7 Environnement de simulation pour l'IoT : COOJA

Parmi les fameux outils qui peuvent être utilisés afin d'étudier les problèmes de recherche dans un écosystème IoT nous pouvons citer l'environnement de simulation Cooja.

Le simulateur Cooja [86] est largement utilisé par la communauté des chercheurs de l'IoT avec un pourcentage de travaux publiés menés via Cooja qui a atteint 63% en 2017 [87].

Cooja peut être considéré comme une approche hybride en termes d'outil d'émulation et de simulation inter-niveaux. Il est intégré d'une manière native dans Contiki en constituant une glu entre la partie qui émule le matériel (MSPsim, Avrora) et le système d'exploitation Contiki. MSPsim [88, 89] et Avrora [90, 91] représentent des projets open-source qui émulent des microcontrôleurs de type MSP430 ou AVR respectivement. Le simulateur Cooja est assez proche du vrai matériel car il utilise le logiciel MSPSim pour émuler l'architecture MSP430 et les performances d'un microcontrôleur MSP430F1611, qui est utilisé par TelosB. Cooja simule le fonctionnement de différents types de mouvements réels de capteurs tels que Tmote Sky, Z1, WiSMote, MicaZ et ESB (carte de capteur intégrée). Ces types représentent une interface entre la description matérielle du noeud et le code contiki.

Cooja est un simulateur basé sur Java mais permet de développer des codes en C, conçu pour simuler des réseaux de capteurs exécutant le système d'exploitation Contiki [92]. Il permet une simulation simultanée à trois niveaux différents : niveau application, niveau système d'exploitation et niveau instruction code machine. Cooja implémente un certain nombre de modèles de canaux sans fil tels qu'Unit Disk Graph Medium (UDGM), Distance Loss (DL) and Directed Graph Radio Medium (DGRM). Dans UDGM et DL, la plage de transmission est modélisée comme un disque (portée de transmission) où tous les noeuds à l'intérieur de cette portée peuvent transmettre et recevoir des paquets avec une probabilité de taux de réussite de transmission (TX) et taux de réussite de réception (RX) respectivement. Il stocke la simulation dans un fichier xml avec l'extension 'csc' (fichier de configuration d'une simulation Cooja). Ce fichier contient des informations sur l'environnement de simulation, les plugins, les noeuds et leurs positions, et le support radio...etc. Le fait que Cooja fait partie du système d'exploitation Contiki, on lui place naturellement comme le meilleur choix pour le développement des réseaux à faible puissance notamment les RCSFs et IoT. Il bénéficie également de la communauté Contiki qui devient de plus en plus importante et offre un support non négligeable.

Enfin, les fonctionnalités et les caractéristiques susmentionnées de Cooja, en particulier, la prise en charge des simulations au niveau matériel sont les raisons cruciales de le considérer comme un simulateur pour notre étude.

1.8 Internet des objets multimédia (IoMT)

La croissance vigoureuse des dispositifs connectés à Internet au cours de la dernière décennie et la demande brutale du trafic multimédia ont donné naissance à l'émergence d'un nouveau paradigme sous-jacent à l'IoT, appelé l'internet des objets multimédia (***en anglais*** IoMT). Dans ce nouveau paradigme on assiste à des échanges de contenus multimédias tels que l'audio, la vidéo et le streaming et ce type d'échanges suscite un réel intérêt auprès de la communauté des chercheurs.

Plusieurs définitions sur ce nouveau paradigme IoMT ont été présentées, notamment :

Définition 1 : Les auteurs dans [50] ont introduit l'IoMT comme "*un nouveau paradigme dans lequel les objets multimédias hétérogènes intelligents interagissent et coopèrent entre eux ainsi qu'avec d'autres objets connectés à Internet afin de faciliter les services et les applications multimédias qui sont disponibles à l'échelle mondiale pour les utilisateurs*".

Définition 2 : Les auteurs dans [93,94] expliquent le concept des objets multimédias comme : "*Des objets capables d'acquérir des contenus multimédias du monde physique, étant équipés de dispositifs multimédias tels que des caméras et des microphones* ". Ainsi qu'ils définissent l'IoMT comme : "*Un réseau d'objets interconnectés capables d'acquérir des contenus multimédias du monde réel et/ou de présenter des informations de manière multimédia [93]*".

Définition 3 : Les auteurs dans [28] ont défini l'IoMT comme "*un ensemble d'objets multimédias équipés d'une connectivité Internet et d'une interaction avec d'autres objets sans intervention humaine conduisant à de vastes opportunités pour l'amélioration du mode de vie à l'être humain*".

Les catégories émergentes d'objets IoT ont tendance à être mobiles, multi-sensorielles et intelligentes telles que les capteurs portables, les téléphones intelligents et les véhicules intelligents. Ces derniers entraînent de plus en plus une augmentation du contenu multimédia dans l'IoT. Le contenu multimédia fait référence à une combinaison de deux ou plusieurs contenus multimédias différents tels que des données scalaires, de l'audio, de l'image, de la vidéo...etc. Récemment, le trafic vidéo sur Internet a considérablement augmenté et cette tendance devrait se poursuivre au cours des prochaines années. L'indice du réseau visuel de Cisco prévoyait qu'en 2021, le trafic vidéo IP mondial représentera 82% de tout le trafic Internet grand public [95]. Ainsi, le même rapport indique également que la vidéosurveillance représentera 3,4% du trafic vidéo Internet mondial [95]. De même le pourcentage réel pourrait même dépasser les prévisions à cause de l'émergence de nouvelles technologies qui utilisent la vidéosurveillance, comme les véhicules aériens sans pilote civils *(Unmanned Aerial Vehicle (UAV))* [96] et les véhicules autonomes [97].

Les objets intelligents multimédias sont généralement limités en termes de ressources notamment une bande passante et une consommation énergétique plus élevée, des ressources de mémoire volumineuses et une puissance de calcul plus élevée pour analyser et traiter les données multimédias fournies. Grâce aux technologies Micro-Electro-Mechanical Systems (MEMS) et Complementary Metal Oxide Semiconductor (CMOS), les dispositifs IoMT sont considérés comme des objets minuscules et à faible coût, possé-

dant un émetteur-récepteur de faible puissance, un microprocesseur, une batterie et un capteur [98].

Dans un réseau IoMT on peut distinguer trois scénarios d'utilisation du contenu multimédia :

1. Multimédia comme entrée IoT : Le contenu multimédia est acquis par des objets multimédias et il est utilisé par une application IoT afin de fournir un service bien déterminé.

2. Multimédia en tant que sortie IoT : Les objets IoT acquièrent des signaux, des données et des informations (contenu non multimédia) qui sont présentés sous forme d'un contenu multimédia par une application IoT.

3. Multimédia comme entrée et sortie IoT : Le contenu multimédia est acquis par des objets multimédia et il est présenté de manière multimédia par une application IoT.

Chaque scénario est illustré par une figure ci-dessous. La Figure 1.9 illustre un exemple du **premier scénario** : une caméra qui enregistre des images de personnes qui veulent entrer dans un endroit où l'entrée n'est autorisée qu'à des personnes bien précises. Ce scénario a besoin d'un dispositif multimédia (caméra) et d'un actionneur de porte. Une fois les images de personnes qui veulent entrer sont capturées par la caméra, elles sont renvoyées vers une plateforme IoT où une application est déployée. Cette application IoT joue le rôle d'un logiciel d'identification qui permet l'entrée dans ce lieu uniquement aux personnes autorisées. Une fois que le logiciel a identifié la personne, une commande est envoyée à l'actionneur de porte pour l'ouvrir, sinon la porte reste fermée et l'accès est refusé.

FIGURE 1.9 – Ouverture d'une porte aux personnes autorisées [19, 20]

Le **deuxième scénario** est illustré par la Figure 1.10. Divers objets IoT mesurent certains paramètres médicaux d'un patient (par exemple la température, les impulsions, la pression. . .etc.) qui sont collectés par la plateforme IoT. Cette application sert à présenter l'état du patient à partir du contenu multimédia mesuré, par exemple en utilisant des graphiques, des animations, des alarmes. . .etc.

FIGURE 1.10 – Application IoMT qui affiche les paramètres physiologiques à partir d'un contenu multimédia mesuré [21–25]

Enfin, le **troisième scénario** est représenté par Figure 1.11 où certaines caméras de surveillance enregistrent les images et le son d'un lieu. Ces informations multimédias sont collectées par une application IoT et présentées de manière multimédia (vidéos, audios) afin de fournir un service de contrôle de sécurité à distance.

L'IoMT s'étale sur une variété de domaines d'applications multimédias, [28], notamment : le développement d'une ville intelligente et la transformation des vies humaines, i.e. le multimédia dans l'agriculture, la santé intelligente, la sécurité, les processus industriels, les systèmes de gestion routière et les applications en temps réel. . .etc.

1.8.1 Domaines d'applications des IoMT

En raison de sa capacité à fournir des informations plus volumineuses, l'IoMT joue un rôle crucial dans de nombreux plans stratégiques sociétaux, scientifiques, civils et militaires. Des exemples de cas d'utilisation de l'IoMT comprennent la sensibilisation à la situation en matière de sécurité publique, la surveillance militaire, la gestion des catastrophes, la surveillance industrielle et domestique, la surveillance de la faune, la surveillance agricole et la surveillance générale des établissements de soins de santé et des personnes âgées, la surveillance du trafic, et la surveillance des habitats. . .etc. Parmi les types d'applications ayant contribué à la croissance exponentielle du trafic multimédia via Internet, nous citons la vidéoconférence, la vidéo à la demande à distance, la téléprésence,

FIGURE 1.11 – Application de surveillance à l'aide d'un dispositif multimédia [26, 27]

la gestion des transports optimisée à l'aide de caméras intelligentes, la diffusion de contenu en temps réel et les jeux en ligne...etc. La Figure 1.12 conceptualise la communication multimédia dans différentes applications sous-jacentes à l'IoMT.

Plus de fonctionnalités telles que la reconnaissance faciale, la détection de mouvement, l'identification de la plaque d'immatriculation, l'état du patient, la détection de trous et d'obstacles et la détection du crime peuvent être extraites en utilisant divers outils d'agrégation de données, d'analyse et d'extraction [28]. Ainsi dans [28], les auteurs ont classé de nombreuses applications IoMT en fonction de différents rôles en fournissant une taxonomie des applications de la communication multimédia sans fil dans l'IoT.

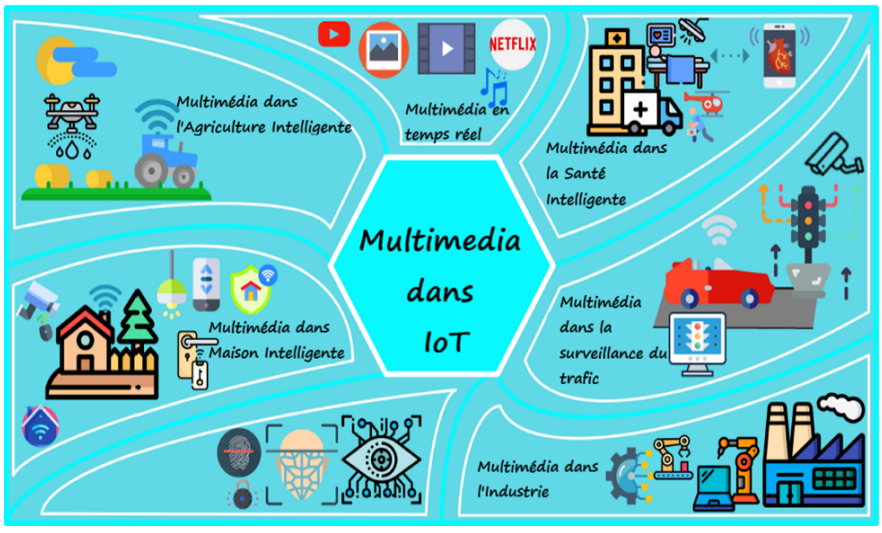


FIGURE 1.12 – L'intégration des applications multimédias dans l'IoMT [28]

On s'attend à ce que l'IoMT ait le potentiel d'un nombre énorme d'applications, parmi

ces applications nous citons dans le tableau 1.1 celles qui ont été développées dans le cadre des projets.

1.8.2 Défis des applications IoMT

L'introduction d'objets multimédias favorise un large éventail d'applications dans plusieurs domaines. D'où la naissance d'un grand intérêt pour le développement et l'utilisation de ses différents types d'applications. Par conséquent, le trafic multimédia s'augmente de plus en plus avec une croissance énorme dans le réseau mondial. En outre, plus la quantité de trafic est volumineuse, plus ça posera plus de défis engendrés par les dispositifs multimédias ou bien par le transport du trafic multimédia sur le réseau. En plus, l'information multimédia décrit un certain nombre de caractéristiques inhérents qui imposent un certain nombre de restrictions. Ainsi, plus de défis imposés par d'autres dispositifs hétérogènes qui font partie du réseau IoMT.

Afin de répondre aux contraintes de QoS du trafic multimédia, les exigences du réseau définies en termes de délai de bout en bout, de gigue et de taux de perte doivent être respectées afin de garantir une livraison fiable du contenu multimédia. Il n'en ait en aucun doute que de nombreuses recherches sur les solutions de divers problèmes sont actives pour aboutir à une structure réalisable et efficace de l'IoMT. En revanche, il en reste encore des défis à résoudre, certains sont décrits ci-dessous :

1. Sécurité : Comme il y aura de nombreux objets connectés ensemble et déployés à grande échelle, la sécurité représente un défi majeur car elle fournit des points d'entrée aléatoires aux malwares en créant plus de complexité et de nouveaux risques.

2. Gestion de l'hétérogénéité : Dans l'IoMT, différents types de dispositifs peuvent coexister en fournissant différents types de données multimédias qui peuvent différer en taille, en format...etc. Par conséquent, un nouveau défi pour le serveur qui collecte ces données provenant de nombreuses sources en utilisant des techniques différentes.

3. Taille des paquets de données : Les données multimédias sont caractérisées par une taille plus volumineuse que les données textuelles. Par ailleurs, la collecte et le traitement (transmission, réception et traitement) de ce type de données nécessitent beaucoup de temps. Ainsi, si la taille des paquets de données est trop grande ou le nombre de transmissions est élevé, cela va causer un problème de trafic au niveau du réseau.

4. Perturbation technologique et M2M fragmenté : Les systèmes intelligents ne sont pas correctement compatibles avec l'infrastructure IoT en créant des problèmes pour les fournisseurs de services réseau. Notamment la nouvelle technologie de la communication multimédia IoMT, avec ces nouveaux atouts, il n'est pas possible de la mettre en oeuvre de manière efficace.

5. Normes communes : Afin de faciliter la communication entre les dispositifs IoMT hétérogènes, il est nécessaire qu'ils fonctionnent selon certaines normes communes qui ne sont pas encore disponibles. Ainsi, les interfaces de programmes d'application bien documentées doivent être lancées par les fournisseurs de services réseau afin que les utilisateurs puissent bénéficier des avantages des normes ouvertes.

TABLE 1.1 – Applications de la communication multimédia dans l'IoT

Différentes applications		Méthodologie proposée
E-Health	Surveillance de la santé à l'aide du multimédia	Architecture multimédia de santé personnelle [99] Architecture de communication M2M pour les appareils portables E-Health [100] Réseau 5G à petites cellules pour ambulance intelligente [101] Assistant de chirurgie robotique [102]
Surveillance de l'habitat	Authentification biométrique	Internet des objets biométriques [103] Authentification biométrique pour I'IoT [104]
	Biométrie vocale	Biométrie vocale [105] Sécurité de l'interface utilisateur vocale [106] H-IoT sécurisé [107]
	Système de surveillance	Système de surveillance M-IoT basé sur une caméra Pi [108] VIPS pour le système de surveillance M-IoT [109] MVSS sécurisé dans M-IoT [110]
Industrie intelligente	Surveillance industrielle IoMT	Inspection automatique des billettes en acier à base de profondeur de vision [111] Inspection de billettes d'acier basée sur la modélisation 3D [112] Surveillance des conditions pour l'industrie pétrolière [113]
	Musée intelligent basé sur le traitement d'images	L'industrie intelligente des musées avec M-IoT [114] Musée intelligent utilisant la diffusion de contenu basée sur Beacon [115] Application de M-IoT pour les robots de transport en entrepôt automatisé [116]
	L'IoMT dans l'agriculture intelligente	Surveillance des cultures agricoles basée sur M-IoT [117] Application de reconnaissance alimentaire de M-IoT [118] Reconnaissance de la fraîcheur des aliments à l'aide du traitement d'image dans M-IoT [119]
Systèmes de Gestion des Routes	Surveillance du trafic	Traitement des images basé sur le contexte et axé sur l'ontologie [120] Traitement cloud pour la surveillance du trafic multimédia mobile [121]
	Détection de trajectoire multimédia	Détection de bosses [122] Surveillance des véhicules basée sur Android IoT [123]
	Authentification multimédia et détection de crime	Taxi autonome pour Smart City [124] Péage basé sur l'IoT [125]

Ces défis ont créé un rythme de recherche accéléré dans le domaine de l'IoMT.

1.8.3 Non adaptation de quelques protocoles de communication d'IoT pour l'IoMT

Nous résumons les différentes causes qui peuvent en rendre un protocole dédié aux réseaux IoT non adapté pour un réseau IoMT :

- Le contenu multimédia acquis à partir de l'environnement IoMT physique possède des caractéristiques distinctes et des mécanismes de communication différentes par rapport aux données scalaires acquises par des dispositifs IoT typiques.
- Les dispositifs multimédias exigent des ressources de traitement et de mémoire plus élevées afin de traiter les données multimédias acquises.
- La transmission multimédia est très gourmande en terme bande passante en comparaison avec le trafic de données scalaires dans l'IoT.
- La livraison de données multimédias exige à satisfaire une certaine QoS par rapport à une transmission scalaire.

Cependant, les activités actuelles de recherche et de développement se sont orientées plus envers les systèmes IoT basés sur des données scalaires en ignorant les défis liés à une communication multimédia. Cela peut produire un manque d'avantage de services et d'applications basés sur les informations multimédias essentiellement fournies par l'IoMT.

Qu'est ce qui est infaisable dans le routage IoT et empêchera son fonctionnement dans l'IoMT ?

Le protocole de routage RPL dans la pile de communication IoT actuelle est flexible et adaptatif pour fonctionner de manière économe en énergie conformément aux exigences de l'application. Les implémentations RPL pour la communication de données scalaires ne sont pas réalisables pour l'IoMT car :

- Le trafic multimédia (audio, vidéo ou audio + vidéo) s'impose avec plus de contraintes et d'exigences strictes de QoS en termes de bande passante, de délai, de gigue, de taux de perte de paquets. . .etc.
- Les métriques de routage proposées pour la sélection des chemins de routage sont basées sur la qualité de la liaison, l'énergie ou la longueur du chemin. Ce qui n'est pas envisageable pour un routage efficace d'un trafic multimédia pour des limites et des exigences de QoS spécifiques.
- Le protocole de routage RPL standard ne prend pas en considération l'équilibrage de charge entre les différents chemins de routage, ainsi, il ne commute pas de chemins lors d'une de surcharge de données ' évènement qui peut se produire dans le cas d'un flux multimédia'.

Jusqu'à présent, très peu d'optimisation a été faite pour que RPL prenne en charge la communication multimédia.

1.9 Comparaison entre les paradigmes IoT et IoMT

Comme dit le proverbe, "une image vaut mille mots", les données multimédias fournissent des informations très complètes qui peuvent être adéquatement normalisées dans des formats, des modèles et une description sémantique appropriés en fonction du contexte de l'application pour en faire une information utile.

Les applications basées sur l'IoMT nécessitent des exigences de QoS strictes afin de fournir une expérience satisfaisante des différents utilisateurs. Certaines applications multimédias peuvent être tolérantes aux pertes et d'autres encore peuvent nécessiter une communication sensible aux délais. De plus, la capacité de bande passante des systèmes IoT est généralement faible car les éléments devraient fournir des mesures scalaires sur l'environnement surveillé ou recevoir de petits paquets de commandes. Différemment, dans l'IoMT, la quantité de données générées peut varier de quelques Kbps à plusieurs Mbps, de sorte que les systèmes concernés doivent s'adapter à la bande passante offerte. En résumé, le tableau 1.2 répertorie une comparaison des caractéristiques similaires et distinctives entre les deux paradigmes IoT et IoMT.

Table 1.2 – Différents paramètres de comparaison entre les paradigmes IoT et IoMT

Paramètres	***IoT***	***IoMT***
Taille des données	non volumineuse	très volumineuse
QoS du multimédia	indisponible	disponible
Connectivité IP	adressable uniquement	adressable uniquement
Capacité de bande passante	faible	élevée
Ressource de mémoire	élevée	très élevée
Puissance de calcul	élevée	très élevée
Sensibilité au délai	indisponible	disponible
Consommation d'énergie	faible	élevée
Équité des protocoles MAC	faible	élevée
Topologie	ad hoc et dynamique	ad hoc et dynamique
Évolutivité	élevée	élevée
Ressources et capacités des noeuds	hétérogénéité limitée	hétérogénéité
Portée des applications	dynamique et flexible	dynamique et flexible

1.10 Conclusion

Dans ce chapitre, nous avons fourni une vue historique sur les précurseurs de l'Internet des Objets qui repose sur les deux technologies : les RCSFs et RFID. Ainsi, nous avons défini une terminologie clé dans l'IoT qui est les réseaux LLNs. Ensuite, nous avons exposé plusieurs définitions pour l'écosystème IoT, ainsi que les différentes applications potentielles de l'IoT. De plus, ce chapitre a discuté le contexte essentiel pour faciliter la compréhension des problèmes de recherche au sein de cette thèse, notamment le processus évolutif de la pile protocolaire d'IoT. Nous avons également défini un aperçu des protocoles hébergés dans cette pile standardisée IoT. De plus, nous avons donné un bref aperçu sur les mesures de performance du système d'exploitation d'IoT, représenté par Contiki et

ses installations de communication, en surlignant les caractéristiques d'économie d'énergie dans Contiki. Nous avons également présenté une définition sur le paradigme d'IoMT ainsi que ses domaines d'applications. A la fin du chapitre, nous avons fourni une interrogation sur ce qui est infaisable dans le routage IoT et empêchera son fonctionnement dans l'IoMT.

Dans le chapitre suivant, nous examinons une gamme de protocoles de routage existants dans l'IoT. Ainsi, nous focalisons notre intérêt de recherche sur le protocole RPL en révélant une revue enrichie de la littérature sur les différentes extensions appris par ce protocole. Cette étude nous a permis de proposer de nouvelles solutions de routage pour les IoMT qui seront présentées dans les prochains chapitres.

Chapitre 2

État de l'art sur les protocoles de routage dans l'IoT

Chapitre 2

État de l'art sur les protocoles de routage dans l'IoT

2.1 Introduction

Le routage des données depuis une source vers une destination est un processus fondamental dans chaque réseau. Dans l'IoT, les dispositifs de communication fonctionnent avec des normes de réseau différentes, pouvant rencontrer une connectivité irrégulière entre eux et beaucoup d'entre eux se caractérisent par une limitation de ressources en posant plusieurs défis et problèmes de routage [126]. Pour cette raison, certaines études ont proposé de concevoir un protocole de routage intelligent. Selon les auteurs dans [127], un protocole de routage intelligent devrait être en mesure de sélectionner les informations les plus appropriées selon les besoins et de les utiliser pour obtenir une transmission de données fiable dans un environnement hétérogène multi-utilisateurs tel que l'écosystème IoT.

Plusieurs facteurs peuvent affecter le processus de routage dans l'IoT, par exemple : l'hétérogénéité des dispositifs, les contraintes de ressources, une connectivité constante ou intermittente entre les dispositifs, le changement fréquent de la topologie du réseau en présence des dispositifs mobiles, etc ... Par conséquent, le routage dans l'IoT devrait être optimisé en particulier en termes d'efficacité énergétique, i.e. un protocole de routage optimisé devrait sélectionner intelligemment les noeuds qui ont des ressources énergétiques suffisantes. En plus, la minimisation des délais d'acheminement de données est essentielle dans le routage, en particulier dans l'IoT où la génération de données est énorme. En résumé, un protocole de routage dans l'IoT doit être efficace, évolutif, adaptable à différents scénarios et capable de trouver des chemins optimaux.

Dans ce chapitre, nous étudions une gamme de protocoles de routage existants dans IoT. De plus, une connaissance du contexte du protocole RPL et des différentes métriques sont présentées. Puis, ce chapitre se termine par une revue de la littérature des améliorations du protocole RPL en discutant les lacunes trouvées dans le protocole RPL, qui ont par conséquent initié l'objectif de nos contributions.

FIGURE 2.1 – Classification des protocoles de routage dans l'IoT

2.2 Classification des protocoles de routage dans l'IoT

De nombreux protocoles de routage ont été proposés dans l'environnement d'IoT et chacun d'entre d'eux a sa propre technique de routage des données. Le déploiement de ces protocoles dépend des caractéristiques de différentes applications, notamment de leurs objectifs et des exigences de QoS. La Figure 2.1 illustre notre classification proposée des différents protocoles de routage utilisés dans l'écosystème IoT.

Bien qu'il existe de nombreux protocoles de routage pour l'IoT, nous pouvons classer ces protocoles en trois grandes familles :

2.2.1 Protocoles basés sur la topologie

a) Routage Plat

Cette classe de protocoles est appliquée dans une structure de réseau plate, où les noeuds ont une importance et des rôles similaires dans le réseau. Le routage à base plat se caractérise par sa simplicité de construction des chemins. Par conséquent, il représente en fait une solution appropriée pour de nombreuses solutions IoT homogènes en raison de leur faible complexité opérationnelle. Généralement, le processus de routage est divisé en deux phases : phase de découverte des chemins et phase de maintenance de ces chemins.

Plusieurs études ont été basées sur ce type d'architecture pour les protocoles de routage dans les applications RCSF/IoT, par exemple parmi les protocoles de routage qui ont été évalués dans cette classe nous citons :

- **An Improved AOMDV Routing Protocol for Internet of Things (AOMDV-IoT) [128]**
  AOMDV-IoT est un protocole de routage proactif, de vecteur de distance à chemins multiples pour IoT. Ce protocole vise à trouver et à créer efficacement une connexion entre les noeuds et Internet. Certaines améliorations ont été apportées par ce protocole notamment : une table de connexion internet (Internet Connexion Table (ICT)) et une adresse de liaison Internet (Internet Linking Address (ILA)) comme adresse IP. En outre, la table de routage et la table ICT sont affectées à chaque noeud ce qui peut consommer plus d'espace mémoire au niveau de chaque noeud.

  Lorsque le noeud vise à créer un lien vers Internet, son adresse IP de destination est attribuée à ILA. Ensuite, il cherche un noeud approprié connecté à Internet dans sa table ICT. Si plusieurs noeuds sont trouvés, le noeud qui sera choisi est celui dont le nombre de sauts est le plus petit et l'ILA sera modifié sur la base de l'adresse IP du noeud de destination. Par contre si aucun noeud n'est trouvé, le noeud source diffuse un message "Route REQuest packet (RREQ)" pour actualiser à la fois le routage et les tables ICT.

  AOMDV-IoT est basé sur quatre types de messages lors de son processus de routage :

  – RREQ : un paquet diffusé par le noeud source afin de chercher un noeud connecté à Internet.
  – Route REply packet (RREP) : un paquet de réponse envoyé depuis la destination vers la source. Ce paquet comprend les informations de connexion Internet (comme le message ACK).
  – Route ERRor packet (RERR) : un message d'avertissement envoyé par les voisins du noeud inaccessible afin d'avertir les autres noeuds en cas d'inaccessibilité ou de défaillance de la connexion Internet.
  – Hello : Un message périodique utilisé pour la maintenance des tables de routage.

  AOMDV-IoT a montré certaines performances par rapport au protocole AOMDV traditionnel en termes de taux de paquets délivrés et de délai moyen de bout en bout. En revanche, il présente certains inconvénients qui peuvent l'exclure d'être un protocole de routage candidat pour des applications IoT comme :

  - Absence de mécanisme de sécurité lors du routage des données.
  - Cet algorithme de routage ne prend pas en compte l'efficacité énergétique des noeuds dans son processus de routage, il est basé uniquement sur un nombre de sauts minimal.
  - Absence de services d'informations contextuelles optimisant le protocole de routage.

- **Dynamic Source Routing Protocol (DSR)** [129]
  DSR est communément classé avec les protocoles réactifs, ce qui signifie que les routes sont connues avant le routage des données. Plus précisément, DSR donne une liste qui contient tous les sauts qui doivent être suivis pour atteindre sa destination. Cette liste est ajoutée dans l'en-tête du paquet de données étant donné que le noeud destinataire est connu. Afin de pouvoir connaître ce noeud destinataire, le protocole DSR vérifie les chemins mis en cache et au cas où la destination ne serait pas trouvée, une recherche de chemin sera lancée. La recherche de routes commence à l'aide des paquets RREQ où le paquet RREQ a une adresse d'expéditeur et de destination, ce qui permet aux noeuds intermédiaires de vérifier l'adresse désignée et de vérifier si le chemin est connu. Si l'adresse est inconnue, le noeud intermédiaire attache son adresse à l'enregistrement du chemin et l'envoie aux noeuds suivants. Le problème de boucle de routage est évité par le fait qu'un noeud rejette la demande qu'il a récemment reçue depuis le chemin au cas où le même initiateur aurait enregistré l'adresse du noeud récepteur. La maintenance des routes est effectuée à l'aide de paquets d'erreur de route (RERR) et d'acquittements. Lorsque l'émission est envoyée, le noeud attend un accusé de réception, au cas où une erreur se produirait et qu'un certain accusé de réception ne serait pas renvoyé, une demande d'accusé de réception est envoyée. Après une pause, une erreur de route RERR est produite et envoyée à l'initiateur des paquets. L'entretien et la découverte du chemin sont un processus difficile pour DSR et il serait conseillé d'avoir une communication plus rapide.

- **Multipath-Enhanced Lightweight On-demand Ad hoc Distance-vector Routing Protocol –Next Generation (LOADng)** [130]
  LOADng est un protocole de routage proactif conçu pour les réseaux à ressources limitées. Le protocole standard LOADng diffuse une demande de route RREQ qui initie le processus de découverte de route. Chaque noeud recevant ce RREQ met à jour sa propre table de routage en fonction du numéro de séquence du paquet, générant une route inverse vers la source en retransmettant le message RREQ. Le message de réponse de route (RREP) ne sera généré que par le noeud de destination prévu. Le message RREP sera ensuite envoyé en unicast au prochain saut vers le noeud source, ce qui générera un chemin vers la destination. Le noeud enverra un accusé de réception de réponse du chemin RREP-ACK à partir duquel il recevra le message RREP. Les liaisons ont un taux d'échec de liaison élevé. En cas d'échec d'un lien, une nouvelle découverte du chemin doit être lancée. La découverte du chemin est créée sur un débit substantiel dans le réseau lorsque les messages RREQ sont inondés. Le routage à trajets multiples augmente la possibilité de trouver un chemin alternatif et réduit ainsi le besoin de sélectionner fréquemment des routes.

Le protocole Multipath-Enhanced LOADng propose trois schémas différents pour identifier p chemins multiples entre une source et une destination données.

Dans l'un de ces schémas, afin d'établir p chemins multiples entre une paire de noeuds (source et destination), la source génére p messages 'RREQ' indépendants avec des numéros de séquence incrémentés. Le noeud intermédiaire recevant RREQ mettra à jour la route vers la destination dans sa table de routage. La destination ne répondra avec un paquet RREP qu'au premier RREQ reçu avec un numéro de séquence donné. Les noeuds intermédiaires envoient le message RREP à la source en unicast, puis ils ne participeront pas à la découverte des routes suivantes. Les exemplaires suivants des messages RREQ seront rejetés. Lors de la réception du message RREP, le noeud source diffusera un nouveau RREQ avec un nouveau numéro de séquence, conduisant à la formation du chemin suivant entre le noeud source et le noeud destinataire. Ainsi, tous les chemins (p) seront des trajets multiples à noeuds disjoints.

b) Routage hiérarchique

L'idée principale du routage hiérarchique est que le réseau est divisé en clusters et chaque cluster est représenté par un Cluster Head (CH) (le noeud maître dans le cluster est appelé CH). Le CH est sélectionné selon divers critères tels que le niveau d'énergie, la qualité du lien et l'emplacement. Contrairement à la classe routage plat, des efforts particuliers sont faits pour organiser le réseau en traitant les noeuds différemment selon leur niveau d'énergie. Dans chaque cluster, chaque noeud envoie les données captées à son CH correspondant. Un CH peut seulement relayer la donnée collectée par ses noeuds membres comme il peut agréger l'ensemble des données reçues en un seul paquet et il le transmet à la station de base. En d'autres termes, les noeuds à faible énergie collectent les données et ceux qui possèdent une énergie plus élevée traitent ces données et les transmettent.

Afin de faciliter l'équilibrage de charge, les CHs se pivotent autour des noeuds du réseau [131]. LEACH [132] est un exemple de protocole de routage hiérarchique dans le contexte de l'IoT [131].

La classe du routage hiérarchique est divisée en deux sous-classes :

1. Protocoles basés sur les arbres : Dans cette sous-classe, les noeuds d'une topologie d'arbre partagent la même destination spécifique pour le routage des données en créant un modèle de trafic de plusieurs à un (many-to-one).

2. Protocoles basés sur les clusters : Dans cette sous-classe, les noeuds sont regroupés en clusters et chaque noeud de la hiérarchie joue un rôle différent. Le principal inconvénient de ce type de protocoles est qu'il nécessite plus de temps pour la formation de clusters en générant un délai et une complexité supplémentaires, ce qui n'est pas adapté à de nombreuses applications IoT.

Ainsi, d'autres protocoles peuvent exister dans cette même classe de routage, tels que :

- **Cluster HeadEfficient Tree-based Self-organizing Protocol (ETSP)) [133]** Dans le protocole ETSP, les noeuds du réseau sont classés en trois types : noeud

racine, noeud récepteur et noeud capteur. Au début du processus du protocole ETSP, il n'y a qu'un noeud racine dont le saut est nul. Ensuite, ce même noeud recherche les noeuds fils en envoyant des paquets de diffusion. Après avoir reçu ces paquets, les noeuds voisins enregistrent les informations de topologie et utilisent différentes métriques telles que le nombre de noeuds fils, le nombre de sauts, la distance de communication et l'énergie résiduelle pour atteindre le poids des noeuds récepteurs disponibles. Ensuite, le noeud avec le poids maximum est sélectionné comme noeud récepteur.

Le modèle de graphe géométrique aléatoire basé sur le modèle Log-normal shadowing radio est supposé dériver les caractéristiques de base du réseau. Dans tous les cas, le réseau peut être considéré comme un graphe aléatoire géométrique avec les noeuds du réseau comme les sommets du graphe et la présence de liens de communication entre deux nœuds quelconques formant les bords du réseau. Dans un graphe géométrique aléatoire, les noeuds sont uniformément répartis sur une zone géographique et l'existence d'un lien entre deux noeuds est indépendante de tout autre lien du réseau. Ce protocole a besoin plus de temps de transmission et consomme plus d'énergie pour sa mise en oeuvre.

- **A Hierarchical Clustered based on modified Dynamic Source Routing (HCDSR)** [134]
  HCDSR est un protocole de routage tolérant aux pannes basé sur le protocole DSR modifié, conçu pour les réseaux de capteurs hiérarchisé en clusters pour les applications IoT. Dans HCDSR, un vice cluster-head prend en charge les fonctions du CH en cas de défaillance de son CH correspondant et plusieurs chemins ont été triés sur la base d'une fonction de coût qui prend en compte l'énergie totale dans un chemin et la distance de la source au noeud puits. De plus, HCDSR utilise des seuils d'énergie pour prendre des décisions à propos des CH qui participeraient au processus de routage. L'un des principaux avantages de ce protocole est que le temps moyen de recouvrement de chemin corrompu est petit. Dans ce protocole, les défauts de routage, en particulier la perturbation du chemin, est due à la défaillance des cluster-heads ou des vice cluster heads.

  Globalement, le but de ce protocole est d'augmenter la tolérance aux pannes des différents échanges de données et d'assurer autant que possible la stabilité du service. Cependant, ce protocole n'est pas optimisé en raison de l'augmentation du taux d'échanges des messages de contrôle pour améliorer leurs performances.

c) Routage géographique

Dans ce schéma de routage, chaque noeud est adressé par son emplacement (sa localisation). La force du signal des noeuds à proximité est utilisée pour détecter la distance entre eux et ceux qui sont séparés par une distance suffisante peuvent extraire les coordonnées relatives des noeuds en utilisant les informations échangées.

Dans les protocoles de routage basés sur la localisation, les chemins de routage sont choisis en fonction de la localisation de la destination et des positions de certains noeuds du réseau. Parmi les protocoles géographiques les plus répandus dans l'IoT, nous citons Link Quality based Geographic Routing resilient to location errors (LQGR) [135], geometric

based behavior of GOAFR (GeoRank) [136], Lightweight and Distributed Geographic Multicast Routing Protocol for IoT Applications (LDGM-IoT) [137].

- **Le protocole LQGR [135]**
  LQGR est un protocole de routage géographique qui sélectionne son prochain saut (noeud relais) en fonction de la qualité du lien, de l'erreur de localisation et de la vitesse de ce noeud. Dans ce protocole, chaque noeud rassemble périodiquement les informations sur la qualité du lien avec ses noeuds voisins et la distance entre lui-même et ses voisins. LQGR augmente la stabilité et la précision en réduisant les messages de contrôle inutiles, ainsi, il réduit le temps de décision de routage géographique dans un environnement IoT.

- **Le protocole GeoRank [136]**
  Le protocole GeoRank représente l'intégration du comportement basé sur la géométrie de GOAFR avec le comportement basé sur le rang de RPL. Ce protocole est principalement adapté aux réseaux à grande échelle avec une densité de liaison non uniforme, comme un réseau sans fil pour les noeuds d'éclairage public, où la densité de liaison varie de faible à élevée en fonction de la présence d'obstructions et de bâtiments à différents endroits du réseau. Ainsi, il prend en charge un réseau WSN à grande échelle compatible IPv6 pour diverses applications dans un IoT urbain.

  Le protocole GeoRank dépend de la position géographique pour implémenter la partie géométrique du protocole. Par conséquent, tous les noeuds du réseau doivent être statiques, ce qui favorise également le protocole RPL. Cela ne signifie pas qu'il ne doit y avoir que des noeuds statiques sur le réseau, mais les noeuds mobiles doivent être à un saut d'un noeud statique. Comme le système d'éclairage public et d'autres applications possibles d'un tel réseau sont principalement constitués par des dispositifs statiques, il est possible de stocker la position du noeud pendant le processus d'installation. Cette contrainte selon laquelle les noeuds mobiles doivent être à un saut d'un noeud statique, représente une limitation de ce protocole.

- **Le protocole LDGM-IoT [137]**
  LDGM-IoT est un protocole de routage géographique multicast léger et distribué, qui vise à réduire le nombre de liaisons de transmission dans une arborescence multicast et à raccourcir la distance maximale de nombre de sauts depuis la source vers les destinations. Le schéma de ce protocole contient trois phases, la phase de demande de routes, la phase de mise à jour inverse et la phase de modification. Dans la phase de demande de routes, un noeud source initie une procédure de demande de routes pour trouver des chemins vers des destinations. A partir des informations de localisation des voisins et des destinations, chaque noeud intermédiaire trouve des voisins comme ses prochains sauts afin d'atteindre plusieurs destinations. Lorsqu'un paquet de demande de route atteint une destination, la destination démarre la phase de mise à jour inverse pour confirmer et affiner les chemins de routage construits. Ensuite, après la phase de mise à jour inverse, chaque noeud exécute localement la phase de modification pour vérifier si les noeuds choisis comme sauts suivants peuvent être fusionnés pour enregistrer les liaisons de transmission. Dans ce qui suit, nous donnons plus de détails sur ces phases :

- Dans la phase de demande de routes, les noeuds utilisent localement les règles d'attribution de priorité conçues pour sélectionner le moins de noeuds relais (sauts suivants), qui sont situés plus près des destinations de multidiffusion.
- Dans la phase de mise à jour inverse, un noeud de destination peut éliminer les boucles de routage. Dans cette phase, les noeuds intermédiaires peuvent calculer localement pour réduire les liaisons de transmission dans l'arbre multicast construit. De plus, dans la phase de modification, chaque noeud intermédiaire peut réduire davantage les liaisons de transmission sur la base des règles de routage maintenues et de ses informations de voisinage.

Ce protocole est basé sur le chemin le plus court dans la sélection des liaisons de multidiffusion. Cela va à l'encontre de la nature de l'environnement IoT, qui peut comprendre des liaisons plus longues mais qui a plus d'efficacité que les liaisons les plus courtes.

2.2.2 Protocoles basés sur les contraintes de fonctionnement

a) Routage basé sur le contexte

Les décisions de routage dans cette classe seront prises en fonction du contexte recueilli dans les différentes parties du réseau. Ces protocoles de routage sont appelés "protocoles de routage sensibles au contexte". Le contexte de données est la quantité d'informations collectées depuis l'environnement qui peut être utilisée afin de caractériser la situation du réseau. Les protocoles de routage sensibles au contexte utilisent ces informations pour prendre des décisions de routage. Ces informations sont associées aux noeuds et peuvent contenir l'énergie résiduelle, la mémoire, la puissance de traitement, la position du noeud ou sa vitesse de déplacement. Dans l'IoT, il est important de collecter le contexte de l'environnement pour un routage rapide en génèrant des connaissances qui sont utilisées pour prendre des décisions de routage [138].

Les protocoles existants utilisent principalement l'énergie résiduelle des noeuds comme paramètre de routage basé sur le contexte. D'une autre part la mémoire du noeud, sa puissance de traitement et la qualité de la liaison peuvent être également considérées comme des paramètres de contexte importants [139].

Parmi les avantages de ce type de routage nous citons : l'équilibrage de la charge du réseau, la maximisation de la durée de vie du réseau et la réduction du délai. Parmi les protocoles de routage basés sur le contexte, nous mentionnons Context Awareness in Sea Computing (CASCR) [140], Emergency Response IoT based on Global Information Decision (ERGID) [141], Pruned Adaptive IoT Routing (PAIR) [142], Game Theoretic Approach for Context Based Routing (GT-ACR) [143], Spectrum aware Energy Efficient multi-hop multi-channel routing scheme for D2D communication in IoT (SpEED-IoT) [144], Smart and Self-organised Routing Algorithm (SSRA) [145], et Context-aware Energy Conserving Algorithm for routing (CECA) [146].

- **Le protocole PAIR [142]**
  Ce protocole introduit un modèle qui aide les noeuds intermédiaires (noeuds relais ou routeur) à obtenir des avantages très utiles lorsqu'ils utilisent leurs ressources afin de faire relier les noeuds entre eux pour établir un chemin de routage plus optimisé.

Le modèle proposé par le protocole PAIR est basé sur les paramètres suivants de chaque noeud relais : consommation d'énergie, charge actuelle et espace mémoire, et distance entre le prochain voisin.

Le protocole PAIR fonctionne en deux étapes appelées : "forward" et "backward". Dans l'étape "forward", les messages de configuration sont diffusés depuis la source vers ses voisins qui contiennent le coût collecté depuis la source au noeud courant. Une fois que les noeuds intermédiaires reçoivent ces messages, ils les transmettent à leurs voisins en mettant à jour le coût en fonction de l'ensemble des paramètres caractérisant le noeud (consommation d'énergie, ...etc). Le noeud destinataire envoie l'accusé de réception (ACK) sur le meilleur chemin sélectionné en fonction des valeurs collectées des paramètres de coût à partir du message de configuration.

Si le message d'accusé de réception subit une interruption de son chemin au niveau d'un noeud i, il est converti en message de configuration (appelé *i_setup*). Ensuite il est transmis aux voisins du noeud *i* pour des fins de découverte de routes. Après avoir reçu le message *i_setup*, le chemin actif est établi entre la source et la destination et la transmission des données peut commencer.

Pendant la transmission de données, s'il rencontre une rupture de liaison, soit la transmission des données se fait sur un chemin alternatif, soit en tamponnant les données reçues et des messages *i_setup* sont générés pour découvrir un nouveau chemin vers la destination.

Parmi les avantages du protocole PAIR, nous citons :

i) Il s'agit d'un protocole de routage multi-saut et basé sur le contexte.

ii) Il aide à résoudre le problème de la coopération entre les noeuds dans les réseaux hétérogènes en essayant de donner une certaine incitation aux noeuds relais car ces derniers dépensent leur énergie pour relayer des données qui ne leur procurent aucun avantage.

Cependant, le protocole PAIR présente quelques inconvénients :

i) La sécurité des données n'est pas prise en compte.

ii) La mémoire requise peut être élevée car chaque noeud doit mémoriser les données sur le noeud relais actuel pour trouver un éventuel chemin lorsque la rupture de liaison est observée.

- **Le protocole ERGID** [141]
  ERGID est un protocole de routage pour la réponse d'urgence basé sur la décision globale d'information afin d'améliorer les performances de transmission de données fiables et d'intervention d'urgence dans l'IoT. En d'autre terme, il améliore la capacité de réponse en temps réel du réseau en fournissant une transmission de données avec moins de délais de bout en bout et de perte de paquets, ainsi tout en réduisant la consommation d'énergie. De plus, un choix de probabilité d'énergie résiduelle a été adopté pour équilibrer la charge dans le réseau. En outre, la proposition de ce protocole repose sur deux mécanismes différents. Le premier concerne l'implication de la méthode "Delay Iterative Method (DIM)", qui classe les noeuds d'une route

candidate en fonction d'une estimation du délai. Ce mécanisme est utilisé pour atténuer le problème d'ignorance des chemins valides. En plus, DIM cherche à assurer une communication en temps réel pour les applications d'intervention d'urgence et effectue des mises à jour périodiques dans la table de routage. Le deuxième mécanisme, appelé choix de probabilité d'énergie résiduelle "Residual Energy Probability Choice (REPC)", permet l'utilisation d'informations d'énergie résiduelle pendant le processus de sélection du noeud suivant. Ainsi, grâce à la composition de ces mécanismes, ERGID donne un faible délai de bout en bout (fourni par DIM) et une répartition efficace de la consommation d'énergie (fournie par REPC).

Les auteurs ont développé le protocole de routage "ERGID" pour les réponses d'urgence qui répond à la plupart des exigences de l'IoT mais qui a encore quelques problèmes liés à la perte de paquets et à l'efficacité énergétique lorsqu'il est comparé aux protocoles de routage existants de l'IoT. De plus, ERGID est limité à l'intervention d'urgence dans l'IoT à petite échelle en raison de sa consommation d'énergie et n'est pas axé sur les applications à grande échelle.

- **Le protocole GT-ACR [143]**
  GT-ACR représente un nouveau protocole de routage optimisé qui utilise des informations de contexte combinées à l'approche de la théorie des jeux pour le routage dans l'IoT opportuniste. Dans ce protocole, les informations contextuelles des noeuds sont utilisées pour établir une combinaison stable de contextes à travers l'analyse et la transformation de la théorie des jeux. GT-ACR réalise la sélection du prochain saut par le résultat d'un jeu coopératif à somme non nulle, établissant la stratégie de routage en utilisant l'équilibre de Nash appliqué aux paramètres suivants ; les rencontres entre les noeuds et la distance entre un noeud et la destination du message. En effet, ce protocole est plus performant en termes de réduction du nombre de sauts, de perte de messages et de surcharge.

  En outre, GT-ACR est basé sur l'identification des attributs les plus significatifs d'un noeud, à savoir la valeur de réunion d'un noeud et la distance d'un noeud vers sa destination prédéfinie. Le contexte des paramètres du noeud pris en compte sont : la probabilité de rencontre, la valeur d'énergie résiduelle, le poids de transmission et l'occupation de l'espace. Ces paramètres sont prédits à l'aide de filtres de Kalman où le jeu non coopératif des deux joueurs est conçu à partir de ces paramètres, puis utilisé pour décider de la transmission des données entre deux nœuds. Cependant, les coûts de calcul pourraient augmenter en raison de la charge de travail accrue de l'utilisation des filtres de Kalman.

b) Routage basé sur l'occurrence d'événements

Dans les protocoles événementiels, le routage des données est lancé une fois que le capteur détecte un événement pertinent [147]. Certaines applications IoT nécessitent un routage basé sur des événements en temps réel, ce qui représente un issu fréquent dans les préoccupations liées à l'IoT.

L'idée du routage basé sur les événements est de permettre à un ensemble de dispositifs de spécifier des intérêts dans certaines conditions d'événements. Si un événement a été déclenché, les abonnés (subscribers) intéressés par cet événement seront avertis [148].

Des exemples de protocoles appartenant à cette classe de routage : REL (Routing by Energy and Link quality) [149], MBPP (Multiple Base station and Packet Priority based clustering Scheme) [150], ainsi que le protocole EECBR (Energy Efficient Content Based Routing) [148].

- **Le protocole EECBR [148]**
  Ce protocole utilise le concept de routage basé sur événement qui est effectué de manière distribuée via des règles simples. Une caractéristique fondamentale de ce protocole réside dans l'efficacité énergétique de ce dernier, qui s'obtient grâce à la construction d'une topologie virtuelle en équilibrant la charge énergétique entre les dispositifs IoT, ainsi, qu'en raison de la propriété d'auto-organisation de la hiérarchie obtenue. L'idée principale de ce protocole est d'utiliser le modèle de communication "publish/subcribe" qui fournit une possibilité d'enregistrer des capteurs dépendants aux événements intéressés. Lors de l'apparition d'un événement, les capteurs dépendants sont notifiés et la topologie virtuelle est utilisée pour relayer les événements des publishers vers les capteurs intéressés.

  EECBR est un protocole simple qui traite le problème du routage à base d'événements dans l'IoT d'une manière économe en énergie en équilibrant la consommation d'énergie des dispositifs IoT. Ce protocole ne possède pas d'autres performances que l'optimisation énergétique.

- **Le protocole REL [149]**
  Ce est basé sur l'optimisation du mécanisme de sélection du chemin tout en utilisant des mécanismes d'estimation de la qualité de la liaison, de l'évaluation de l'énergie, du nombre de sauts et de l'équilibrage de charge, ce qui augmente la fiabilité du système et empêche la mort prématurée des noeuds. REL utilise trois métriques : l'énergie résiduelle, la qualité de la liaison basée sur des liaisons faibles et le nombre de sauts pour minimiser les chemins longs et inefficaces. Pour le processus de sélection de route, il existe deux valeurs de seuil : le premier seuil est utilisé dans la technique d'équilibrage de charge et la recherche de route. Le deuxième seuil est calculé la différence maximale de sauts par rapport à la route actuelle.

  Le protocole REL présente de nombreux inconvénients car il est principalement conçu pour WSN qui ne peut être considéré comme une partie de l'environnement IoT. En outre, il fournit une évaluation approfondie de l'énergie des noeuds, qui est une métrique importante pour les WSN mais pas suffisante pour l'IoT. De plus, la métrique de rapport de livraison de paquets n'est que relativement mesurée par le nombre de noeuds au lieu d'être mesurée par le temps. Ainsi, les résultats de l'évaluation du protocole ne sont pas précis. REL sélectionne un chemin avec une bonne qualité de liaison et une consommation d'énergie efficace, mais présente l'inconvénient de moins de probabilité de succès de routage et de délai d'établissement du chemin. Ce protocole s'applique uniquement aux environnements statiques.

- **Le protocole MBPP [150]**
  Dans le protocole MBPP, une fois les clusters sont formés, les CHs sélectionnent les dispositifs IoT actifs (Active IoT Device (AID)) parmi tous les dispositifs IoT membres d'un cluster. Les AID sont sélectionnés de manière à fournir la couverture réseau de l'ensemble des clusters. Les AID stockent les données détectées dans leurs

files d'attente et planifient leur transmission à leur CH correspondant dans leurs intervalles de temps alloués en fonction de l'abonnement et de la priorité des données. Chaque paquet de données se verra attribuer un numéro de priorité. Le paquet avec la priorité la plus élevée sera transmis en premier. Par exemple, les données d'urgence en temps réel devraient avoir la priorité la plus élevée pour être transmises. Si un tel paquet de données d'urgence en temps réel n'est pas disponible dans la file d'attente prête d'un AID, ce dernier transmet des données en temps non réel. Ainsi, chaque AID transmet soit le paquet de données soit un paquet spécial au CH dans son intervalle de temps en utilisant un schéma d'accès multiple par répartition dans le temps (TDMA). Le paquet spécial est de très petite taille juste pour informer le CH que le noeud est toujours en vie au cas où le noeud n'aurait pas de paquet de données à envoyer. Si le CH ne reçoit aucune donnée ou un paquet spécial d'un appareil IoT dans son intervalle de temps, il y a une forte probabilité que l'appareil IoT soit en panne. Cependant, le CH exclut le dispositif IoT de son intervalle de temps et de son cluster uniquement s'il ne reçoit aucune donnée ou paquet spécial pour un certain nombre d'intervalles de temps (détection de panne). La taille du paquet spécial est beaucoup plus petite que celle de l'événement ou des données envoyées. Par conséquent, l'envoi d'un paquet spécial consomme moins d'énergie par rapport à celui d'un paquet de données. À la fin d'un tour, un CH agrège les paquets de données reçus depuis tous les appareils IoT actifs (AID) pour éliminer la transmission de données redondantes et réduire la consommation d'énergie. Chaque CH est à nouveau lié à une station de base en fonction de la distance euclidienne (un CH est lié à la station de base la plus courte). Ainsi, une fois qu'un CH a agrégé des données, il transmet des données à la station de base à laquelle il est connecté. La station de base transmet des données au serveur central via Internet en utilisant un réseau de communication sans fil à grande portée (si nécessaire).

Les données en temps réel et d'urgence auront la priorité la plus élevée. Cependant, les données de priorité inférieure peuvent être interrompues si elles ne peuvent pas être transmises pendant une longue période de temps lors de l'arrivée de données de priorité plus élevée.

c) Routage basé sur l'énergie

Afin de prolonger la durée de vie du réseau, plusieurs protocoles de routage basé sur l'économie de l'énergie ont été proposés pour les applications IoT.

L'efficacité énergétique des noeuds est le facteur clé qui affecte les performances dans les réseaux distribués pour l'IoT [151]. Les protocoles basés sur cette classe acheminent les données dans le réseau en fonction du niveau d'énergie des noeuds. Ces derniers sont sélectionnés lorsque leurs ressources énergétiques sont élevées ou supérieures à un seuil spécifié, afin de maximiser la durée de vie du réseau. Parmi les protocoles de routage dédiés dans cette classe, nous citons : Reliable and Energy-Efficient Opportunistic Routing protocol (REOR) [152], Node Level Energy Efficiency protocol (NLEE) [153], Enhanced version of the Channel-Aware Routing Protocol (CARP) (E-CARP) [154], Energy Efficient Link Stable Routing (EELSR) [155], Optimal Secured Energy Aware Protocol (OSEAP) [156], Scalable Energy Efficient-M2M (SEE-M2M) [157], An Energy Aware Coded Opportunistic Routing (ECOR) [158], Energy Efficient Probabilistic Routing algorithm (EEPR) [151].

- **Le protocole EEPR [151]**
  EEPR est un protocole qui contrôle la diffusion des paquets de demande de routes de manière stochastique afin d'augmenter la durée de vie du réseau. EEPR suit le contexte de celui du protocole AODV dans le principe de transmission des messages "RREQ" mais selon des restrictions afin de réduire le taux de perte de paquets ainsi que la congestion du réseau.

  Ce protocole utilise, comme métriques de routage, à la fois la métrique *ETX* et l'énergie résiduelle de chaque noeud. En utilisant la métrique *ETX*, EEPR compose le chemin de routage avec une bonne qualité de liaison. En outre, l'utilisation de l'énergie résiduelle permet d'augmenter la durée de vie du réseau. De plus, EEPR contrôle la surcharge causée par le nombre de paquets "RREQ" et génère des chemins de routage économes en énergie.

  Dans le fonctionnement du protocole EEPR, lorsqu'un noeud source souhaite transférer des données vers un noeud destinataire, il diffuse un message de demande de route vers ses noeuds voisins à un saut. Un noeud voisin intermédiaire qui n'est pas le noeud destinataire ou qui n'a aucune information de route valide vers la destination calcule la probabilité de transmission en utilisant son énergie résiduelle et sa valeur *ETX*. Si la valeur de probabilité estimée est suffisamment élevée, le noeud intermédiaire retransmet le message de demande de route. Le noeud source reçoit des messages de réponse de route "RREP" et sélectionne un chemin pour le transfert des données.

  Les inconvénients du protocole EEPR sont :

  – Dans EEPR, le durée pour établir les chemins est légèrement plus longue et une probabilité de réussite de routage est légèrement inférieure.
  – EEPR est susceptible à toutes les formes d'attaques.

- **Le protocole NLEE [153]**
  Dans [153], les auteurs ont proposé le protocole NLEE pour améliorer l'efficacité énergétique de l'IoT. Le protocole NLEE prend en compte l'énergie résiduelle de ses noeuds voisins à un saut et la valeur moyenne de l'énergie résiduelle de tous les noeuds du réseau. Pour cette raison, deux facteurs sont considérés : chaque noeud connaît la valeur moyenne de l'énergie résiduelle de tous les noeuds du réseau calculée par le contrôleur de réseau en utilisant périodiquement des informations sur l'énergie résiduelle de chaque noeud. Deuxièmement, chaque noeud connaît l'énergie résiduelle de ses noeuds voisins à un saut à partir des paquets Hello qui sont périodiquement diffusés afin d'indiquer l'existence et l'emplacement du saut du noeud par rapport à la source et à la destination. Lorsqu'un noeud source a besoin d'un chemin de routage pour transmettre les paquets, il diffuse le paquet de demande de route "RREQ" à son voisinage à 1 saut pour calculer les sauts depuis la source vers la destination. Ensuite, lorsqu'un noeud reçoit le paquet RREQ, il calcule la probabilité de transmission en utilisant son énergie résiduelle et la valeur du nombre de transmissions attendues.

  Ce schéma de routage permet de maintenir une meilleure conservation de l'énergie grâce à l'utilisation efficace de l'énergie des noeuds. Il fournit également le chemin

le plus court du réseau entre la source et la destination tout en augmentant le délai de configuration du routage. Cependant, la probabilité de réussite du routage est diminuée.

- **Le protocole OSEAP [156]**
  Dans [156], une nouvelle méthode qui associe le protocole OSEAP et l'algorithme IBFO (Improved Bacterial Foraging Optimization) pour un routage sécurisé et économe en énergie a été proposée. Dans OSEAP, tous les noeuds de la topologie du réseau IoT sont regroupés à l'aide d'un algorithme de clustering Fuzzy C-Means (FCM).

  La topologie virtuelle basée sur la topologie du réseau est industrialisée et englobe un ensemble de noeuds de capteurs. Après la mise en clusters des noeuds, les CHs sont sélectionnés. Pour diminuer successivement la consommation d'énergie d'un groupe de capteurs concernés par un événement précis, OSEAP gère avec une grande efficacité l'ordonnancement de l'activité des capteurs. En outre, afin de garantir un protocole sensible à l'énergie, le protocole OSEAP utilise la procédure de distribution de clé de groupe basée sur une consommation d'énergie minimale. La clé sera changée arbitrairement afin d'éliminer les attaques. À ce stade, la clé optimale sera désignée à l'aide de l'algorithme IBFO. Cependant, l'algorithme FCM ne convient pas pour le clustering de noeuds parce que, dans FCM, les noeuds sont regroupés en fonction de leur importance, mais en réalité, les noeuds doivent être regroupés en fonction de leur distance par rapport aux autres noeuds. En outre, l'algorithme IBFO entraîne une charge de calcul supplémentaire sur le processus d'établissement de la route lorsque le noeud source veut envoyer des informations aux noeuds de destination. Dans OSEAP, il n'y a pas de discussion sur la stratégie de sélection des noeuds, i.e. il n'y a pas de mécanisme qui mesure le degré de confiance des noeuds.

d) Routage basé sur la QoS

Les applications d'IoT ont des exigences de QoS différentes, et plusieurs problèmes restent en suspens afin d'améliorer certains protocoles de routage compte tenu des contraintes des dispositifs.

Les protocoles de routage basés sur la QoS sont capables de fournir différents niveaux de QoS en fonction des décisions de routage et des métriques de QoS. Les auteurs dans [159] ont surligné l'idée suivante : la QoS est importante mais la consommation d'énergie doit être prise en considération. C'est le cas de certains protocoles qui prennent en compte la QoS et les contraintes énergétiques dans leur processus de routage. À titre d'exemple de ce type de protocoles nous citons : centralized MultiPAth QoS-driven Routing protocol (MPAR) [160], Effective energy Harvesting Aware Routing Algorithm (EHARA) [161] et RPL [162]. Nous présentons le protocole RPL [62] avec plus de détails dans la section 2.3.

- **Le protocole MPAR [160]**
  MPAR est un protocole de routage de QoS centralisé et multi-chemin pour les réseaux sans fil industriels. MPAR a été conçu pour identifier les routes redondantes qui doivent être établies entre tous les noeuds source et de destination afin de satisfaire les exigences de fiabilité et de délai de bout en bout exigées par les applications industrielles. À cette fin, MPAR utilise les informations collectées par le gestionnaire

de réseau pour estimer la fiabilité de bout en bout et les performances de délai des routes à sauts multiples. En d'autres termes, MPAR identifie les routes redondantes (nombre de routes redondantes et l'identité des noeuds appartenant à chaque route) nécessaires pour satisfaire les exigences de QoS exigées par l'application. Les routes redondantes nécessaires sont identifiées une par une dans un processus itératif jusqu'à ce qu'une route à trajets multiples capable de satisfaire les exigences de qualité de service puisse être identifiée.

MPAR est présenté dans le cadre de la norme WirelessHART compte tenu de son adoption industrielle importante. Cependant, MPAR peut également être adapté à d'autres réseaux sans fil à sauts multiples basés sur l'approche TDMA centralisée. De plus, MPAR utilise l'estimation probabiliste pour les routes en termes de fiabilité et de délai pour reconnaître les noeuds et les routes essentiels pour créer les connexions de bout en bout. Néanmoins, la stabilité des réseaux maillés sans fil est un problème important. L'instabilité de ces réseaux est principalement due aux fluctuations de la qualité des liaisons et aux fréquents battements des routes.

- **Le protocole EHARA [161]**
  Dans [161], les auteurs ont conçu le protocole de routage EHARA. Ce protocole est basé sur le processus de réduction d'énergie et le processus de prédiction d'énergie qui définit les mesures de coût pour sélectionner la meilleure route. Des sources hybrides de récupération d'énergie sont prises en compte dans les travaux proposés, i.e. des panneaux solaires, des véhicules en mouvement et des RF. Le processus de prédiction d'énergie utilise une approche de filtre de Kalman qui prend en compte le pas de temps précédent et les statistiques actuelles pour déterminer une meilleure estimation des arrivées actuelles d'énergie provenant de différentes sources. Le processus de réduction d'énergie est proposé pour prolonger la durée de vie du réseau en mettant en veille les noeuds avec une énergie minimale qui sont incapables d'effectuer des opérations jusqu'à ce que le niveau d'énergie soit récupéré. Le noeud avec le niveau d'énergie le plus élevé et le coût minimal basé sur le chemin le plus court de Dijkstra est sélectionné pour acheminer les données.

  EHARA est un protocole de routage réparti prenant en compte la récupération d'énergie dans les réseaux IoT hétérogènes. Il permet de garantir la QoS du réseau en présence de conditions de disponibilité d'énergie et de charge de trafic variable. En combinant différents algorithmes de récupération d'énergie, le protocole augmente la durée de vie des noeuds et la qualité de service du réseau. Cependant, ce protocole ne traite pas les problèmes de sécurité. En outre, la consommation d'énergie dans différents états des noeuds et la durée de chaque état des noeuds affectent les performances du schéma de routage proposé.

e) Routage basé sur l'intelligence d'essaim

Cette classe est basée sur les lois qui régissent les systèmes biologiques. Les exemples les plus fameux sont les algorithmes d'optimisation des colonies de fourmis (Ant Colony Optimization (ACO)). Ils peuvent également être basés sur d'autres systèmes biologiques tels que le système immunitaire humain et la propagation des épidémies. Cette classe est subdivisée en deux sous-classes : mécanisme immunitaire et bio-inspirée. Dans

la première sous-classe, les mécanismes de routage dépendent sur un système immunitaire. Par exemple, dans le protocole "Improved Particle Swarm Optimization Algorithm (IPSO)" [163], un système de mesure physiologique pour mesurer les signaux physiologiques de l'utilisateur, ainsi qu'un système de surveillance à distance sont mis en place. En outre, dans la même sous-classe nous trouvons le protocole "Improved Efficient and Intelligent Fault-Tolerance Algorithm (IEIFTA)" [164], où la direction de mutation de la particule est déterminée par l'équation d'évolution multi-essaims, et sa diversité est améliorée par le mécanisme immunitaire.

Dans la deuxième sous-classe, les protocoles de routage sont basés sur la modélisation du comportement biologique des insectes qui peut aider à la conception d'algorithmes optimaux afin de résoudre divers problèmes de routage. Comme protocole de routage basé sur les mécanismes bio-inspirés, nous citons : bio-inspired Particle MultiSwarm Optimization (PMSO) [165], Efficient IoT Communications based on Ant System (EICAntS) [166], Energy aware Ant Routing Algorithm (EARA) [167].

- **Le protocole EARA [167]**
  L'objectif principal de ce protocole est d'adapter le processus de routage pour une maximisation de la durée de vie du réseau [167]. Il s'agit d'un algorithme d'intelligence en bio-inspiré. Il prend en compte non seulement les valeurs des phéromones mais également le niveau d'énergie résiduelle des noeuds. Comme l'énergie résiduelle dans les dispositifs IoT change au fil du temps, les auteurs ont introduit le mécanisme de mise à jour des informations énergétiques. Par rapport à l'algorithme de routage des fourmis (ARA), les agents des fourmis d'EARA conservent les informations de deux champs supplémentaires :

  i) L'énergie moyenne des noeuds qui est calculée en fonction du nombre de sauts parcourus par un paquet ;

  ii) Il stocke également la plus faible valeur de l'énergie résiduelle que peut un agent de fourmis la retrouver durant son chemin.

  EARA utilise des agents de fourmis d'énergie périodiques (Periodic Energy Ant agents (PEANT)) pour mettre à jour les valeurs d'énergie dans la table de routage des noeuds. Les PEANT diffusés envers une destination collectent les informations énergétiques sur ce chemin. L'inondation des PEANT peut être une opération coûteuse en termes d'énergie consommée, par conséquent, l'algorithme envoie ces paquets de contrôle occasionnellement. Les noeuds de destination dans EARA y parviennent en gardant une trace de l'énergie résiduelle de leur propre batterie. Si l'énergie résiduelle est modifiée par un seuil configurable, EARA inonde le réseau avec de nouveaux PEANT. L'intervalle de temps de diffusion des PEANT dépend principalement de deux paramètres, à savoir la capacité maximale de la batterie et la valeur du seuil d'énergie préconfigurée.

  Le protocole de routage EARA ne prend pas en compte la sécurité des données. En outre, dans EARA le changement de la valeur seuil d'énergie peut affecter ses performances.

- **Le protocole IPSO [163]**
  IPSO est un algorithme d'optimisation de l'essaim de particules (PSO) pour l'IoT

de soins médicaux sous Android afin d'améliorer la précision de la mesure de la fusion de données physiologiques multi-capteurs dans le système IoT. Dans [163], les auteurs ont présenté une nouvelle méthode pour collecter différentes données des patients dans les hôpitaux à travers des multi-capteurs et les analyser sur la base d'une PSO améliorée dans un environnement de cloud computing. La contribution principale de cet algorithme est d'utiliser une PSO améliorée pour analyser efficacement les données des patients. En plus, il augmente la précision de l'effet radio de mesure pour la fusion des signaux multi-physiologiques (poids corporel, graisse corporelle, pression artérielle, oxygène sanguin, fréquence cardiaque). Le protocole développé peut être utilisé dans les hôpitaux pour collecter des données personnelles afin de surveiller le système d'information sur les soins. En fonction de chaque patient surveillé, une méthode plus simple et plus rapide de fonction d'alerte médicale précoce est contenue, de sorte que les ressources médicales peuvent être utilisées de manière plus appropriée pour éviter le gaspillage. Cependant, IPSO ne traite pas les données (les soins médicaux) en temps réel.

- **Le protocole EICAntS [166]**
  L'algorithme d'optimisation des colonies de fourmis est utilisé pour un routage optimal dans le réseau IoT basé sur un système de fourmis afin d'améliorer le mécanisme de détermination de chemin en utilisant les avantages d'un cadre de province d'insectes. Le protocole EICAntS prend en compte les paramètres suivants pour une sélection efficace des chemins, tels que la mobilité, l'énergie et la longueur du chemin. Ainsi, ce groupe de métriques permet de déterminer la qualité des chemins en termes de longueur de chemin, de consommation d'énergie et de stabilité. Après avoir reçu des paquets du noeud source, le noeud de destination calcule le facteur global, puis le dirige vers le noeud source. Ensuite, le noeud source met à jour la valeur précédente du facteur global dans sa table de routage.

  Ce protocole bio-inspiré définit une métrique d'efficacité globale pour estimer la qualité de la liaison en plus de l'effet énergétique d'un noeud. Les noeuds voisins sont sélectionnés en fonction d'une quantité de phéromones supérieure calculée à l'aide de la métrique d'efficacité globale. Ainsi, le nombre de métriques de mise à jour est élevé à intervalles irréguliers en raison de la longueur de chemin différente. Cependant, cette approche de découverte et de sélection de services repose principalement sur des architectures centralisées. En outre, l'utilisation du paramètre d'énergie par le calcul proposé nécessite une démonstration supplémentaire en considérant les divers composants ayant un impact sur l'utilisation de l'énergie ou de la vitalité. L'impact énergétique ne prend en compte que la classe de données ou d'informations traitées par le noeud.

2.2.3 Routage basé sur la sécurité

Pour prévenir les attaques de routage, plusieurs stratégies de routage sécurisé ont été proposées dans la littérature. Dans cette classe de protocoles, nous présentons un aperçu sur les schémas de routage basés sur la confiance afin de fournir une fonctionnalité de routage sécurisé. Dans le routage sécurisé, la réputation évalue principalement le routage et le transfert, l'utilisation des mécanismes de chiffrement et d'authentification et la bonne

transmission des accusés de réception par paquet transmis [168]. La confiance [169] est le niveau de confiance qu'une entité détient envers les autres. Il s'agit de l'agrégation de toutes les valeurs de réputation que l'entité détient pour un autre participant. Un noeud avec des valeurs de réputation élevées est considéré comme un noeud fiable. Les noeuds légitimes dépendent principalement d'entités fiables pour accomplir les tâches de communication. D'un autre côté, une mauvaise réputation peut révéler des entités égoïstes ou malveillantes, ainsi qu'elle est utilisée pour la détection d'intrusions. Cependant, les noeuds légitimes essaient d'éviter les entités peu recommandables et ne servent pas leur trafic.

Parmi les protocoles de routage basé sur la confiance nous retrouvons : a Trust-Aware Secure Routing Framework (TSRF) [170], Multi-context trust aware routing (MCTAR) [171], Self-Channel Observation Trust and REputation System (SCOTRES) [168], Crow Whale-energy trust routing (CrowWhale-ETR) [172], Secure Anti-Void Energy-Efficient Routing (SAVEERS) [173].

En outre, une sous-classe de la classe principale du routage basé sur la confiance est l'authenticité. Dans cette sous-classe, les dispositifs IoT devraient pouvoir vérifier si certaines entités sont autorisées à accéder à leurs données mesurées. Au niveau du réseau, seuls les dispositifs autorisés devraient pouvoir accéder au réseau IoT. Les dispositifs non autorisés ne devraient pas être en mesure d'acheminer leurs messages sur les dispositifs IoT. Ainsi, le système authentifie les périphériques IoT avant qu'ils ne puissent rejoindre ou créer un nouveau réseau. Cette sous-classe de protocoles se focalise sur l'augmentation de la sécurité des données en empêchant les attaques malveillantes. Parmi les protocoles de routage basé sur cette sous-classe, nous citons le protocole "Secure Multi-Hop Routing Protocol (SMRP)" [174], "Secure and Efficient Protocol for Route Optimization in PMIPv6 based Smart Home IoT (SERO-SH-IoT)" [175], "Lightweight authentication and secured routing for NDN IoT in smart cities (LASeR)" [176], "Secure Hybrid Routing (SHR)" [177].

- **Le protocole SMRP [174]**
  SMRP utilise un paramètre multicouche dans l'algorithme de routage et lorsque les noeuds veulent rejoindre le réseau, ils doivent s'authentifier. Ce protocole n'entraîne aucune surcharge supplémentaire sur le processus de routage, car les paramètres multicouches contiennent les applications autorisées sur le réseau, une identification unique contrôlable par l'utilisateur et une liste des dispositifs autorisés sur le réseau. On peut cependant voir que le protocole consomme énormément du temps supplémentaire lors de la création du paramètre multicouche. Par conséquent, cet inconvénient rend ce protocole inadapté pour les réseaux à grande échelle.

  En outre, dans ce protocole, les propriétaires de chaque réseau IoT doivent enregistrer leurs propres applications, adresse réseau et adresse de liaison de données auprès d'un fournisseur de services (SP) légitime. Sur la base des informations des registres, avant la formation du réseau, le SP a le devoir de générer un fichier chiffré (EF) et de l'installer sur chaque dispositif.

  Comme tous les autres protocoles de routage, les dispositifs IoT envoient des messages *HELLO* après chaque intervalle de temps. Lorsque le dispositif (device 1) arrive à proximité d'un autre dispositif (device 2), l'en-tête des messages *HELLO* reçus de device 2 est vérifié par rapport aux en-têtes des messages *HELLO* du device 1. En cas de correspondance, les dispositifs communiqueront. Si un dispositif (x) souhaite

se connecter à un réseau IoT, il sollicitera un dispositif (y). Ensuite, le dispositif (y) vérifie l'adresse réseau, l'adresse de liaison de données du dispositif (x) dans la liste des dispositifs autorisés. Si le dispositif (x) est autorisé à rejoindre le réseau et que la ou les applications en cours d'exécution correspondent aux applications en cours d'exécution sur le dispositif (y), un signal est envoyé au générateur de code unique. Ce code unique est intégré dans les bits "réservés" des messages *HELLO* pour renforcer le niveau de sécurité. Parmi les inconvénients de ce protocole, nous citons :

i) SMRP ne conserve pas l'énergie des noeuds lors du routage. Cela peut réduire la durée de vie du réseau.

ii) La mémoire requise est plus élevée car il est nécessaire de stocker le fichier EF sur tous les dispositifs, ce qui peut être un handicap pour le passage à l'échelle ; i.e. autant les dispositifs sont moins nombreux sur le réseau IoT, la taille du fichier EF sera petite, sinon la taille augmente, ce qui peut entraîner des exigences de mémoire élevées dans les dispositifs.

iii) De plus, le nombre de dispositifs dans un réseau IoT appartenant au propriétaire spécifique doit être précisé à l'avance.

- **Le protocole SCOTRES** [168]
  SCOTRES est un système orienté confiance proposé pour un routage sécurisé dans les réseaux ad-hoc afin de faire progresser l'intelligence des entités du réseau en utilisant 5 métriques innovantes :

  – La consommation des ressources de chaque noeud est considérée par la métrique d'énergie pour imposer une quantité similaire de collaboration et augmenter la durée de vie du réseau ;

  – La métrique de topologie connaît les positions des nœuds et améliore l'équilibrage de charge ;

  – La tolérance en cas de dysfonctionnement périodique est fournie par la métrique d'intégrité de canal en raison de mauvaises circonstances de canal et le réseau est protégé contre les attaques de brouillage ;

  – La collaboration de chaque sujet pour une opération réseau particulière est évaluée par la métrique de réputation pour détecter les attaques spécifiques ;

  – la conformité totale est estimée par métrique de confiance, protégeant contre les attaques combinatoires

  Cependant, le protocole proposé ne prend pas en compte la confiance des noeuds clés dans le réseau. Bien que l'optimisation du routage puisse améliorer la sécurité dans une certaine mesure, elle ne peut fondamentalement pas garantir la crédibilité des noeuds et réduire efficacement la consommation d'énergie des noeuds dans les applications mobiles. De plus, bien que ce type de protocole prenne en compte le problème de crédibilité, l'optimisation du routage ne peut pas fondamentalement faire face aux attaques internes auxquelles est confronté le noeud lui-même.

- **Le protocole SERO-SH-IoT [175]**
  SERO-SH-IoT est un protocole de routage optimisé sécurisé pour le service Home-IoT. Il utilise la confiance entre le domaine Proxy mobile IPv6 (PMIPv6) et le système de maison intelligente basé sur une technique d'optimisation du chemin pour une communication efficace dans le réseau intelligent Home-IoT. Pour la sécurité, les auteurs ont utilisé l'algorithme Dife–Hellman. La sécurité et les performances sont assurées par le chemin des MN et le Les dispositifs IoT, la confiance entre le domaine PMIPv6 et la maison intelligente sont utilisés dans le nouveau protocole proposé. De plus, il comprend des étapes pour une gestion sécurisée du RO et du transfert, où l'authentification mutuelle, l'échange de clés, et la confidentialité sont pris en charge. La performance du protocole proposé est formellement analysée à l'aide de la logique BAN et de la validation automatisée des protocoles et applications de sécurité Internet (AVISPA). En outre, le protocole proposé repose sur une ancre de mobilité centralisée, basée sur le domaine PMIpv6, pour sécuriser les chemins et gérer le transfert transparent des MN se déplaçant sur différents réseaux. Une approche centralisée est connue pour présenter certaines limitations telles que l'évolutivité, le point de défaillance unique, etc.

  Le protocole présenté utilise l'authentification mutuelle avec le schéma standard de sécurité de la charge utile. Les résultats de l'étude sont explorés avec une latence réduite. Cependant, une telle implémentation de concept n'inclut pas le processus de virtualisation en ce qui concerne la validation. De plus, la variation du trafic n'est pas étudiée.

Justificatif du choix du protocole RPL

Durant notre étude, notre première contribution est basée sur l'amélioration du protocole de routage RPL. Notre choix est avisé envers ce protocole car il permet de configurer différentes métriques selon les exigences de différentes applications, comme décrit dans la *RFC 6551* [178]. En plus, RPL est un protocole de routage sensible à la QoS et basé sur des contraintes. Ainsi, la raison principale de notre choix du protocole RPL est le fait que le standard RoLL n'a pas spécifié une fonction d'objectif (OF) qui vise l'équilibrage de charge et l'efficacité énergétique. Par conséquent, la proposition de nouvelles métriques de routage reste une question ouverte à explorer.

2.3 Présentation du protocole RPL

Le groupe de travail *IETF RoLL* a développé un protocole de routage pour les réseaux LLNs et les réseaux de capteurs 6LoWPAN, appelé RPL (Routing Protocol for Low power and Lossy Networks). C'est un protocole de routage qui fonctionne au-dessus des deux couches IEEE 802.15.4 PHY et MAC.

RPL [62,179] est un protocole de routage à vecteur de distance, dans lequel un graphe acyclique orienté destination basé sur un ensemble de métriques est construit. Cette topologie est sous forme d'arborescence connue sous le nom de graphe acyclique dirigé (Directed Acyclic Graph (DAG)) composé d'un ou plusieurs noeuds puits. Dans le cas d'une seule racine, il est appelé graphe acyclique orienté vers la destination (Destination

Oriented DAG (DODAG)). Le noeud récepteur peut également être appelé routeur frontière du réseau (LLN Border Router (LBR)) lorsqu'il agit comme un pont entre le LLN et Internet.

RPL est conçu pour répondre aux exigences de base pour la transmission de données dans les LLN. Il est en cours d'élaboration en tant que norme à déployer dans un certain nombre d'environnements : réseaux urbains, réseaux intelligents, réseaux industriels, bâtiments et réseaux domestiques. Avec sa topologie robuste sur les liaisons avec perte, RPL met à jour les informations de routage afin de maintenir les informations sur l'état du réseau. RPL prend en charge différents types de trafic tels que (*M2P*) multipoint à point, point à multipoint (*P2M*) et point à point (*P2P*). Ainsi, Dans les réseaux LLN, il existe trois types de noeuds : les noeuds racines qui fournissent la connectivité à d'autres réseaux, les noeuds intermédiaires qui transfèrent les paquets aux noeuds racines et les noeuds feuilles (les noeuds qui se situent au bord du réseau).

Un noeud peut appartenir à plusieurs instances RPL dans le même réseau pouvant être exécutées simultanément, et chaque instance est identifiée de manière unique par un RPL_InstanceID. L'instance RPL consiste en un ou plusieurs DODAG utilisant une racine indépendante, ce qui peut contribuer à satisfaire plusieurs QoS des applications IoT.

RPL répond à plusieurs spécifications exigées par différents types d'applications notamment :

- La domotique, comme la commutation d'éclairage, le contrôle des stores, les systèmes d'alarme, la surveillance de la température, etc. [180].
- L'automatisation des bâtiments : systèmes de gestion des bâtiments déployés dans différents environnements tels que les universités, les hôpitaux, les immeubles de bureaux, etc. [181].
- Les applications industrielles pour améliorer la productivité et la sécurité des usines [182].
- Les applications urbaines et les réseaux intelligents pour la surveillance environnementale [183].

Limitations du protocole RPL :

i) Ne prend pas en charge le routage à chemins multiples.

ii) L'équilibrage énergétique et l'équilibrage de charge ne sont pas aussi pris en compte.

2.3.1 Construction du DODAG

Le DODAG est construit selon un processus de découverte de voisins (Neighbor Discovery (ND)) [184], qui repose sur deux opérations principales :

1. La construction de directions vers le bas (de la racine aux noeuds feuilles) dans laquelle le processus commence au noeud racine par la diffusion d'un message de contrôle DIO à ses voisins, afin d'annoncer son DODAGID (qui contient les informations de rang et l'OF). Dans cette étape, il existe deux possibilités : soit le noeud

recevant le message DIO souhaite rejoindre le DODAG, soit il est déjà associé au DODAG et souhaite bénéficier de certains avantages. Dans la première possibilité, il exploite les informations fournies dans le message DIO en ajoutant l'expéditeur du message DIO à sa liste de parents candidats. Ensuite, il calcule son rang en fonction de l'OF et enfin il transmet le message DIO mis à jour. Après avoir calculé son propre rang en fonction de l'OF, il sélectionne l'un des parents depuis la liste des parents comme parent préféré. Ensuite, le noeud transmet le message DIO avec les informations mises à jour à ses voisins et répète le même processus jusqu'à ce que tous les noeuds possèdent une route ascendante pour transmettre le trafic vers la racine. Tandis au second cas, où un noeud est déjà associé au DODAG et il reçoit plus qu'un message DIO, le noeud a le choix de rejeter le message DIO ou de le traiter en conservant son rang dans le DODAG ou d'optimiser son rang par un niveau inférieur.

2. La deuxième étape dans la construction de la direction ascendante consiste à propager les messages DAO des noeuds feuilles vers la racine du DODAG. D'une autre manière, RPL spécifie un mécanisme pour les applications nécessitant un trafic descendant depuis la passerelle (racine) vers un noeud, dans lequel un noeud envoie un message de contrôle de type DAO en unicast dans le but de créer une information du chemin inverse. En plus, un autre type de message de contrôle *ICMPv6* appelé DIS qui est fourni par le noeud qui ne reçoit pas de message DIO en sollicitant les voisins d'un message DIO.

Chaque noeud rejoignant le DODAG possède une route vers la racine. Les noeuds qui rejoignent le DODAG agissent l'une des deux manières suivantes : si le noeud agit comme un routeur, il diffuse les informations du graphe à ses voisins, sinon le noeud agit comme un noeud feuille et n'envoie pas les messages DIO. Tous les noeuds voisins répètent tout ce processus et construisent les bords du DODAG (feuilles). Le processus de construction du DODAG est illustré dans la Figure 2.2.

La construction du DODAG est basée sur la fonction d'objectif OF qui déploie un ensemble de métriques de routage pour construire le DODAG sur la base d'algorithmes ou d'une formule de calcul.

2.3.2 Messages de contrôle dans RPL

Le protocole RPL définit quatre nouveaux messages de contrôle *ICMPv6* [59] afin de construire et maintenir la topologie de routage ainsi de partager les informations de routage et de gérer les DODAG. Ces messages sont : DIS, DIO, DAO et DAO-ACK. Nous définissons chaque message de contrôle comme suit :

- **DODAG Information Solicitation (DIS)** : Ce sont des messages de sollicitation pour les messages DIO, i.e. ils sont généralement utilisés pour demander des informations liées au routage aux noeuds voisins. Les messages DIS sont utilisés pour déclencher une transmission DIO à partir d'un noeud RPL. Ces messages n'ont pas de corps et sont envoyés par un noeud sollicitant de rejoindre le réseau. Comme alternative pour attendre une réception d'un message DIO, un noeud diffuse un message DIS dans son voisinage et sollicite des messages DIO des noeuds voisins.

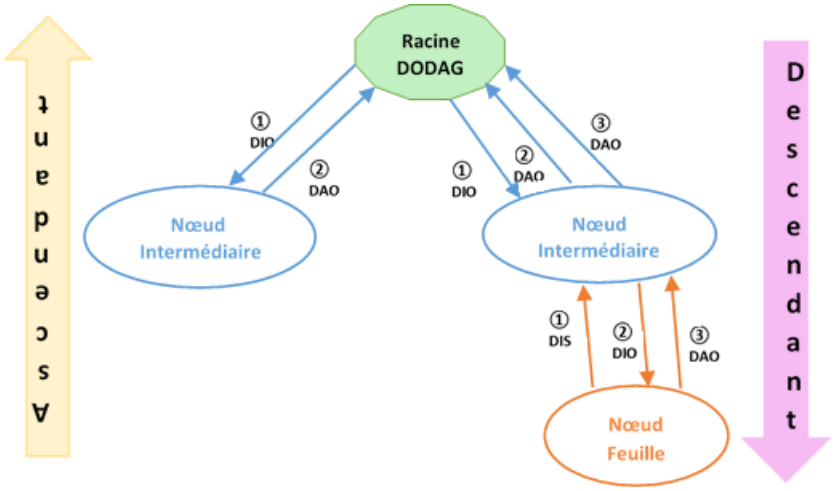


FIGURE 2.2 – Le processus de construction du graphe DODAG

- **DODAG Information Object (DIO)** : Ce sont des messages qui contiennent les informations requises par les noeuds RPL pour découvrir une instance RPL, obtenir leurs paramètres de configuration (tels que l'identité des racines DODAG, les métriques de routage, ainsi que le rang), sélectionner un ensemble de parents et maintenir le graphe DODAG. Un message DIO est composé de cinq champs principaux correspondants à l'ID d'instance RPL, l'ID DODAG, le numéro de version, la valeur de rang et le champ "Mode of Operation (MoP)". Les champs ID d'instance RPL et ID DODAG sont définis par le noeud racine. Ils indiquent respectivement l'identifiant de l'instance RPL et l'identifiant du graphe DODAG qui est l'adresse IPv6 de la racine. Le numéro de version d'un DODAG est incrémenté par le noeud racine, chaque fois que le DODAG est mis à jour. Le champ MoP donné par la racine permet la maintenance des routes descendantes et des communications multicast. Les noeuds rejoignant le DODAG doivent correspondre au champ MoP ainsi qu'à ses propriétés, afin de participer en tant que routeur, sinon les noeuds RPL peuvent uniquement rejoindre le graphe en tant que noeuds feuilles.

  Ce type de messages est diffusé par le noeud racine au début de la construction et la maintenance de la topologie DODAG. La racine appelée "Sink ou Border Router" est le seul noeud capable d'initier la diffusion des messages DIO. Ces messages peuvent également être envoyés en monodiffusion, pour répondre à un message DIS reçu d'un des voisins. La stratégie de transmission des messages DIO est contrôlée par un algorithme appelé *Trickle* [185].

  Les messages DIO imposent une surcharge de réseau importante qui peut être contrôlée avec un algorithme de minuterie *Trickle* [186]. Le plus petit intervalle entre deux messages DIO est égal à *DIO-Minimum-Interval* qui continue à se doubler jusqu'à ce qu'il atteigne la valeur maximale déterminée par DIO *(Interval-Doubling)*.

  Les informations sur le rang, l'OF, les ID, etc. sont intégrées dans les messages DODAG Information Option (DIO).

- **Destination Advertisement Object (DAO)** : Ces messages sont utilisés pour construire des routes descendantes tout au long du graphe DODAG ; i.e. les mes-

sages DAO sont envoyés par le noeud fils envers le noeud parent afin de faire circuler le trafic P2M (depuis le noeud racine vers les noeuds descendants). Ces messages peuvent être unicast qui sont envoyés d'un noeud fils envers le noeud parent sélectionné en mode conservation (storing mode) ou unicast envoyés vers le noeud racine quand le mode de fonctionnement est non conservation (non-storing mode). Les messages DAO incluent le RPL_InstanceID, le rang, la durée de vie DAO, la balise Route et la destination Prefix. Ces messages sont facultatifs et utilisés uniquement lorsqu'une route descendante est nécessaire. DAO est le seul message de contrôle pouvant être acquitté par la destination.

- **Destination Advertisement Object ACKnowledgement (DAO-ACK)** : Ce sont des messages d'acquittement aux messages DAO. Un message DAO-ACK est renvoyé à l'expéditeur en monodiffusion (unicast) en réponse à un message DAO (parent DAO ou racine DODAG). Ce type de messages indique si le voisin qui a reçu le message DAO est disposé à agir comme un saut précédent pour l'expéditeur dans la route descendante ou non-disposé. En cas de la non-réception du message DAO-Ack par l'expéditeur du message DAO, ce dernier peut réémettre le message DAO initial une autre fois.

2.3.3 L'algorithme Trickle

L'algorithme *Trickle* est utilisé comme une temporisation dynamique de la vitesse d'envoi des messages DIO [185], i.e. plus la topologie devient stable, moins les messages de contrôle sont envoyés, afin d'économiser de l'énergie et également pour réduire les messages redondants. Lorsqu'une incohérence est détectée, l'algorithme *Trickle* réinitialise son minuteur et les noeuds envoient des messages DIO plus fréquemment pour mettre à jour le DODAG.

L'algorithme maintient un minuteur *Trickle* qui s'exécute pendant un intervalle défini en se caractérisant par trois paramètres : taille d'intervalle minimale *Imin*, taille d'intervalle maximale *Imax* et une constante de redondance (e> 0). Lorsque l'algorithme commence à s'exécuter, il définit la taille d'intervalle actuelle *Icourant* à une valeur dans la plage de $[Imin, Imax]$. Lorsque l'intervalle commence, l'algorithme réinitialise un compteur c à 0 et règle le temps dans l'intervalle courant *tcurrent* à un point aléatoire dans la plage *[Icurrent = 2 ; Icurrent]*. Chaque fois que l'algorithme reçoit une transmission qui est "cohérente", il incrémente la valeur *c*. Si l'algorithme reçoit une transmission qui est "incohérente" et *Icurrent* est supérieur à *Imin*, il réinitialise le minuteur *Trickle*. A l'instant *tcurrent*, un message DIO est envoyé si et seulement si c'est inférieur à e. Lorsque la période *Icurrent* expire, l'algorithme double la longueur de l'intervalle de sorte qu'elle ne dépasse pas *Imax*. Les événements suivants sont considérés comme des incohérences dans RPL :

- Lorsque des boucles de routage sont détectées.

- Lorsqu'un noeud reçoit d'un voisin des informations obsolètes (numéro de version d'instance antérieur).

2.3.4 La fonction d'objectif (OF)

La fonction d'objectif (OF) joue un rôle majeur dans RPL en permettant de :

- Construire le DODAG,
- Calculer le rang du noeud , i.e. définir comment transformer une métrique en rang (la distance à la racine),
- Définir comment sélectionner les routes au sein d'une instance RPL,
- L'optimisation des chemins de routage dans un DODAG,
- Spécifier les règles qu'un noeud doit suivre pour choisir son parent préféré.

La construction du DODAG est basée sur la fonction d'objectif (OF) qui déploie un ensemble de métriques de routage pour construire la topologie DODAG sur la base d'algorithmes ou d'une formule de calcul. La fonction d'objectif (OF) combine les métriques et les contraintes pour trouver le meilleur chemin. Par exemple, elle trouve le chemin qui a un délai minimum et ce même chemin ne contient pas un noeud alimenté par batterie. Dans cet exemple, le chemin avec un délai minimum représente la métrique et les noeuds non alimentés par batterie représentent la contrainte.

La norme offre le choix de sélectionner la fonction d'objectif (OF) appropriée selon les exigences de l'application, ce qui rend le protocole RPL hautement adaptatif et dynamique. Par ce moyen, la fonction d'objectif (OF) optimise les coûts du chemin de routage en fonction des exigences de l'application, par exemple, les exigences de l'IoMT sont plus contraignantes que celles de l'IoT. Afin de propager la fonction d'objectif (OF) à l'intérieur d'une instance RPL donnée, la racine inclut un point de code objectif "Objectif Code Point (OCP)" dans son message DIO (chaque OF est identifiée par un OCP). La fonction d'objectif est également utilisée pour définir le rang d'un noeud qui représente la distance entre les noeuds et un noeud racine DODAG. OF (*OF0*) est définie comme une fonction par défaut commune à toutes les implémentations et assure l'interopérabilité entre les différentes implémentations.

Ainsi, les noeuds terminaux choisissent un parent préféré en tenant compte d'une fonction d'objectif (OF) qui est minimisée ou maximisée selon les exigences de l'application en fonction de certaines métriques de routage (par exemple *ETX*, HC (Hop Count), Node-Energy...etc.) représentant le coût de chemin quantitatif.

Le groupe de travail *IETF ROLL* a défini deux fonctions d'objectifs :

- ***Objective Function Zero (OF0)*** [187] : C'est une fonction d'objectif (OF) générique, parfois référée comme une fonction de comptage de sauts, et doit être prise en charge par tous les noeuds du réseau. Elle fonctionne en calculant le rang basé sur l'ajout d'une valeur scalaire qui représente les propriétés du lien (normalisée entre 1 et 9 pour exprimer les propriétés du lien avec 1 : excellent et 9 : très mauvais) au rang de son parent préféré (annoncé par un message DIO). La valeur scalaire peut être n'importe quel type de métrique utilisée. Si *OF0* utilise le nombre de sauts comme métrique de routage, tous les scalaires sont égaux à 1 et les chemins les plus courts vers le récepteur sont calculés.

- ***MRHOF*** [188] : Cette fonction vise à optimiser le chemin qui minimise une métrique en évitant des changements de chemin trop fréquents pour des variations de métriques trop petites en introduisant une hystérésis. *MRHOF* fonctionne avec des métriques additives le long d'une route, et la métrique correspondante (nombre de sauts, latence ou *ETX*) est diffusée par les messages DIO grâce à l'option conteneur métrique DIO. Afin de sélectionner les parents, *MRHOF* introduit une fonction d'hystérésis qui peut être exprimée par l'algorithme 1.

Algorithm 1 : La fonction *MRHOF*

P_1 et P_2 étant respectivement le coût du chemin vers le parent 1 et le parent 2
P_1 est le meilleur parent actuel et P_2 est un parent candidat
Si ($P_1\_Path\_cost + PARENT\_SWITCH\_THRESHOLD > P_2\_Path\_Cost$)
Alors Commuter en P_2 en tant que parent préféré
Sinon Gardez P_1 comme parent préféré
Fin si
où *PARENT_SWITCH_THRESHOLD* est la fonction d'hystérésis, i.e. la différence minimale entre le coût du chemin à travers le parent préféré et le coût du chemin d'un parent candidat afin de déclencher la sélection d'un nouveau parent préféré.

2.3.5 Rang (Rank)

La valeur de rang (***en anglais*** *Rank*) d'un noeud correspond à sa position dans le graphe par rapport à la racine. Chaque noeud du DODAG a un rang, qui représente sa distance relative à la racine calculée par la fonction d'objectif OF. Le rang d'un noeud doit toujours être supérieur au rang de ses parents afin de garantir l'aspect cyclique du graphe. Cette valeur augmente en descendant vers les noeuds feuilles. Pour éviter les boucles de routage, un rang 0 est attribué au noeud racine, ainsi, il s'augmente au fur et à mesure dans la direction vers les noeuds feuilles de sorte que chaque noeud fils a un rang supérieur à celui de ses parents.

La propriété du rang est au coeur des opérations de routage efficaces du protocole RPL notamment la construction DODAG. De plus, le rang permet de gérer la surcharge des messages de contrôle, d'empêcher la formation des boucles de routage et de créer une topologie de réseau optimale. Par ailleurs, toute attaque sur la propriété du rang perturbera gravement le bon fonctionnement du protocole RPL. Le calcul du rang pour *OF0* est donné par l'algorithme 2. L'augmentation du rang représente la propriété du lien comme indiqué dans l'algorithme 2.

Le calcul du rang de *MRHOF* est introduit par la notion de coût du chemin qui quantifie la propriété de ce dernier vers la racine RPL par rapport à la métrique utilisée. Le coût du chemin est obtenu en ajoutant le coût de la métrique de liaison concernant un parent avec le coût du chemin annoncé par ce dernier. La façon de transformer le coût d'un chemin en rang dépend de la métrique. Le calcul du rang pour *MRHOF* est donné par l'algorithme 3.

Algorithm 2 : Calcul du rang pour *OF0*

$R(N) = R(P) + augmentation\_rang$
$rank\_increase = (Rf * Sp + Sr) * MinHopRankIncrease$
où :
- *R(P) :* rang des parents préférés
- *Sp :* step_of_rank : L'expression des propriétés du lien normalisé entre les valeurs 1 jusqu'à 9. Il faut noter que dans [187], il ne définit pas comment normaliser une métrique donnée car elle dépend de l'implémentation.
- *Sr :* stretch_of_rank : l'augmentation maximale au *step_of_rank* d'un parent préféré pour permettre la sélection d'un autre noeud successeur.
- *Rf :* rank_factor : un facteur utilisé pour augmenter l'importance des propriétés du lien dans le calcul du *rank_increase*

Algorithm 3 : Calcul du rang pour *MRHOF*

$Pathcost = parentpath\_cost + link\_cost$
$Rang = fonction(pathcost)$
où *link_cost* est le coût associé au lien du parent par rapport à la métrique sélectionnée et *parentpath_cost* est annoncé par le parent et représente le *path_cost* du parent lui-même. La manière de transformer *path_cost* en rang dépend de la métrique choisie, cette notion est définie dans [188].

2.3.6 Modes de transmission dans le protocole RPL

Le protocole RPL prend en charge trois modèles de trafic différents : Multipoint-à-Point (MP2P), Point-à-Multipoint (P2MP) et point à point (P2P) qui sont discutés plus en détails dans ce qui suit.

- **MP2P** : RPL active le trafic (*MP2P*), i.e. routes ascendantes depuis les noeuds vers la racine, en envoyant des messages DIO depuis la racine DODAG vers les noeuds terminaux. Un parent préféré est sélectionné comme prochain saut parmi l'ensemble des parents candidats pour les routes ascendantes. Ce modèle de trafic est le plus dominant dans RPL.

- **P2MP** : Le protocole RPL active le trafic P2M et fournit des routes descendantes, i.e. depuis la racine DODAG vers les noeuds terminaux. Le trafic P2M est accompli en envoyant des messages DAO vers la racine DODAG. Les routes descendantes sont maintenues par des noeuds en se basant sur deux modes à savoir "mode de stockage" (*en anglais storing*) et "mode non-stockage" (*en anglais non-storing*). En mode de stockage, chaque noeud qui n'est pas une racine dans un graphe DODAG doit stocker les informations préexistantes qu'il a reçues sous forme de messages DAO depuis les noeuds voisins. À chaque saut sur la route, le noeud examine sa table de routage et décide à quel voisin l'envoyer ensuite. Certains noeuds du réseau ont des contraintes de mémoire et peuvent être incapables de stocker des entrées de routage. Ce type de noeuds supporte le mode non-stockage et dans ce mode seule la racine DODAG stocke les routes et qui est responsable de tout le routage. Dans ce mode le seul noeud stockant une table de routage est le routeur frontière (noeud

racine), qui utilise le routage source pour envoyer les paquets. Dans ce cas, tous les paquets pour la communication P2P doivent être envoyés à la racine du DODAG.

- **P2P** : Un autre type de trafic qui prend son sens depuis les noeuds intermédiaires ou la racine vers les noeuds feuilles. Ce trafic prend une direction vers le haut (vers un parent ancêtre commun) auquel il est transmis ensuite vers le bas vers la destination (descendant). Le routage P2P peut également être pris en charge par le mode de trafic "stockage" et "non-stockage".

RPL ne permet pas l'usage des deux modes "stockage" et "non-stockage" dans le même réseau. Il a été démontré que cela peut faire rebondir les paquets entre les deux noeuds sur les chemins qui ont des MoP différents (stockage et non-stockage) en atteignant jamais la destination [189]. En effet, une optimisation simple permet à un noeud d'envoyer un paquet directement à la destination, s'il s'agit d'un voisin à un seul saut.

2.3.7 Métriques de routage

a) Types de métriques

Les métriques et les contraintes de routage sont transportées dans l'objet *DAG Metric Container* défini dans [62]. Si plusieurs métriques et/ou contraintes sont présentes dans le conteneur de métriques DAG, leur utilisation pour déterminer le meilleur chemin peut être définie par une fonction d'objectif (OF). La Figure 2.3 présente quelques exemples de métriques utilisées par les fonctions d'objectifs. Les métriques de routage qui peuvent être utilisées par RPL pour construire le DODAG se subdivise en deux catégories [178] :

Métrique de noeud

- État et attribut du noeud (Node State and Attribute (NSA)) : Fournit des informations sur les caractéristiques du noeud, par exemple, surcharge du processeur, manque de mémoire. . .etc. Il peut être utilisé pour annoncer les noeuds du réseau qui doivent être évités.

- Énergie du noeud (Node Energy Object) : Elle présente l'énergie dépensée par les noeuds pendant leurs opérations dans le réseau. Elle peut également représenter l'énergie restante de la batterie. En raison de la distribution des noeuds et de leur distance vers la racine, certains noeuds peuvent perdre leur énergie plus rapidement.

- Nombre de sauts (Hop Count Object) : Il calcule le nombre de sauts entre la source et la destination. Le *Hop-Count* est la métrique de routage la plus utilisée dans les réseaux sans fil. Il est utilisé pour mesurer la longueur de chemin dans un réseau. Le principal inconvénient de cette métrique est de choisir le chemin qui fournit un faible nombre de sauts quelle que soit la qualité de la liaison [190].

Métrique de lien

- Débit de liaison (Throughput) : La plage de débit gérée par le lien en plus du débit actuellement disponible.

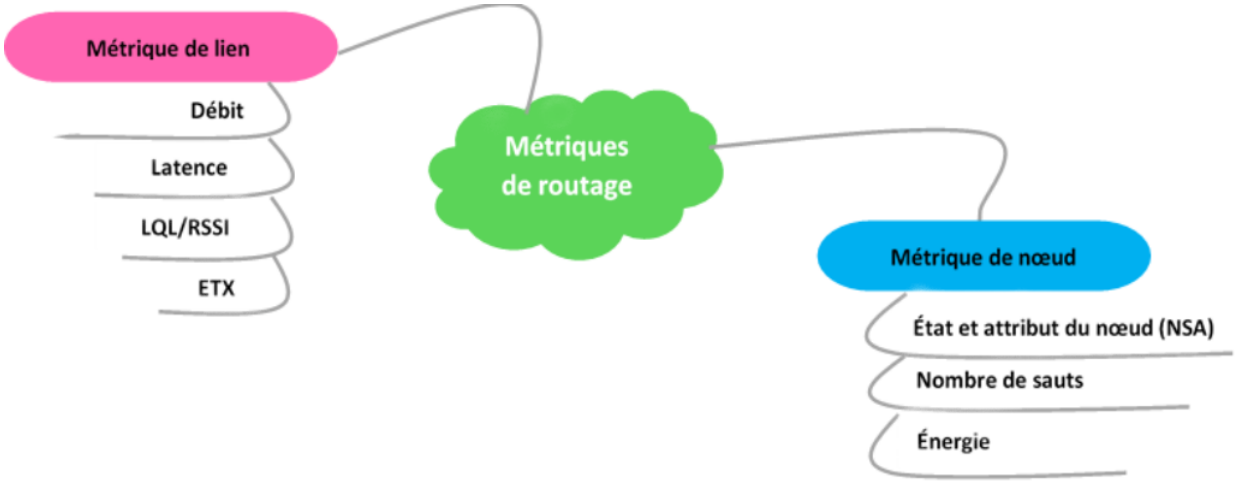


FIGURE 2.3 – Différentes métriques de noeud et de lien utilisées par les fonctions d'objectifs [29]

- Latence de liaison (Latency) : L'intervalle de temps entre le temps d'envoi du paquet par la source et le temps de réception du paquet par la destination.
- Fiabilité de la liaison (Link Reliability) : Il peut s'agir d'une valeur discrète, de 0 à 7, où 0 indique que la qualité de la liaison est inconnue et 1 indique la qualité de liaison la plus élevée. Elle peut également être exprimé comme le nombre attendu de transmissions d'un paquet pour qu'il soit reçu sans erreur à sa destination [191]. Un exemple sur la métrique qui garantit la fiabilité de la liaison :
  - *ETX* (Expected Transmission Count) : Le nombre de transmissions attendu indique le niveau de fiabilité du réseau. *ETX* représente le nombre des transmissions nécessaires pour recevoir un accusé de réception depuis la destination [190, 192]. Une autre définition de la métrique *ETX* [178] : c'est une métrique "additive", et sur chaque liaison, elle exprime le nombre de transmissions pour une livraison réussie d'un message au voisin du saut suivant. En se basant sur la métrique *ETX*, les liens avec perte sont distingués indépendamment de la cause de perte de données, par exemple, provoquée par la couche physique ou bien au niveau de la couche MAC.

    Le chemin qui fournit la valeur la plus faible d'*ETX* est choisi comme le moyen optimal pour atteindre le noeud racine. Par contre, la valeur élevée d'*ETX* reflète le manque de la fiabilité dans le réseau.
  - *Received Signal Strength Indicator (RSSI)* : Les principaux estimateurs de la liaison radio sont : le RSSI et le LQI. Le RSSI est une couche de liaison matérielle, qui agit comme un émetteur-récepteur radio chargé de vérifier la disponibilité du signal de fréquence reçu avant d'envoyer des données [29].

b) Combinaison des métriques de routage dans RPL

Afin qu'un réseau unique répond à des exigences diverses, la conception de métriques composites appropriées combinant des métriques de routage primaires a pour but de

prendre en considération la QoS dans le contexte du routage RPL [193]. Cette combinaison des métriques fait appel à deux types d'opérateurs de composition : la composition additive et la composition lexicographique.

- **Composition additive** : Une métrique de routage est appelée additive sur le chemin si le poids d'un chemin est égal à la somme des poids des liens qui produisent le chemin lorsqu'il est concaténé. Le poids d'un chemin dans une métrique de routage composite additive peut être exprimé comme ω, est la fonction qui mappe un chemin ou un lien vers un poids pour la métrique de routage additive.

- **Composition lexicographique** : Lorsque plusieurs métriques sont combinées suivant une approche lexicographique, cela impose au routage de prioriser l'une des métriques de la composition par rapport aux autres. Cela signifie que les métriques de routage principales sont hiérarchisées et lorsqu'un chemin offre un meilleur poids par rapport à la première métrique, il sera préféré quel que soit le poids du chemin des métriques restantes. La deuxième métrique n'est prise en compte que si plusieurs chemins correspondent à des poids égaux pour la première métrique. Par exemple, le nombre de sauts et le débit sont deux mesures où un critère d'optimisation évident est de sélectionner le chemin avec le nombre de sauts le plus petit et le débit maximal. Même si le nombre de sauts est minimisé et le débit est maximisé, il est possible de les combiner dans une métrique de routage composite lexicographique et cela conduirait à sélectionner parmi les chemins les plus courts, celui avec le plus grand débit.

Exemple d'une métrique composite Dans tout protocole de routage, la consommation d'énergie et la fiabilité sont des caractéristiques très importantes qui ont un impact direct sur les performances des réseaux. Dans le cas où RPL ne considère que la métrique d'énergie, les décisions de routage dépendront de la disponibilité énergétique des noeuds, ce qui augmentera le taux de perte de paquets ainsi que le délai. Dans l'autre cas, si nous prenons en considération que la fiabilité des liens entre les noeuds sans tenir compte de l'énergie restante, ni de l'énergie consommée par les noeuds. Par conséquent, certaines routes peuvent être plus encombrées que d'autres, en particulier les noeuds les plus proches du noeud racine, qui sont plus susceptibles à un épuisement prématuré de l'énergie entraînant une déconnexion rapide du réseau.

En outre, dans *MRHOF*, deux métriques peuvent être utilisées soit la métrique *ETX* ou la métrique d'énergie selon la définition de la norme RPL. Chacune de ces métriques possède ses avantages et ses inconvénients, par exemple la métrique *ETX* consomme beaucoup d'énergie et la métrique d'énergie ne garantit pas la fiabilité de la livraison des paquets entre les noeuds. Par conséquent, afin de résoudre ce problème et en bénéficiant de la combinaison de plusieurs métriques de routage en une métrique composite, comme dans notre cas, nous avons combiné l'*ETX* avec l'énergie, ce qui a conduit à l'amélioration des performances.

2.4 Revue sur les différentes améliorations du protocole RPL dans l'IoT

Il existe de nombreux aspects que les protocoles de routage doivent couvrir afin de répondre aux exigences des applications IoT. Le protocole RPL représente le candidat le plus populaire pour le routage de données dans les LLN, attiré par un grand nombre de travaux de recherche, de nombreuses améliorations dans la littérature pour relever un ou plusieurs défis de routage. Dans cette section, nous avons examiné une taxonomie sur l'ensemble des travaux connexes de ce protocole. Ainsi, nous fournissons une analyse approfondie sur les principaux moteurs des améliorations et extensions du protocole RPL. Nous subdivisons cette analyse en sept sous-sections : analyse des performances de RPL, l'efficacité énergétique, l'interopérabilité entre les MoP, les améliorations du stockage MoP et la compatibilité, les améliorations des OFs & métriques combinées, la mobilité, la QoS et la sécurité.

De nombreuses recherches se sont concentrées sur le coeur du protocole RPL et son déploiement dans divers environnements afin de mettre en lumière ses caractéristiques et ses limites [194, 195]. Notamment l'état de l'art sur RPL qui a été présentée dans [179] où les auteurs ont fourni une revue complète sur les différents domaines et défis de l'application RPL. D'un autre côté, un état de l'art récent dans [29] qui met l'accent sur les fonctions d'objectifs existantes en mettant en évidence les avantages et les lacunes de chaque solution étudiée en donnant une étude comparative des OF existantes ainsi qu'une classification des métriques utilisées. De plus dans [196], les auteurs ont présenté des solutions de routage les plus pertinentes pour les réseaux LLN en identifiant les exigences et les problèmes les plus étudiés par les protocoles de routage actuels proposés pour les scénarios IoT, en particulier les améliorations RPL. D'autres états de l'art peuvent se retrouver dans [162, 197–201].

De nombreuses suggestions ont été proposées pour améliorer le protocole RPL, qu'on les classe sous plusieurs catégories notamment :

2.4.1 Analyse des performances de RPL

Des études d'analyse des performances du protocole RPL basées sur les métriques de routage : le nombre de sauts et/ou *ETX*, ont été étudiées dans les deux travaux [184, 202]. Différentes OFs du protocole RPL et leur analyse de performances à l'aide de plusieurs passerelles sont présentées dans [203]. Les auteurs dans [135] ont examiné une évaluation du protocole RPL pour les réseaux à faible puissance et avec perte dans laquelle plusieurs problèmes ont été identifiés, notamment : l'incompatibilité des modes de fonctionnement "mode avec stockage" et "mode sans stockage", ainsi que les boucles de routage.

Une autre analyse des performances de RPL est rapportée dans [204] qui identifie la mise en place rapide du réseau RPL ainsi que l'efficacité des délais de communication. Néanmoins, la surcharge élevée représente un inconvénient potentiel de ce protocole. Une autre étude [205] a également signalé des problèmes de manque de fiabilité du protocole RPL en raison du manque de connaissance de la qualité de lien dans tout le réseau.

Les auteurs dans [206] ont présenté les principales mesures et fonctionnalités de RPL. Cependant, ils ont limité leur étude que sur un petit nombre d'articles liés aux OFs de RPL sans fournir une analyse approfondie de la faisabilité des études rapportées. De plus,

les auteurs n'ont pas analysé des solutions proposées pour atténuer les faiblesses du RPL en termes de maintenance du routage et de routage descendant. En outre, les auteurs dans [207] utilisent une variété de paramètres et d'environnements pour évaluer les OFs normalisées. Ils utilisent des noeuds stationnaires dans la distribution de la grille tandis que les noeuds mobiles sont distribués de manière aléatoire. Un ensemble de mesures prend en compte le temps de convergence, les changements dans les structures d'arborescence DODAG, le taux de désabonnement moyen dans le réseau, la consommation d'énergie, le taux de paquets reçus et perdus (PDR), le taux de paquets dupliqués et le nombre moyen de sauts...etc. Les résultats montrent que la fonction d'objectif *OF0* surpasse la fonction d'objectif *MRHOF* en termes de consommation d'énergie, de temps de convergence et de cycles de service dans la distribution statique du réseau. Sinon, les deux fonctions d'objectifs agissent de la même manière lors de la distribution aléatoire mobile.

Encore plus de recherches ont été proposées pour étudier les performances du protocole RPL dans différents scénarios. Par exemple, les auteurs dans [208] sont focalisés sur l'amélioration des performances de RPL du point de vue de la convergence dans le processus de formation d'arbres dans les réseaux basés sur IEEE 802.15.4.

a) Efficacité Énergétique

En raison des contraintes d'énergie de divers dispositifs IoT, il est nécessaire que la tâche d'envoi de paquets puisse être effectuée avec un minimum de dépense d'énergie. Par conséquent, la consommation d'énergie représente une QoS cruciale pour tous les protocoles de routage dédiés pour les LLNs. Sur ce compte, le protocole RPL prend en compte la consommation d'énergie et propose des méthodes pour minimiser son utilisation. Le problème de la consommation d'énergie dans RPL est abordé par un algorithme de minuteur appelé "*Trickle Timer*" [185], qui vise à minimiser le nombre de messages de contrôle inutiles. Cependant, il est prouvé que ce minuteur présente ses propres inconvénients dans les environnements dynamiques en entraînant une transmission inefficace des données et une perte d'énergie élevée en raison de l'échec de la livraison des paquets [209].

De nombreux chercheurs prennent en compte la consommation d'énergie lorsqu'ils suggèrent une amélioration du protocole RPL, d'où l'une des approches les plus courantes consiste à utiliser l'énergie comme métrique de routage dans l'OF. Une autre étude basée également sur le même principe note que la consommation d'énergie augmente avec des densités de noeuds plus élevées et des réseaux plus grands [210]. Par ailleurs, les noeuds dans ces cas souffrent d'un nombre plus élevé de transmissions.

Dans une étude sur une fonction d'objectif éco-énergétique dédiée aux applications du compteur intelligent et les applications industrielles [211], les auteurs utilisent l'énergie résiduelle et la consommation d'énergie prévue dans l'OF dénommée OF éco-énergétique intelligente (Smart Energy Efficient Objective Function (SEEOF)). Les résultats montrent une amélioration de 22% à 27% de la durée de vie du réseau par rapport aux réseaux utilisant *MRHOF* comme OF. Dans une autre étude [212], l'énergie résiduelle est utilisée comme une seule métrique dans l'OF servant à améliorer la distribution de la consommation d'énergie et prolonge la durée de vie du réseau. Elle ne prend pas en compte d'autres mesures importantes comme le taux de perte de paquets, le délai ou le débit.

Les auteurs dans [213] ont présenté une nouvelle proposition d'amélioration de l'équilibrage énergétique dans le réseau visant à maximiser la durée de vie des noeuds. L'approche est basée sur le protocole RPL en créant une solution de routage qui considère l'estimation

de la consommation d'énergie. En utilisant un mécanisme pour mesurer la durée de vie attendue (ELT) des noeuds et en explorant les chemins multiples, l'approche proposée tente d'éviter l'utilisation des goulots d'étranglement (noeuds avec moins d'énergie) et équilibre la consommation d'énergie. Les auteurs ont également suggéré l'utilisation d'un mécanisme pour limiter l'échange parental ce qui réduit le nombre de messages de contrôle en contribuant à moins de transmissions et d'épuisement d'énergie.

Les études qui visent l'équilibrage de charge ont un impact significatif sur la consommation d'énergie, par conséquent, la répartition de cette charge réduit la congestion et conduit à un débit plus élevé. Cela signifie également que la consommation d'énergie est répartie plus efficacement entre les noeuds en offrant une meilleure durée de vie pour l'ensemble du réseau. Dans une étude sur la technique de coordination entre les noeuds puits [214], les messages de contrôle de RPL sont utilisés pour ajuster la taille du sous-réseau par rapport aux autres noeuds puits. Les résultats de simulation montrent une amélioration à la fois du débit et de la distribution d'énergie entre les noeuds du réseau. En outre, dans une étude d'équilibrage énergétique, les auteurs proposent une méthode d'estimation de la consommation d'énergie comme métrique de routage basée sur le RDC [215]. Ils ont obtenu une meilleure distribution de l'énergie et un PDR plus élevé. Cependant, cette amélioration est marginale par rapport à l'utilisation du *MRHOF* comme OF. En plus, la proposition n'apporte aucun avantage supplémentaire autre qu'une économie d'énergie marginale. Une autre technique de routage et d'agrégation pour une énergie minimale (RAME) dans [216], qui utilise les informations des noeuds avec l'énergie la plus faible pour réguler le trafic. Cette approche limite le débit, mais elle est très efficace pour les applications qui sont critiques en terme d'énergie.

b) Interopérabilité entre les modes d'opération (MoP) de RPL

Dans le protocole RPL, le modèle de trafic pris en charge est défini en fonction du MoP utilisé. Cependant, le choix du MoP idéal à adopter implique également la prise en compte des ressources de calcul des différents dispositifs. En d'autre termes, le choix du MoP avec la prise en charge de différents modèles de trafic (i.e. le mode stockage du MoP) peut exiger plus de capacité matérielle et empêcher les dispositifs "plus faibles" d'exécuter le protocole. Dans ce cas, une solution plus raisonnable pourrait être de créer un réseau avec un MoP différent exécuté par les noeuds ayant plus de capacités et de gérer les noeuds "les plus faibles" uniquement comme des noeuds feuilles. Cependant, le scénario présenté pourrait rencontrer plusieurs problèmes d'interopérabilité une fois que les messages de contrôle sont utilisés et traités différemment selon le MoP. En outre, comme indiqué sur le document officiel de RPL, chaque MoP doit être adopté individuellement par l'ensemble des noeuds du réseau.

Ainsi, compte tenu des limites qui peuvent émerger pour l'utilisation simultanée des différents MoP, les auteurs dans [217] ont présenté le protocole DualMOP-RPL, une version améliorée de RPL qui prend en charge à la fois le mode stockage et non stockage en même temps sans réduire les performances du réseau. Afin d'atteindre cet objectif, ils introduisent cinq améliorations différentes dans le protocole RPL. La première permet aux noeuds "plus faibles", initialement définis comme des feuilles, d'exécuter un MoP différent que celui de la racine et de fonctionner comme des routeurs. La deuxième amélioration permet aux noeuds en mode "non stockage" d'envoyer des messages DAO saut par saut, contrairement à ce qui se passe dans RPL, où les noeuds en mode "non stockage"

n'envoient des messages DAO qu'à la racine. Tandis qu'à la troisième et la quatrième améliorations suggèrent des modifications dans les champs du message DAO et des adaptations dans leur traitement pour les noeuds en mode "stockage" et "non stockage". De ce fait, le message DAO peut être entièrement et correctement compris par les deux modes, évitant ainsi des problèmes d'ignorance des champs. La cinquième amélioration modifie un indicateur à l'intérieur du message DAO pour indiquer si la racine DODAG utilise ou non le mode de stockage. Les informations de cet indicateur doivent être enregistrées dans la table de routage des noeuds en mode de stockage pour optimiser la construction des routes descendantes. Cependant, l'interopérabilité entre les MoP de RPL peut entraîner des boucles de routage et un partitionnement du réseau. Ainsi, bien que la proposition atteigne une livraison de paquets identique aux scénarios MoP homogènes à travers des simulations et des environnements réels, la taille du réseau n'est limitée qu'à 25 noeuds (problème du passage à l'échelle).

Une autre solution qui permet l'utilisation interopérable de différents MoP sur RPL est proposée par [218] où les auteurs visent à améliorer la prise en charge du protocole RPL avec différents trafics. Après avoir réalisé plusieurs expériences avec le protocole RPL, les auteurs ont identifié une dégradation des performances du protocole RPL dans des scénarios à trafic descendant. Par conséquent, l'extension proposée nommée "Diverse Traffic-RPL (DT-RPL)" fournit une communication bidirectionnelle entre les noeuds du réseau en mettant à jour la qualité des liens à travers le trafic ascendant et descendant. Dans le fonctionnement du RPL par défaut, les noeuds ne mettent à jour leur qualité de lien qu'avec un paquet ascendant. En utilisant DT-RPL, les paquets descendants transportent des informations sur la qualité de lien dans un espace réservé spécifique à l'intérieur de l'en-tête MAC IEEE 802.15.4. Ainsi, le récepteur d'un paquet descendant calcule la qualité du lien et met à jour ses informations sur son parent en participant à une accélération des mises à jour de la table de routage. Ainsi, DT-RPL rend possible l'utilisation de différents modèles de trafic et contribue également à l'augmentation du taux de livraison des paquets.

Pour surmonter le problème existant dans RPL lié à la charge lourde et dynamique des réseaux, les auteurs dans [219] ont proposé une extension du protocole RPL appelé RPL contextuel et d'équilibrage de charge (Context Aware and Load Balancing RPL (CLRPL)). Le protocole vise à réduire le taux de perte de paquets et à augmenter la durée de vie du réseau LLN avec un débit élevé et un trafic très variable. Le protocole CLRPL est divisé en trois parties. La première réside dans une OF composée nommée Context aware Objective Function (CAOF) qui calcule le rang de chaque noeud en fonction de : ETX entre le noeud et son parent, l'énergie résiduelle du noeud et le rang du parent. Après avoir calculé le rang de chaque expéditeur de message DIO sur la base des informations stockées, CAOF utilise un algorithme pour trier les noeuds par rang du meilleur au pire. Ainsi, le message DIO avec le meilleur classement est diffusé en premier pour éviter le phénomène de troupeau tonitruant [219]. La deuxième partie est la métrique de routage contextuelle CARF qui utilise des informations afin d'obtenir une valeur utilisée lors de la sélection de parent. La troisième partie est un mécanisme de sélection de parent en choisissant celui avec la valeur inférieure calculée par CARF. Quand deux parents candidats aient la même valeur CARF, le mécanisme sélectionne le parent avec le plus petit nombre de noeuds fils. Ainsi, en tenant compte de la charge de travail des chemins ainsi que des informations sur l'énergie et la qualité de la liaison, CLRPL peut réduire la consommation d'énergie et

améliore le taux de perte de paquets.

L'inconvénient des approches d'interopérabilité présentées est qu'un noeud ne peut pas basculer dynamiquement entre les MoP de RPL.

c) Améliorations de RPL en mode de stockage

Cette partie des améliorations est constituée d'un ensemble de techniques de gestion des tables des voisins. Ces techniques décrivent des politiques d'insertion et de remplacement d'entrées dans les tables de routage RPL afin de mieux gérer les informations des tables des voisins et compte tenu de la limitation de la mémoire des noeuds. En détaillant plus, chaque routeur dans RPL en mode stockage doit maintenir l'état de routage de tous les noeuds dans son sous-arbre (sous-DODAG) [62]. En effet, sachant que dans un réseau LLN à ressources limitées, un noeud routeur (avec ces capacités contraignantes) peut échouer facilement d'ajouter une entrée de routage pour une telle destination en raison de ses limitations de stockage en mémoire. Par conséquent, tous les paquets dirigés vers cette destination seront perdus à cause de l'inaccessibilité de cette dernière, ce qui va impacter considérablement l'évolutivité de RPL.

Dans ce contexte, plusieurs études ont essayé de résoudre ce problème de surcharge de la mémoire d'un réseau en mode stockage. D-RPL [220] a été proposé afin de réduire les besoins en mémoire du MoP de stockage de RPL. D-RPL utilise la multidiffusion au lieu de l'algorithme de transfert RPL normal dans le cas où la limite de la mémoire d'un noeud est atteinte, i.e. chaque noeud diffuse un paquet descendant si la destination n'est pas incluse dans sa table de routage. Par conséquent, cette technique permet la livraison des paquets descendants avec une table de routage de petite taille. Cependant, les auteurs ne fournissent aucun résultat expérimental pour évaluer les performances de la multidiffusion. Une autre approche qui vise à traiter le problème de la limitation de mémoire est présentée dans [194] où les auteurs proposent une extension de RPL à mémoire efficace (Memory Efficient storing mode in RPL (MERPL)). L'idée principale de MERPL est le fait qu'un noeud, dont les entrées de routage atteignent un seuil prédéterminé (N), devrait déléguer un fils dans son sous-DODAG pour agir comme source de stockage. Par la suite, le noeud surchargé doit supprimer depuis sa table de routage toutes les entrées de routage dont le prochain saut est bien ce fils délégué. Ensuite, toutes ces destinations accessibles via le fils délégué doivent être annoncées à la racine du DODAG dans un message DAO distinct. Les résultats de comparaison de MERPL avec RPL indiquent que MERPL réduit en effet les exigences de stockage, en particulier au niveau des noeuds proches de la racine. La longueur moyenne du chemin dans MERPL est également plus courte que celle dans RPL en mode sans stockage, mais légèrement plus longue qu'en mode avec stockage.

Dans le même contexte, les auteurs dans [221] ont présenté une version améliorée de RPL appelée Enhanced-RPL afin de réduire le problème de forte limitation de stockage pour les tables de routage des parents préférés. En d'autres termes, Enhanced-RPL résout le problème de destination inaccessible causé par une surcharge du parent préféré de certains noeuds. Dans la norme RPL plus précisément dans le mode de routage descendant, une fois qu'un noeud fils veut annoncer son préfixe, un message DAO est envoyé à son parent préféré. Cependant, lorsque la table de routage du parent est pleine, elle n'accepte aucun nouveau noeud (problème de scalabilité). Le protocole est basé sur un mécanisme DAO-NACK permettant aux noeuds rejetés de rechercher un autre parent. En effet, Enhanced-RPL propose une liste de parents candidats au noeud fils qui a perdu la

chance de s'annoncer à son parent préféré.

En effet, nous avons de même contribuer à résoudre ce problème de stockage mémoire en proposant une amélioration du protocole RPL nommée "Optimized RPL (Opt-RPL)" [222] qui vise à réduire le nombre de messages de contrôle en vérifiant la mémoire des noeuds, en particulier, les nouveaux noeuds qui souhaitent rejoindre le réseau. En plus de la restriction du stockage mémoire des noeuds, ces derniers consomment plus d'énergie pendant le processus de construction du réseau. Par conséquent, l'avantage de la réduction des messages de contrôle se reflétera sur de nombreuses exigences de QoS ; ce qui a été expérimenté par le protocole Opt-RPL en fournissant de meilleures performances par rapport au standard RPL en termes d'overhead et de consommation énergétique.

d) Améliorations des OFs & Métriques combinées

Dans RPL [62], il n'y a aucune obligation d'utiliser une OF bien spécifique ou un ensemble de contraintes. Il est donc possible de manipuler la fonction d'objectif par défaut et ses paramètres. Cette opportunité permet une flexibilité sur le choix des paramètres de routage d'OF. Ainsi, *RFC 6551* a proposé un ensemble de contraintes de routage à utiliser dans RPL, mais elle n'a pas décrit ni exigé comment les choisir ni comment les combiner [62]. En outre, l'*IETF* a défini deux OFs initiales *OF0* [187] et *MRHOF* [223] comme des OFs par défaut dans le protocole standard RPL qui peuvent répondre à des exigences de routage simples. Par conséquent, la définition correcte de l'OF est en fonction des besoins et des exigences de l'application, qui restera toujours un problème chaud et ouvert dans le cadre du protocole RPL. Ainsi, plusieurs travaux ont proposé des OFs alternatives pour RPL prenant en compte différentes métriques de routage.

Certaines approches ne proposent pas une OF complètement nouvelle, mais améliorent la façon dont les rangs des noeuds sont calculés, introduisant ainsi une nouvelle métrique de routage. Dans [224], les auteurs ont proposé une métrique composite additive appelée "Lifetime and Latency Aggregatable Metric (L2AM)". L2AM vise à fournir une consommation d'énergie équilibrée tout en considérant la fiabilité de la transmission de données. À cette fin, la métrique de routage proposée est une fusion de la métrique (*ETX*) avec une nouvelle métrique de consommation d'énergie appelée "Fully Simplified Exponential Lifetime Cost (FSELC)". Lorsqu'un noeud doit envoyer un paquet vers la racine, il doit sélectionner le chemin avec le coût le plus faible de L2AM. Dans une autre approche [225], les auteurs ont présenté une OF sensible à la QoS qui fonctionne avec une logique floue appelée "Objective Function Fuzzy Logic (OF-FL)". Dans cette approche, la QoS combine quatre métriques de routage principales (délai de bout en bout, nombre de sauts, qualité de la liaison et l'énergie du noeud) pour fournir une décision de routage configurable basée sur des paramètres flous dans le but de supporter diverses exigences d'application. A travers des simulations, les auteurs ont comparé OF-FL avec *OF0* et *MRHOF* en démontrant que l'approche OF-FL équilibre la consommation d'énergie sans dégrader les performances de livraison des paquets. La même approche a été suivie dans [226]. Une autre OF à base de la logique floue appelée FUZZY OF a été introduite dans [227] où la proposition visait à fusionner différentes métriques de routage pour optimiser la QoS et la consommation d'énergie. La fonction d'objectif FUZZY OF combine trois métriques de routage, qui sont le délai, *ETX* et l'énergie afin d'obtenir une quatrième valeur appelée qualité qui représente le coût du chemin. Différent de l'OF-FL présenté précédemment, FUZZY OF obtient la qualité d'un chemin en utilisant deux processus de fuzzification.

En effet, la fonction d'objectif OF proposée permet à RPL de construire une topologie de routage tenant compte à la fois de la QoS et des aspects énergétiques. Dans le même contexte dans [228], les auteurs ont également adopté des systèmes flous pour concevoir un nouvel ensemble de fonctions d'objectifs contextuelles pour RPL. Ils ont défini quatre fonctions d'objectifs sensibles à la qualité de la livraison et au contexte (DQCA-OF) en tenant compte des métriques : *ETX*, l'énergie consommée et le nombre de sauts (HC). Ils ont également proposé un système flou pour combiner alternativement les métriques des DQCA-OF. Ainsi, pour chaque DQCA-OF existe un DQCA-OF (FL) qui fusionne les métriques de routage en utilisant le système flou proposé pour classer les routes. Par conséquent, un ensemble de huit OFs qui peuvent être choisies dynamiquement en fonction des exigences de l'application IoT pour améliorer la consommation d'énergie et la QoS.

Un autre type de fonctions d'objectifs développées pour une implémentation du protocole RPL dédié pour les LLNs agricoles (A-LLN) est présenté dans [229]. La fonction d'objectif "A Scalable Context-Aware Objective Function (SCAOF)" introduit des fonctionnalités contextuelles dans RPL pour répondre aux exigences de la QoS dans les A-LLN. L'OF proposée combine des métriques comme la métrique du lien de couleur de liaison (LCO) et une métrique additive composée d'*ETX* et de l'énergie restante (RE). Pour sélectionner son parent préféré, un noeud fils recherche ses parents avec le LCO approprié, ensuite, il choisit celui avec la deuxième métrique la plus basse (composée d'*ETX* et de RE). Ainsi, le noeud doit calculer son rang sur la base d'*ETX* et de RE et le transmettre ensuite à ses voisins. Dans [230], les auteurs ont proposé un protocole appelé "Parent Aware Objective Function (PAOF)". PAOF permet d'offrir un équilibrage de la charge réseau pour les réseaux LLN. Il combine d'une manière lexicale à la fois *ETX* et le nombre de parents pour effectuer la sélection des parents préférés. Ainsi, bien que PAOF considère deux métriques de routage, la décision principale est basée sur l'*ETX*, tandis que la deuxième métrique est utilisée juste en cas de différence significative entre les valeurs *ETX* des noeuds candidats.

Dans une autre combinaison de métriques, les auteurs dans [231] ont proposé une extension du protocole RPL basée sur des métriques composites économes en énergie dans les LLNs. Cette OF proposée est composée de plusieurs paramètres : l'énergie résiduelle (RER), l'indice de décharge de la batterie (BDI), et la métrique ETX. Cette amélioration évite l'épuisement de la batterie près du noeud récepteur afin de transférer les données depuis la source vers la destination.

Ainsi, dans ce même contexte, nous avons suggéré une combinaison des deux métriques principales (ETX et ENG) du protocole RPL dans [232], en considérant à la fois la fiabilité et la consommation énergétique. Cette combinaison a dévoilé des résultats encourageants en termes de taux de paquets délivrés, de taux de perte de paquets, de consommation énergétique, et de durée de vie du réseau IoT.

e) Gestion de la mobilité

L'un des inconvénients évidents du protocole standard RPL est le manque de prise en charge de la mobilité. Par conséquent, plusieurs travaux se concentrent sur la proposition des solutions d'intégration du concept de la mobilité.

Les auteurs de [233] ont proposé une version améliorée de RPL pour les réseaux ad hoc de véhicules (VANETs). Ils ont inclus l'information géographique en tant que nou-

velle métrique afin de prédire la direction des noeuds et de les sélectionner comme parents préférés pour minimiser le nombre de dissociations et de reformation des DODAG. Cependant, ce protocole est testé uniquement pour la collecte de données avec un seul CH qui collecte des données à partir de noeuds routiers statiques indépendamment des exigences de l'application et en supposant que le noeud mobile ne change pas de direction. En outre, les auteurs dans [209] ont proposé une analyse de RPL sous la mobilité à l'aide de l'algorithme inverse de '*Trickle*'. Selon leur proposition, les noeuds mobiles sont préconfigurés avec un indicateur de mobilité et sont configurés pour agir en tant que noeuds feuilles pour s'assurer qu'ils ne participent pas dans le processus de construction du DODAG. Lorsqu'un noeud mobile se connecte à un DODAG, il définit le minuteur de *Trickle* sur la valeur maximale et la diminue périodiquement jusqu'à ce qu'il atteigne la valeur minimale ou se déplace vers un autre parent. Cependant, cette approche suppose qu'il y a toujours un noeud statique à portée de tout noeud mobile. Elle nécessite également l'utilisation de paramètres différents pour les noeuds statiques et mobiles, ce qui la rend moins flexible. En plus, ce protocole n'a pas de schéma de détection de mobilité et il utilise plutôt différents paramètres d'entretien pour les noeuds mobiles. Une autre extension de RPL avec mobilité est étudiée par [186] en introduisant un mécanisme appelé Corona dans RPL (Co-RPL). Les auteurs ont introduit deux améliorations principales du protocole, la première est basée sur le principe Corona dans lequel le réseau est divisé en Coronas circulaires autour de la racine DODAG. Ce principe permet aux noeuds de trouver un parent alternatif plus rapidement sans avoir à reformer le DODAG. Quant au deuxième principe offre une fonction d'objectif basée sur la logique floue (FL-OF) qui utilise le délai de bout en bout, le nombre de sauts, la qualité de la liaison et l'énergie résiduelle comme métriques de routage. Ce protocole permet d'obtenir un PDR plus élevé, moins de délai de bout en bout et une meilleure consommation d'énergie en comparaison avec le RPL standard. Cependant, ce protocole est conçu pour les noeuds se déplaçant à des vitesses basses pouvant atteindre 4 m/s et il ne s'adresse pas à un réseau hybride avec un modèle de mobilité dynamique.

Une autre amélioration de RPL conçue pour les applications médicales [234] présente une évaluation du protocole RPL pour les réseaux hybrides avec des noeuds mobiles et statiques. Les auteurs n'apportent aucune amélioration au RPL lui-même, mais obligent plutôt les noeuds mobiles à agir comme des noeuds terminaux qui, selon les spécifications du RPL, ne peuvent pas s'annoncer comme des routeurs et n'envoient pas de messages DIO avec les paramètres de l'OF. Cette approche améliore la stabilité du réseau en permettant aux noeuds mobiles de se connecter au DODAG mais pas d'agir en tant que noeud parent ni de participer à la formation du DODAG. Le problème avec cette approche est qu'elle suppose qu'il y a toujours un noeud fixe à portée de tout autre noeud. En outre, elle n'ajoute pas d'amélioration à la conception de RPL mais évalue plutôt son utilisation dans le scénario donné.

De plus, une version mobile de RPL appelée mRPL a été proposée dans [235] pour gérer la mobilité dans les environnements IoT. Ce protocole vise à améliorer le temps "handoff" pour les noeuds mobiles en ajoutant quatre temporisateurs à l'algorithme *Trickle* d'origine afin de détecter les noeuds déconnectés par une approche intelligente et rapide. Ce protocole est comparé au standard RPL dans différents scénarios de simulations et les résultats obtenus ont montré que mRPL surpasse le standard RPL en termes de PDR, d'overhead et de délai. Un test pratique est également effectué à l'aide de noeud

"Tmote-Sky" et les résultats étaient similaires à ceux fournis par la simulation. Cependant, mRPL s'appuie fortement sur les valeurs "Average Received Signal Strength Indicator (ARSSI)", et néglige les autres mesures, ce qui entraîne des transferts inutiles et parfois l'établissement de liens avec moins de fiabilité. Ce protocole est testé pour un seul noeud mobile se déplaçant à une vitesse constante (2 m/s) près de neuf noeuds statiques et ne considère pas plus d'un noeud mobile ou de noeuds se déplaçant à des vitesses plus élevées. Ainsi, une extension de mRPL nommée mRPL++ dans [236], qui représente une version "Smarter-HOP" de mRPL pour optimiser la mobilité dans RPL. Cette extension inclut l'OF dans le processus de sélection des parents pour s'assurer que les noeuds sont conscients des métriques autres que RSSI. En plus, mRPL++ améliore la prise de décision en utilisant le produit de l'ARSSI et le rapport entre les coûts des métriques dans l'OF des noeuds parents concurrents. Cependant, ce protocole souffre toujours des points faibles de mRPL et dépend toujours du RSSI de sorte qu'il ne peut pas être négligé quelle que soit l'OF.

Toujours dans le même contexte, les auteurs dans [237] ont présenté une stratégie de routage appelée "Kalman positioning RPL (KP-RPL)" en fournissant un routage robuste pour les RCSFs avec des noeuds statiques et mobiles. Chaque noeud mobile crée une liste initiale des noeuds statiques se trouvant dans sa portée de transmission et selon le RSSI, il liste ceux avec une faible *ETX* en les considérant comme des "liens potentiellement non fiables". Ce protocole améliore la fiabilité du réseau de 25% selon les résultats de la simulation. Cependant, il suppose qu'un seul noeud mobile se déplace à portée d'un certain nombre de noeuds statiques et ne prend pas en compte les noeuds mobiles supplémentaires. KP-RPL s'appuie également sur le positionnement pour estimer la position du noeud mobile et établit sur cette base une liste noire. Par conséquent, une localisation inexacte peut entraîner une grave dégradation du réseau en affectant la décision de routage en plus de cela, les liens fiables peuvent également être mis sur la liste noire.

Une autre étude [238] où les auteurs ont amélioré le fonctionnement du RPL dans les environnements mobiles avec des exigences dynamiques en proposant le protocole D-RPL pour le routage multi-sauts dans les applications IoT dynamiques. D-RPL utilise certaines fonctionnalités de mRPL en plus d'une minuterie adaptative qui fonctionne comme une minuterie inversée de '*Trickle*' lorsqu'une mobilité est détectée. Il inclut également des métriques de routage dans la prise de décision afin de minimiser le nombre de transferts inutiles. Cette conception a également été étendue en proposant un RPL mobile basée sur la théorie des jeux "Game-Theory based Mobile RPL (GTM-RPL)" [239] pour optimiser les performances de RPL dans un environnement mobile où les noeuds mobiles concourent pour les ressources du réseau et visent à atteindre une solution "Nash Equilibrium (NE) pour la gestion des ressources. Les résultats ont prouvé une amélioration des performances du protocole RPL en termes de consommation d'énergie et de délai de bout en bout. L'avantage de GTM-RPL est que même dans un environnement mobile, les noeuds peuvent couvrir de grandes surfaces et communiquer de manière efficace et fiable. Cependant, les dispositifs IoT hétérogènes ont des capacités de calcul différentes et utilisent différentes technologies de communication avec des comportements différents. Par conséquent, les solutions "NE" conventionnelles peuvent ne pas convenir à un environnement IoT pratique.

Dans le but de fournir un support mobile aux réseaux LLNs avec un trafic très dynamique, les auteurs dans [240] ont proposé l'extension appelée "Backpressure RPL (BRPL)".

Il est le premier protocole de routage pour les LLNs qui fusionne RPL et les concepts de routage 'backpressure' [241] qui fournit un support à la mobilité. Il permet l'utilisation de plusieurs topologies logiques (plusieurs DAG) qui peuvent être créées en fonction de différentes fonctions d'objectifs. Cependant, contrairement à RPL, chaque noeud dans BRPL conserve une file d'attente de paquets tamponnés pour chaque DAG. Dans le transfert de paquets, le poids de liaison de chaque voisin est calculé en tenant compte à la fois de sa valeur de rang et de la longueur de la file d'attente. La stratégie dynamique de BRPL permet d'obtenir une réduction significative de la perte de paquets au détriment d'une augmentation du délai de bout en bout.

Un protocole de routage économe en énergie et sensible à la mobilité basé sur RPL a été présenté dans [242] nommé EMA-RPL. Ce protocole prend en considération les réseaux de faible puissance composés de noeuds statiques et mobiles. Il peut réduire l'utilisation de l'énergie et des ressources de calcul des dispositifs mobiles. Cependant, dans un scénario de mobilité dense et élevé, EMA-RPL peut surcharger les noeuds statiques et réduire les performances du réseau. En outre, EMA-RPL exige plusieurs changements dans la structure des messages de contrôle RPL, ce qui peut rendre l'interopérabilité de "EMA-RPL" difficile avec d'autres approches et la mise en oeuvre RPL standard. Nous terminons avec une autre solution de routage pour la prise en charge des noeuds mobiles dans les LLNs proposée par [243]. Cette approche est basée sur le filtre de Kalman étendu appelé "Extended Kalman Filter for Mobile RPL (EKR-MRPL)". EKF-MRPL accorde une attention particulière au mouvement des noeuds mobiles. Cette proposition est divisée en trois phases : détection de mouvement, réaction et notification. EKF-MRPL réduit le nombre de changements de parents préférés et contribue à la réduction de l'utilisation des messages de contrôle grâce à son mécanisme de prédiction de mouvement. Par conséquent, le protocole aide à diminuer la consommation d'énergie et à augmenter le taux de livraison des paquets.

Une étude récente [244] suggère "Mobility Aware RPL (MARPL)" afin d'améliorer ses performances dans les réseaux à noeuds mobiles. MARPL propose un mécanisme de mobilité utilisant une approche multicouche (acquérir des informations depuis la couche liaison de données et la couche réseau pour fournir un support de détection de mobilité). MARPL est composé de trois mécanismes : (i) la détection de la mobilité des voisins ; (ii) la détection de l'indisponibilité des parents préférés et (iii) le réglage de la transmission des messages de contrôle via l'algorithme '*Trickle*'.

f) Qualité de service (QoS)

La transmission fiable de données représente une exigence dans la plupart des applications IoT. Cette dernière est satisfaite en minimisant les paquets perdus, en maximisant le débit et en évitant les longs délais. Par conséquent, une QoS réalisable est considérée comme une caractéristique la plus cruciale pour tous les protocoles de routage dédiés aux réseaux LLNs. Bien que RPL satisfasse largement aux exigences des réseaux LLNs, plusieurs problèmes restent ambiguës et manquent d'amélioration, en particulier répondre aux exigences de la QoS des différents applications IoT.

Notamment dans [245], les auteurs ont proposé une OF nommée QoS_RPL. Ils ont utilisé un algorithme de colonie de fourmis (ACO) cherchant à mieux répondre aux exigences d'efficacité énergétique et de QoS dans les réseaux LLNs. Ils ont utilisé des métriques de routage sensibles à l'énergie et aux délais pour rendre RPL plus économe en énergie.

QoS_RPL peut atteindre une diminution du délai de bout en bout ainsi que l'énergie consommée. Néanmoins, le taux de livraison des paquets a montré une légère réduction par rapport à RPL utilisant la métrique *ETX*. Cependant, cela nécessite une vérification supplémentaire dans un scénario réel.

Ainsi dans une autre approche pour détecter les défaillances d'une liaison, les auteurs de [246] proposent l'algorithme (Pro-RPL) qui compte le nombre de paquets perdus et utilise un seuil pour supposer si une liaison est défaillante ou non. Le protocole proposé essaie de minimiser les messages de contrôle et la consommation d'énergie en surveillant les tendances de défaillance des noeuds du réseau. Les résultats de simulation ont indiqué que ce protocole améliore le PDR et l'efficacité énergétique, cependant, l'absence d'une méthode plus rapide pour détecter les pannes s'avère nécessaire pour améliorer sa réactivité.

D'autres contributions introduisent des techniques de multidiffusion pour améliorer la fiabilité du routage [247, 248]. Ces études proposent les protocoles suivants : "Stateless Multicast RPL Forwarding protocol (SMRF)", "Enhanced SMRF (ESMRF)", et "Bidirectional Multicast RPL Forwarding protocol (BMRF)" pour contrôler les messages multicast dans RPL. Les résultats de l'expérience montrent que ces protocoles ont le potentiel de surpasser l'algorithme '*Trickle*'. Bien qu'ils garantissent une plus grande fiabilité, cette amélioration de la fiabilité se traduit par un coût élevé de consommation d'énergie et de délai.

Un protocole appelé "Coopérative-RPL (C-RPL)" est présenté dans [249] qui utilise une stratégie coopérative pour les noeuds avec différentes applications de détection afin d'économiser l'énergie tout en réduisant les coûts. En effet, les noeuds dans différentes instances sont chargés de transmettre différentes données afin de réduire la consommation d'énergie par rapport à RPL standard. Dans une autre contribution [250], les auteurs ont développé une nouvelle implémentation multicouche de RPL, visant à améliorer la fiabilité de la transmission des données. La solution proposée, nommée RPLca+, est composée de deux bibliothèques spécialisées. La première pour l'estimation de la qualité des liens et la seconde pour la gestion des tables des voisins. Ces techniques décrivent des politiques d'insertion et de remplacement d'entrées dans les tables de routage visant à mieux gérer les informations des voisins. De plus, l'implémentation proposée fournit un mécanisme de synchronisation entre les tables des voisins pour améliorer la cohérence des informations stockées.

De plus, les auteurs dans [251] ont dérivé de la fonction d'objectif conventionnelle du RPL une fonction minimale avec (*MRHOF*). Cette nouvelle OF est appelée OFQS. Elle permet de supporter l'approche multi-instance pour être conforme avec RPL. OFQS est basée sur des métriques multi-objectifs prenant en compte le délai et l'énergie restante des noeuds ainsi que la qualité de la liaison. Dans [252], les auteurs ont mesuré les performances de RPL en termes des paramètres de QoS tels que le taux de livraison des paquets, le temps de convergence du réseau, l'énergie restante, la latence et la surcharge du trafic de contrôle. Ces mesures de QoS ont été effectuées à l'aide du simulateur Cooja et de l'analyseur de réseau Wireshark. Dans E-RPL [253], les auteurs ont présenté une OF multi-contraintes pour RPL. Plusieurs propriétés de QoS ont été utilisées comme métriques telles que le délai et l'énergie, dans lesquelles un protocole RPL amélioré pour l'environnement IoT. E-RPL améliore la consommation d'énergie et le délai de bout en bout par rapport aux OFs existantes (*OF0* et *MRHOF*).

g) RPL sécurisé

Les applications IoT devraient avoir l'intégrité, la confidentialité, la disponibilité, la confidentialité, l'authentification et la confiance. Il existe de nombreuses attaques qui peuvent facilement cibler les noeuds de capteurs en tirant parti de la relative simplicité de leur matériel, en recherchant un gain en exploitant leurs données ou simplement en bloquant leurs services. Du point de vue du routage, la sécurité reste l'un des principaux problèmes lors de l'évaluation des performances du réseau [254]. Les problèmes de sécurité sont généralement mieux couverts dans les recherches dédiées telles que [200, 255–258].

Selon la norme RPL définie dans la *RFC 6550*, il existe trois modes de sécurité :

- Non sécurisé : Les messages de contrôle sont envoyés sans prendre en considération la sécurité.
- Préinstallé : Les noeuds utilisent une clé préinstallée afin de rejoindre un réseau.
- Authentifié : Les noeuds utilisent une clé préinstallée pour rejoindre le réseau en tant que noeud feuille, ensuite les noeuds demandent un message d'authentification qui leur permet de fonctionner en tant que routeurs.

Une attaque "Déni de Service (DoS)" qui force le minuteur '*Trickle*' à se réinitialiser en provoquant des incohérences dans le DODAG et provoque une boucle de reformation du DODAG ainsi qu'une réparation globale. Ce type d'attaques empêche les noeuds de gérer les paquets de données en leur privant de leur énergie. Le standard *IETF* propose dans la norme *RFC* d'utiliser un seuil pour le nombre de réinitialisations par heure de ce minuteur [259]. Cette solution ne résout pas le problème des paquets de données perdus mais au moins, elle limite l'énergie gaspillée pour la reformation du DODAG une fois le seuil atteint. Cette idée a été améliorée dans une autre contribution dans [260] en proposant un seuil adaptatif qui dépend des conditions du réseau et du type d'attaques. La stratégie montre une amélioration significative des performances en termes de consommation d'énergie. De plus dans [261], les auteurs ont suggéré un système de détection d'intrusion (IDS) pour détecter les problèmes d'attaques de 'black hole' et de 'grey hole' où les noeuds malveillants abandonnent silencieusement tout ou une partie des paquets de données. L'algorithme détecte les noeuds malveillants en surveillant le nombre de messages DIO, la perte de paquets et les délais. Selon leurs résultats, cette approche empêche avec succès les noeuds malveillants de participer au processus de formation des DODAG. En outre, l'étude dans [262] implique qu'une surcharge élevée est ajoutée au réseau en raison des noeuds de surveillance ajoutés. Cependant, les résultats montrent que cette approche atténue le problème des attaques par numéro de version et présente une solution évolutive avec le potentiel d'identifier et de localiser un attaquant ou un groupe d'attaquants.

Une attaque DAO interne, i.e. un noeud malveillant transmettant de faux messages DAO, est un problème de sécurité très sérieux dans RPL. Afin de faire face à ce type d'attaques, une étude plus récente [263], propose une extension du protocole RPL nommée SecRPL. Dans SecRPL, un noeud parent maintient un compteur correspondant aux messages DAO transmis par chacun de ses noeuds fils. Si l'un des compteurs des fils dépasse la valeur de seuil prédéfinie, le parent ne transfère pas le message DAO suivant provenant du fils.

Dans une autre étude [264], un modèle basé sur la confiance est présenté afin de sécuriser le protocole RPL. Dans ce modèle, un noeud sélectionne un chemin de transfert de données sur la base de l'indicateur d'intensité du signal reçu et de la valeur de confiance.

Toujours dans le même contexte, afin d'atténuer l'effet des attaques de sécurité comme "Miraibitnet", les auteurs dans [265] suggèrent un protocole de routage RPL sécurisé et évolutif "Secure and scalable RPL routing protocol (SPLIT)" pour les réseaux IoT. SPLIT utilise une technique d'attestation à distance légère pour garantir l'intégrité logicielle des noeuds du réseau, garantissant ainsi leur bon comportement. Pour éviter une surcharge supplémentaire causée par les messages d'attestation, le processus SPLIT se superpose aux messages de contrôle du protocole RPL. Le schéma proposé garantit que les dispositifs n'utilisent aucun logiciel malveillant pour la communication et le traitement des données.

Le tableau 2.1 présente un résumé des différentes catégories d'améliorations du protocole RPL ainsi que leurs principaux avantages et inconvénients en termes de mise en oeuvre et de performances.

TABLE 2.1 – Taxonomie des différentes améliorations du protocole RPL sous différents contextes

Contexte	***Protocoles***	***Techniques***	***Avantages***	***Inconvénients***
Efficacité Énergétique	Lamaazi et al. [210]	Utilise l'énergie comme métrique	- Inclut *ETX* comme métrique - Envisage des scénarios mobiles	Aucune amélioration de RPL
	SEEOF [211]	Utilise des métriques combinées	- Améliore la durée de vie - Considère les applications industrielles	- Aucun test pratique - Mobilité non prise en compte
	Kamgueu et al. [212]	Utilise l'énergie résiduelle comme métrique	Améliore la durée de vie	- Ne prend pas en compte d'autres mesures de routage - Aucun test pratique
	multiELT-RPL [213]	- Utilise plusieurs parents - Calcule la durée de vie attendue des noeuds - Utilise RPL à chemins multiples	- Augmente la durée de vie des noeuds - Estime la qualité des liens	- Mobilité non prise en compte - Augmente l'utilisation de la mémoire - Modifie la structure des messages de contrôle RPL
	Khan et al. [214]	Coordination entre les noeuds racines	- Considère plusieurs sinks - Améliore le débit et la durée de vie	- Aucune expérience pratique - Mobilité non prise en compte - Incompatible avec la norme RPL
	EE [215]	Équilibrage énergétique basé sur RDC	Améliore l'équilibrage de charge et le débit	- Amélioration marginale par rapport au *MRHOF* - Mobilité non prise en compte
	RAME [216]	Routage et agrégation pour un minimum d'énergie	Améliore la durée de vie	- Limite le débit - Mobilité non prise en compte

Interopérabilité entre les MoP de RPL	DualMOP-RPL [217]	Active l'utilisation des MOP stockés et non stockés dans un seul réseau RPL	Résout le problème d'interopérabilité entre les deux MOP	- Augmente la complexité du traitement des messages de contrôle - Modifie la structure des messages de contrôle
	DT-RPL [218]	Permet une mesure bidirectionnelle de la qualité des liens	- Améliore les performances RPL lors d'une communication orientée vers le bas - Ne nécessite pas de changements importants dans RPL	- Ne prend pas en compte de l'énergie pour l'équilibrage de charge - Non adapté pour le passage à l'échelle
	CLRPL [219]	Crée de nouveaux mécanismes pour prendre en compte les informations sur la charge de travail des noeuds	- Implique l'énergie et la qualité des liens dans la sélection des parents - Réduit les changements du parent préféré - Réduit la consommation d'énergie et augmente le PDR	- Nécessite de la mémoire et un tri des messages - Peut augmenter le délai de bout en bout
Améliorations du stockage MoP et compatibilité avec l'IoT	D-RPL [220]	Utilise le multicast pour surmonter le problème de mémoire en mode de stockage	Résout la limitation de mémoire	- Complexité causée par le multicast
	Memory efficient RPL (MERPL) [194]	Combine les modes sans stockage et stockage pour les décisions de transfert dans le sens descendant	Résout le problème de la mémoire et des en-têtes longs	- Problème de définition du facteur prédéterminé N
	Enhanced-RPL [221]	Un noeud peut distribuer des préfixes appartenant à son sous-réseau entre plusieurs parents	- Surmonter les limitations des capacités de stockage des noeud parents - favorise la fiabilité de RPL	Evalué seulement avec le modèle du disque unitaire (UDGM)
Améliorations des OFs & Métriques combinées	L2AM [224]	OF basée sur l'énergie et *ETX*	- Compatible avec RPL par défaut - Mise en oeuvre facile - Améliore la durée de vie	- PDR n'est pas étudié
	OF-FL [225]	OF basée sur des systèmes flous qui combinent le délai, *ETX*, l'énergie du noeud et le nombre de sauts	- Décisions de routage sont prises en tenant compte des différents aspects du réseau - Améliore le délai, la durée de vie du réseau et PDR	- Le système flou a un impact sur la mémoire - Aucune expérience pratique - Favorise la mobilité limitée
	FUZZY OF [227]	OF basée sur des systèmes flous qui combinent l'énergie, le délai et *ETX*	- Réduit le PDR - Réduit le délai	- Le système flou a un impact sur la mémoire - Mobilité non prise en compte - Les métriques de routage ne sont pas optimisées

	DQCA-OF [228]	- Ensemble d'OF basé sur *ETX*, nombre de sauts et consommation d'énergie combinés à l'aide de systèmes flous	- Peut changer ses fonctionnalités en temps d'exécution pour répondre aux exigences de routage - Améliore la QoS du réseau	- Le système flou a un impact sur la mémoire - Nécessite une connaissance préalable des applications
	SCAOF [229]	- OF basée sur l'énergie, la qualité du lien et *ETX*	- Évaluation des performances réalisée dans un banc d'essai - Prolonge la durée de vie du réseau - Augmente la fiabilité et l'efficacité du réseau	- Approche complexe - Nécessite une version étendue de RPL
	PAOF [230]	- OF lexical composite basé sur le numéro du parent et *ETX*	- Répartition de la charge de travail des noeuds - Augmente la durée de vie du réseau	- Ne prend pas en compte l'énergie des noeuds
Gestion de mobilité	Tian et al. [233]	- Inclut la position des noeuds comme métrique. - Utilise une minuterie adaptative	- Améliore le PDR et le délai dans les VANETS	- Suppose que les noeuds ne changent pas de direction - Ne prend pas en compte les scénarios dynamiques
	Cobarzan et al. [209]	Utilise l'algorithme inverse du *Trickle* pour les noeuds mobiles	- Réduit le temps de déconnexion - Améliore le PDR	- Pas de système de détection de mobilité - Nécessite des paramètres différents pour les noeuds mobiles
	Co-RPL [186]	Solution de routage basée sur le mécanisme Corona	- Présente un mécanisme alternatif à la récupération de chemin - Améliore le PDR, le délai et l'energie	- Nécessite des modifications dans les messages de RPL - Nécessite l'extension de la table de routage - Gestion de la mobilité limitée
	Mod-RPL [234]	Configuration des noeuds mobiles en tant que "feuilles"	- Améliore la stabilité et l'efficacité énergétique	- Aucune amélioration de RPL - Favorise la mobilité limitée (les noeuds mobiles ne sont pas utilisés comme routeurs) - Seuls les noeuds mobiles lents sont pris en compte
	mRPL [235]	- Qualité des liens (RSSI) - Minuteries supplémentaires	- Améliore la gestion de la mobilité - Améliore le PDR - Envisage des scénarios dynamiques - Code source disponible	- Par besoin de l'algorithme *Trickle* par utilisation des minuteries périodiques - Augmente le nombre de messages de contrôle
	mRPL++ [236]	Intègre le mécanisme smart-Hop avec RPL	Plus grande flexibilité	- Aucune amélioration de mRPL - OF dépend toujours du RSSI

	KP-RPL [237]	Utilise le filtre Kalman et de la liste noire	(i) Utilise des techniques de localisation (ii) Améliore le PDR	- Sensible à une localisation inexacte - Grande consommation d'énergie
	Dynamic RPL [238]	Minuterie adaptative et DIS adaptatif	- Améliore le PDR, l'efficacité énergétique et le délai - Overhead faible	Amélioration marginale dans les scénarios de faible mobilité
	GTM-RPL [239]	Implique de la théorie des jeux	- Améliore le PDR, l'efficacité énergétique et le délai - Les noeuds peuvent couvrir de grandes surfaces et communiquer de manière fiable	Les solutions peuvent ne pas convenir à un environnement IoT pratique
	BRPL [240]	- Combine RPL avec des concepts de routage 'backpressure' pour distribuer les ressources réseau de manière adaptative	- Réduit le PDR - Peut coexister dans un réseau exécutant déjà RPL par défaut	- Augmente le délai
	EMA-RPL [242]	- Implique RSSI pour prédire le mouvement des noeuds mobiles -Favorise le changement du parent préféré	- Réduit l'utilisation de l'énergie et les ressources de calcul des noeuds mobiles - N'utilise pas un matériel supplémentaire pour la détection de la mobilité	- Les noeuds mobiles n'acheminent pas les paquets - Nécessite d'autres champs sur les messages de contrôle RPL standard
	EKF-RPL [243]	Utilise le filtre de Kalman étendu pour prédire le mouvement des noeuds et réduire les changements des parents	- Réduit les messages de contrôle et la consommation d'énergie - les noeuds mobiles sélectionnent le parent qui peut offrir un temps de liaison plus long	- Peut augmenter le délai - Ne considère pas l'énergie et la qualité du lien lors de la sélection des parents
	MARPL [244]	Adopte une approche multicouche.	- Augmente le PDR et minimise l'overhead - Présente une amélioration de la minuterie RPL	Augmente le délai de reconnexion après une déconnexion d'un lien
QoS	QoS_RPL [245]	Métrique de routage composite basée sur le délai, l'énergie restante et la quantité du phéromone (ACO)	- Améliore la durée de vie - Estime la qualité des liens sur plusieurs chemins - Réduit la consommation d'énergie	- Ne tient pas compte de la mobilité - Aucune expérience pratique - Diminue le PDR - Augmente l'overhead
	Pro-RPL [246]	Détecte la rupture des liens	(i) Utilise des métriques combinées (ii) Améliore la durée de vie	- Ne prend pas en compte la mobilité - Aucune expérience pratique
	ESMRF [247]	Renvoi RPL multicast sans état amélioré	- Améliore la fiabilité - PDR et délai améliorés	- Augmente la consommation d'énergie - Incompatible avec le RPL natif

	BMRF [248]	Transfert RPL multidirectionnel bidirectionnel	- Améliore la fiabilité - Considère le trafic bidirectionnel - Paramètres réglables	- Augmente la consommation d'énergie et le délai - Besoin élevé en mémoire
	C-RPL [249]	Interaction coopérative entre les instances RPL	- Améliore la fiabilité et la consommation d'énergie - Faible coût de mise en oeuvre - Considère plusieurs OFs	Aucun support de mobilité
	RPLca+ [250]	Approche multicouche pour l'estimation de la qualité des liens et la gestion des tables de routage	- Fournit un estimateur de qualité de lien dynamique - Fournit les politiques de gestion des tables de routage - Améliore le PDR	- Présente des messages de contrôle de mise en oeuvre - Augmente la consommation d'énergie
RPL sécurisé	Hui et al. [259]	Limiter les réinitialisations du minuteur '*Trickle*' à l'aide d'un seuil fixe	- Améliore l'efficacité énergétique - Améliore la stabilité du DODAG en cas d'attaques DoS	- Diminue le débit - N'utilise pas les fonctions de sécurité RPL
	Mayzaud et al. [260]	Limite les réinitialisations de minuteur '*Trickle*' à l'aide d'un seuil adaptatif	- Améliore l'efficacité énergétique - Améliore la stabilité du DODAG en cas d'attaques DoS	- Messages de contrôle supplémentaires - N'utilise pas les fonctions de sécurité RPL
	SVELTE [261]	Utilise l'IDS pour créer des listes blanches et noires	- Isole les noeuds malveillants - Améliore la confiance du réseau	- Overhead important - N'utilise pas les fonctions de sécurité RPL
	Mayzaud et al. [262]	Architecture de surveillance distribuée	- Atténue les attaques par numéro de version - Localise l'attaquant - Solution évolutive	- Overhead important - Coût de déploiement élevé - N'utilise pas les fonctions de sécurité RPL
	SecRPL [263]	Propose un mécanisme pour faire face à l'attaque de falsification DAO	- Atténue l'impact de l'attaque de falsification DAO - Restreindre le nombre de messages DAO transférés selon la destination	- Augmente la consommation d'énergie, overhead et le délai - Dégrade la fiabilité du réseau
	SPLIT [265]	Utilise une technique d'attestation à distance légère	Améliore la sécurité surtout pour l'attaque avec rang et l'attaque Sybil	- Messages de contrôle supplémentaires - La connectivité du réseau n'est pas prise en compte - Les facteurs de performance tels que la consommation d'énergie ne sont pas validés

2.5 Conclusion

Dans ce chapitre, une classification des protocoles de routage dans l'écosystème IoT a été proposée en fonction de la topologie, des contraintes et de sécurité. Ensuite, une focalisation sur le protocole RPL en présentant sa définition et son impact sur les protocoles de routage, en particulier dans les réseaux LLNs. Une discussion plus approfondie a été menée sur ce protocole en termes de sa manière de construction de la topologie du réseau, l'OF, son rang, ses différents modes de transmission ainsi que les métriques de routage prédéfinies. Le chapitre a fini par classer les approches proposées dans la littérature pour toutes les améliorations du protocole RPL. Ensuite, nous avons conclu les avantages et les inconvénients des différentes améliorations selon différents points de vue en les regroupant dans un tableau récapitulatif. Cette récapitulation nous a bien aidé de façonner nos questions de recherche en proposant notre amélioration de ce protocole RPL ; qui est détaillées dans le troisième chapitre.

Le chapitre suivant présente une nouvelle solution pour le protocole RPL qui vise à équilibrer le trafic compte tenu d'un trafic gourmand notamment des contenus multimédias au sein d'un réseau contraint exigeant une qualité de service.

Chapitre 3

Algorithme de routage fiable satisfaisant la QoS pour l'IoMT

Chapitre 3

Algorithme de routage fiable satisfaisant la QoS pour l'IoMT

3.1 Introduction

De nos jours, notre environnement a connu une croissance explosive des dispositifs intelligents, principalement appelés objets intelligents qui peuvent interagir avec l'environnement physique et communiquer avec d'autres objets via Internet dans le monde appelé "Internet des objets" (IoT) [45, 266]. Ces objets physiques peuvent affecter considérablement notre vie grâce à leur capacité de communiquer avec d'autres dispositifs tels que les capteurs, les actionneurs, les téléphones portables, les dispositifs domotiques et les dispositifs de réseau intelligent [8, 267]. Avec la même définition que le système IoT, l'internet des objets multimédias (IoMT) est considéré comme une interconnexion d'objets multimédias dans laquelle ils peuvent acquérir des contenus multimédias depuis le monde réel en se basant sur des dispositifs multimédias [94]. En outre, avec la croissance de ce type de dispositifs intelligents, la tendance des applications IoMT est récemment devenue beaucoup plus importante en s'impliquant dans de nombreux domaines tels que les maisons intelligentes, la santé intelligente, les véhicules intelligents, les villes intelligentes...etc. Cette diversité peut apporter de nouvelles exigences plus strictes que celles de l'environnement IoT, principalement en raison de l'augmentation du contenu multimédia dans le réseau. Le contenu multimédia peut être définit comme une combinaison de deux ou plusieurs contenus multimédias différents tels que du texte, de l'audio, de l'image, de la vidéo...etc. [94], en donnant un mélange d'applications en temps réel et en temps non-réel. Par exemple, certaines caméras de surveillance dans une maison intelligente enregistrent simultanément des images et du son ou un scénario vidéo complet de ce qui se passe. Des études récentes qui ont noté une augmentation éminente du flux de trafic multimédia, indiquent que ce dernier, en particulier le type vidéo, domine considérablement le trafic IP sur internet [50]. Ce type de trafic appelé par [268] communications multimédias à grand volume de données "Big Volume of Data (BVD)" dans l'IoMT est considéré comme une tâche complexe à gérer surtout avec un réseau à ressources limitées.

En outre, les communications sans fil sont connues par certaines limitations telles que la bande passante, des unités de traitement limitées, la consommation d'énergie...etc. [269]. En plus de ces contraintes, les flux multimédias imposent plus de charge qui dépasse la capacité des dispositifs d'IoT à satisfaire une bande passante, un espace mémoire et une

énergie plus élevée [270]. La projection de ces exigences dans les protocoles de routage entraîne la nécessité d'avoir un protocole de routage efficace qui supporte les mécanismes de QoS des applications IoMT. Par conséquent, la plupart des protocoles de routage proposés dans l'IoT ne semblent pas adéquats pour satisfaire les contraintes multimédias en raison de l'exigence stricte des paramètres de QoS tels que la bande passante, le délai et le taux de perte de paquets [271]. Parmi ces protocoles, nous citons le protocole RPL qui est bien connu dans les réseaux IoT, mais peu de recherches ont tenté de l'améliorer objectivement pour les applications IoMT. Plusieurs problèmes restent ouverts afin d'améliorer certains protocoles de routage qui garantissent l'ensembles d'exigences de QoS des réseaux contraints.

Un défi important pour la prise en charge des applications multimédias dans l'IoT est la limitation de la bande passante [272]. La bande passante disponible estimée dans la plupart des travaux repose sur la mise en oeuvre d'un protocole à QoS en utilisant une conception multicouche. En d'autres termes, la couche MAC estime la bande passante disponible le long des chemins et la couche de routage achemine les informations en fonction de la bande passante requise par les applications [273]. Ainsi, la bande passante disponible peut être utilisée pour analyser les performances du réseau, car elle peut être utilisée comme une contrainte pour les applications qui nécessitent une large bande passante en améliorant la QoS des flux multimédias et le streaming vidéo sur un réseau [274]. De plus, elle a été abordée dans de nombreuses études antérieures. Pourtant, à notre connaissance, aucune implémentation de fonction d'objectif RPL n'a été proposée pour calculer la bande passante effective dans la couche réseau. Par conséquent, et après avoir été inspiré sur la façon dont il est important de savoir si un chemin peut fournir suffisamment de bande passante libre avant d'acheminer un flux multimédia.

Dans ce travail, nous concevons une nouvelle fonction d'objectif à QoS basée sur la bande passante libre dans une version améliorée du protocole RPL appelée FreeBW-RPL [275]. Notre protocole de routage proposé choisit un parent préféré en considérant l'espace libre de la bande passante maximale "Bandwidth (BW)" autour de son voisinage pendant tout le chemin du routage dans le réseau (depuis le noeud source au noeud destinataire). L'optimisation FreeBW-RPL est basée sur les exigences de la surveillance d'une maison intelligente dans le but de générer un flux de données volumineux. De plus, FreeBW-RPL répartit la charge de trafic dans le réseau et emprunte de manière dynamique plusieurs chemins pour acheminer le trafic lourd en créant des chemins équilibrés en terme d'énergie.

Dans ce chapitre, nous présentons un protocole de routage proactif RPL **basé sur l'estimation** de bout en bout **de la bande passante libre** pour un prototype d'Internet des réseaux multimédias. Après des simulations intensives, nous avons conclu que le protocole FreeBW-RPL maintient le meilleur chemin de transfert de données multimédias en le comparant aux fonctions d'objectifs par défaut du protocole RPL.

3.2 Étude des performances du protocole RPL dans les réseaux IoT

Avant d'avoir passer au domaine multimédia, nous avions évalué les performances du protocole RPL afin d'étudier les différentes lacunes confrontées par ce protocole envers

les ressources limitées du réseau IoT.

Premièrement, nous avons suggéré une métrique composite dans le protocole RPL qui prend en considération à la fois la fiabilité et la consommation énergétique. Ce travail tente d'évaluer cette combinaison des deux métriques principales (ETX et ENG) [232] en améliorant la fonction d'objectif MRHOF. Nous avons remarqué une amélioration des performances du réseau et de sa durée de vie. Grâce à plusieurs simulations, on a obtenu des résultats encourageants pour la métrique proposée, principalement en termes de taux de livraison de paquets (Packet Delivery Ratio (PDR)), de taux de perte de paquets et de consommation d'énergie par rapport aux schémas les plus populaires pour RPL : ETX et énergie.

De plus, en mode de stockage du protocole RPL, chaque routeur doit stocker des chemins pour les destinations dans son sous-DODAG. Cette fonctionnalité fait un facteur limitant dans RPL, qui est la mémoire disponible pour stocker les voisins dans les tables de routage. En plus, les noeuds proches de la racine doivent stocker l'état de routage pour presque tout le "DODAG", ce qui peut être très exigeant surtout pour les dispositifs à ressources limitées. En effet, la norme RPL n'a pas défini d'actions à entreprendre pour un parent refusant d'ajouter une nouvelle route descendante lorsque sa table de routage est pleine.

Deuxièmement, nous avons proposé une amélioration du protocole RPL nommée "Opt-RPL" [222] qui réduit le nombre de messages de contrôle en vérifiant la mémoire des noeuds qui se rejoignent nouvellement dans le réseau. Notre proposition traite le problème de stockage mémoire, en particulier, les nouveaux noeuds qui souhaitent rejoindre le réseau en consommant progressivement de la mémoire. Hormis, la limitation de stockage mémoire des noeuds, ces derniers se trouvent obligés de consommer plus d'énergie pendant le processus de construction du réseau. Par conséquent, l'avantage de la réduction des messages de contrôle se reflétera sur de nombreuses exigences de QoS ; ce qui a été expérimenté par le protocole Opt-RPL en fournissant de meilleures performances par rapport au standard RPL en termes d'overhead et de consommation d'énergie.

3.3 Revue de la littérature des améliorations du protocole RPL dans le domaine multimédia

Plusieurs problèmes sont encore ouverts pour plus d'amélioration et de spécification dans l'IoMT. Ainsi, le routage d'un contenu multimédia à l'aide du protocole RPL dans un environnement requis tel que les réseaux IoMT reste une tâche difficile en raison de la difficulté à respecter certains niveaux de QoS. De plus, la transmission de ce type de données contraints est plus gourmande en bande passante lorsqu'on la compare au trafic de données scalaires conventionnels dans les réseaux IoT [50]. Considérant RPL comme un protocole de routage pour l'IoT, il se caractérise par sa flexibilité pour ne pas restreindre les métriques de routage ni les réglages de paramètres pendant le processus de sélection des chemins de routage [62]. En d'autres termes, le groupe de travail IETF ROLL n'a nécessité aucune utilisation spécifique de la fonction d'objectif, ce qui rend le protocole RPL hautement adaptable selon les exigences de l'application et du réseau pour les systèmes IoMT.

Certaines approches ont proposé d'autres améliorations du protocole RPL afin de

répondre aux défis imposés par les réseaux IoMT tels que [98]. Dans [98], les auteurs ont proposé une version améliorée du protocole RPL nommée Green-RPL dans laquelle ils ont visé à minimiser les émissions de l'empreinte carbone et la consommation d'énergie en garantissant les exigences de QoS. Le protocole Green-RPL repose sur un ensemble de métriques utilisées le long du chemin vers la racine qui sont le délai, la consommation de l'énergie et les types de sources d'énergie. Les résultats de la simulation ont montré que le protocole Green-RPL surpasse OF0 en termes d'efficacité énergétique et de nombre de transmissions de paquets réussies, et que ETX surpasse le protocole Green-RPL en termes d'efficacité énergétique mais pas en nombre de transmissions réussies des paquets. Une autre amélioration du protocole RPL qui considère l'énergie restante des noeuds lors du routage du trafic IoT est proposée dans [276]. Le protocole proposé a été comparé au protocole RPL basé sur ETX. Les résultats expérimentaux ont indiqué une amélioration en termes de durée de vie du réseau, tandis que le protocole proposé consommait presque la même quantité d'énergie que RPL basé sur ETX.

Les applications IoMT nécessitent la satisfaction de la bande passante en tant que contrainte de QoS. Dans ce contexte, de nombreuses solutions de routage inter-couches ont été proposées dans la littérature [273, 277–281]. Dans ces solutions, la couche réseau extrait des informations utiles de la couche MAC sur la bande passante disponible et, en retour, le noeud source peut facilement adapter son débit de transmission. De plus, certains travaux sur les réseaux IoMT ont inclus une communication inter-couches basée sur les couches physique, de liaison de données, de réseau et d'application. Le protocole de routage proposé dans [277] présente une forte hétérogénéité en plus de sa capacité à choisir le chemin de routage optimal qui échange des données multimédias. De plus, ils ont inclus l'aspect de sécurité afin de pouvoir reconnaître les données authentifiées. Un mécanisme d'estimation de la bande passante a été utilisé dans le protocole AODV pour obtenir un nouveau protocole de routage satisfaisant la QoS nommé Adaptive QoS-Aware Ad-hoc On-demand Distance Vector (AQA-AODV) [278]. Ce protocole repose sur les mécanismes d'estimation de la bande passante disponible pour les liaisons et les chemins. En outre, il contient un schéma adaptatif qui peut aider le noeud source d'être informé de l'état actuel du réseau et dont le but principal est d'ajuster le débit de transmission en fonction des exigences de la QoS de l'application.

Les auteurs de [273] ont proposé un schéma d'estimation de la capacité de liaison basé sur une nouvelle estimation passive de la bande passante disponible en prenant en compte les informations de "back-off" et de retransmission. De plus, les auteurs de [279] ont proposé un protocole de routage à la demande appelé M-QoS-AODV dans un réseau MANET multicanal basé sur un schéma distribué d'attribution de canal. Dans [280], les auteurs ont proposé un contrôle d'admission basé sur le routage AODV qui prend en charge la QoS (QoS-aware AODV routing-based Admission Control (QAODV-AC)) permettant une coopération entre les couches : MAC IEEE 802.11 et la couche réseau (plus particulièrement le protocole de routage AODV-QoS). La variation du débit de saturation du MAC IEEE 802.11 est prise en compte comme valeur d'estimation de la bande passante disponible. Une autre technique proposée par [281] qui inclut les paramètres de la couche MAC IEEE 802.11 dans le calcul de la bande passante.

Dans une autre étude la bande passante a été considérée comme une exigence à atteindre afin de bénéficier de la consommation totale d'énergie [282]. Dans cette étude, les auteurs ont proposé un routage multi-chemins coopératif (Clustering based Multi-Path

Routing algorithm for improving the reliability in WSNs (CMPR)) afin d'optimiser la consommation d'énergie tout en garantissant la contrainte de bande passante. Ainsi, ils ont conçu un algorithme CMPR heuristique qui construit un routage multi-chemin coopératif des noeuds disjoints et à faible consommation d'énergie. Une amélioration du protocole RPL appelée "Power Controlled RPL (PC-RPL)" a été proposée dans [283]. PC-RPL contrôle de manière adaptative la topologie de routage via la puissance de transmission et le seuil d'indication de la force du signal reçu (RSSI) des noeuds afin d'améliorer la bande passante délivrée et l'équité en atteignant un meilleur débit.

Les recherches susmentionnées dépendent largement de certaines informations utiles extraites de la couche MAC afin d'estimer la bande passante disponible. Par conséquent, cela peut entraîner une dégradation des performances du réseau, comme la quantité énorme de surcharge causée par les messages échangés entre les différentes couches, l'utilisation croissante des ressources énergétiques et les failles de sécurité. Cependant, à notre connaissance, aucune de ces recherches n'a utilisé l'estimation de la bande passante libre au niveau de la couche réseau, en tant que fonction d'objectif de base dans le protocole RPL. Exceptionnellement dans [280] où l'idée de FreeBW a été implicitement recherchée mais elle n'a pas été discutée d'une manière détaillée car elle n'était pas dédiée au protocole RPL ni au processus de routage multimédia IPv6. Notre protocole amélioré proposé FreeBW-RPL est dédié au routage des informations détectées à partir d'un environnement IoMT, sans dépendre des informations collectées à partir de la couche MAC.

3.4 Protocole FreeBW-RPL

La condition du canal idéal a été mise en évidence dans certaines recherches telles que [284]. Lors de sa comparaison avec la bande passante du canal brute, les auteurs ont conclu qu'elle ne peut pas être saturée par le débit maximal qui peut encore être bien en dessous de la capacité maximale de bande passante. Par contre, elle peut dépendre de manière significative sur le changement moyen de la longueur du paquet pendant la transmission. Par conséquent, à partir de ce résultat, nous pouvons déduire que l'estimation efficace et la bonne gestion de la bande passante au niveau de la couche réseau doivent prendre en compte la quantité de paquets envoyés.

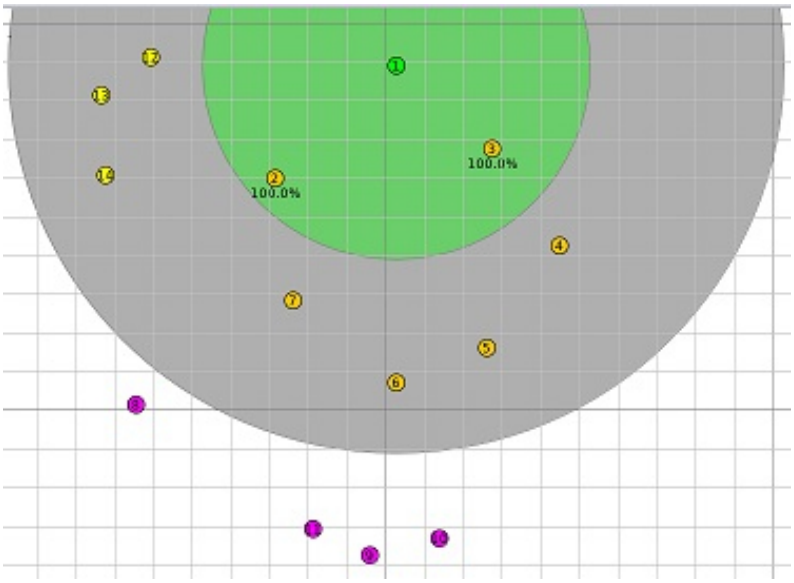
Dans cette section, nous discutons l'amélioration de notre protocole FreeBW-RPL en donnant plus d'informations sur le scénario de réseau et la fonction d'objectif proposée.

3.4.1 Modèle du réseau

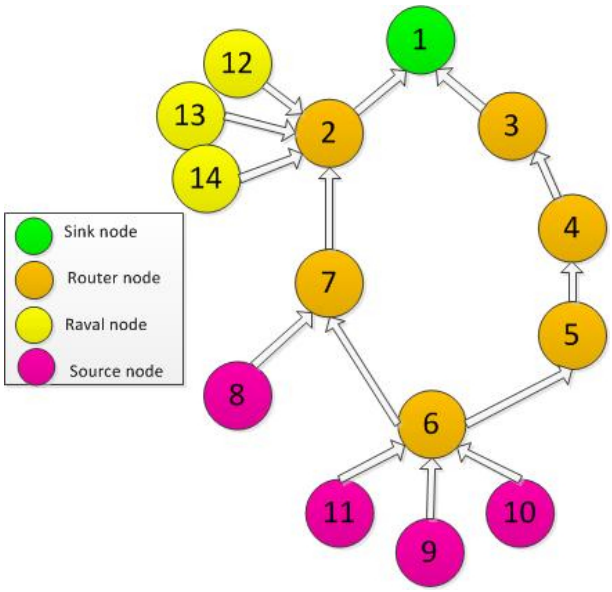
Nous considérons un réseau statique IoMT avec un nombre fixe de noeuds (14 noeuds), y compris la racine DAG, où les noeuds RPL sont organisés comme montre la Figure 3.1b. La racine est convenablement considérée comme un noeud statique et elle est liée à la passerelle Internet. Les noeuds du réseau exécutent le protocole FreeBW-RPL, plus précisément le routage des données repose sur la fonction d'objectif proposée FreeBW.

3.4.2 Fonction d'objectif à QoS basée sur la bande passante

La métrique "bande passante" au niveau de la couche réseau, signifie que la bande passante allouée entre les différents noeuds du réseau fournie pour un service IoMT. Dans



(a) Déploiement des noeuds



(b) Réseau généré

FIGURE 3.1 – Scénario du processus de routage

notre proposition, nous respectons le concept général du calcul de la bande passante au niveau des couches basses (inférieures) telles que la couche MAC. Dans lequel, dans la conception QoS, il est considéré que tout service contraint nécessite une bande passante élevée dans chaque lien entre les différents noeuds du réseau. En effet, toute transmission de paquet peut avoir un impact sur la bande passante disponible en réduisant la quantité de bande passante libre dans ce lien. Par conséquent, nous proposons le protocole FreeBW-RPL en créant une nouvelle fonction d'objectif (OF) nommée "bande passante libre" (Free Bandwidth). L'idée principale est de trouver un chemin optimal en sélectionnant la bande passante libre maximale au long du chemin reliant la source à la racine. Nous illustrons dans les Figures 3.2a and 3.2b un exemple pour la sélection de la bande passante dans

l'ensemble du chemin de routage. Une fois que le noeud (C) ou (D) souhaite envoyer un message DIO, il doit choisir la valeur minimale entre sa valeur de bande passante et la valeur de son parent afin de garder une trace de cette valeur minimale pour les noeuds descendants. Une fois que le noeud (E) reçoit ce message DIO des deux noeuds (C et D) avec deux valeurs minimales différentes (3 et 2) respectivement, il doit prendre la valeur de bande passante maximale entre eux et la sélectionner comme Best_parent. Par la suite, lors de l'opération d'envoi (diffusion du message DIO), le noeud (E) enverra finalement le message DIO mis à jour aux voisins avec la valeur maximale de la bande passante libre reçue tout au long du chemin portant comme valeur 3, comme illustré dans la Figure 3.2b.

La valeur de la bande passante libre est calculée en fonction de l'équation 3.1 où le débit de liaison $Link_{Rate}$ dépend des caractéristiques du noeud et représente la quantité totale de paquets pris en charge par le canal, et le débit d'envoi $Send_{Rate}$ représente l'utilisation de la bande passante pendant le processus de routage. De plus, l'algorithme 4 illustre le calcul de la bande passante libre (décrit dans la section 4.3).

$$Free\ Bandwidth = Link_{Rate} - Send_{Rate} \tag{3.1}$$

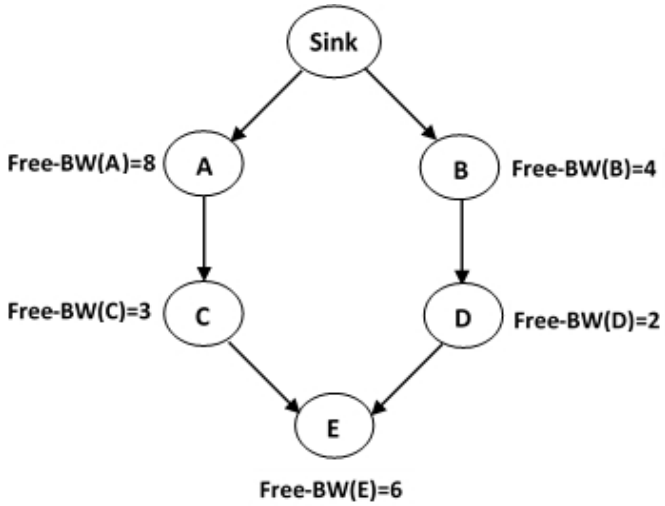
De plus, nous avons essayé dans notre scénario proposé (représenté sur la Figure 3.3) de saturer le noeud 2 en mettant 3 noeuds émetteurs afin de voir comment sera le choix du chemin de routage sélectionné par chacun des OF : ETX, Energy, None et notre FreeBW-OF proposé. Comme illustre la Figure 3.3, une fois que le chemin choisi par les OF par défaut est congestionné, FreeBW-OF choisi celui qui est non congestionné en passant au chemin de couleur bleue et en choisissant un autre parent préféré. Ainsi, nous pouvons déduire que notre FreeBW-OF proposé dépend d'un choix de chemin multiples pendant le processus de routage en donnant plus d'équilibre de charge au réseau.

3.4.3 L'algorithme du FreeBW-RPL

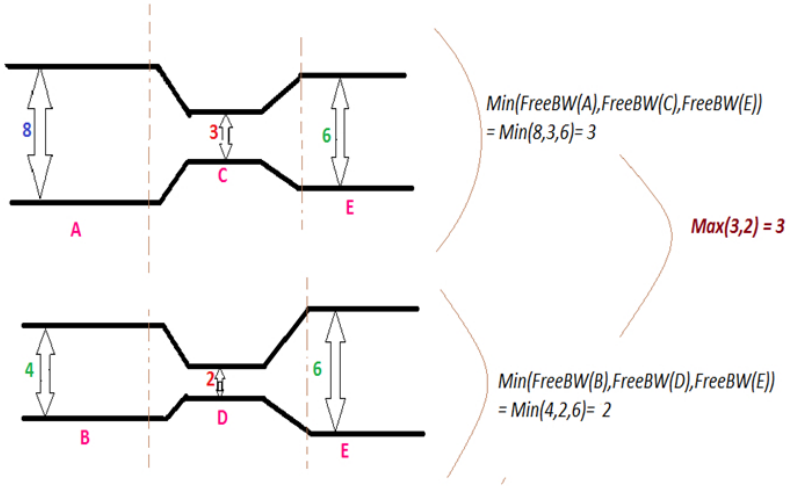
Le protocole FreeBW-RPL inclut un nouveau mécanisme qui calcule la bande passante libre de manière distribuée. Chaque routeur RPL est en écoute des messages DIO provenant des noeuds voisins. Ensuite, il traite les paramètres DIO tels que OF et parent_rank. Lorsqu'un routeur RPL reçoit le premier message DIO, il ajoute l'ID de l'expéditeur DIO à la liste des parents et sélectionne directement l'expéditeur comme meilleur parent. Sinon, il rejoint le parent qui fournit la bande passante libre la plus élevée sur tout le chemin du parent sélectionné au récepteur. Ensuite, il calcule son rang en utilisant la fonction d'objectif Free-BW. Avant l'opération de diffusion du message DIO "mis à jour", le noeud émetteur doit comparer sa propre valeur minimale de FreeBW à celle déjà maximisée (FreeBW du meilleur parent). Finalement, ces nouveaux paramètres seront transmis dans le nouveau message DIO aux voisins. Ce processus est illustré dans l'algorithme 4.

3.5 Evaluation des performances du protocole FreeBW-RPL

Dans cette section, nous évaluons les performances du protocole de routage proposé.



(a) Sélection de la bande passante au long du chemin de routage



(b) Exemple de sélection de la bande passante

FIGURE 3.2 – Sélection de la bande passante

3.5.1 Environnement de travail

Nous avons évalué la performance du protocole FreeBW-RPL en implémentant son code sous le simulateur de réseau COOJA [92], afin d'illustrer l'impact de la nouvelle OF sur différents aspects des caractéristiques des systèmes IoMT. COOJA est considéré comme un émulateur car il teste exactement le code binaire d'une classe qui s'exécute sur des capteurs réels tels que les capteurs Z1 s'exécutant sous le système d'exploitation Contiki [71]. De plus, cela nous donne une flexibilité totale dans l'évaluation des environnements radio et des topologies. Pour le modèle de propagation radio, nous utilisons un modèle de graphe appelé Unit Disk Graph Model (UDGM) : distance loss [285].

Dans notre réseau de simulation, nous avons considéré deux scénarios. Dans le premier, nous avons inclus 14 noeuds sur un espace carré (100 m × 100 m), où le noeud 1 est un noeud racine situé au bord du réseau. Ainsi, dans le deuxième, nous avons implémenté la mise en échelle dans plusieurs scénarios de réseau comprenant de 10 à 50 noeuds dans

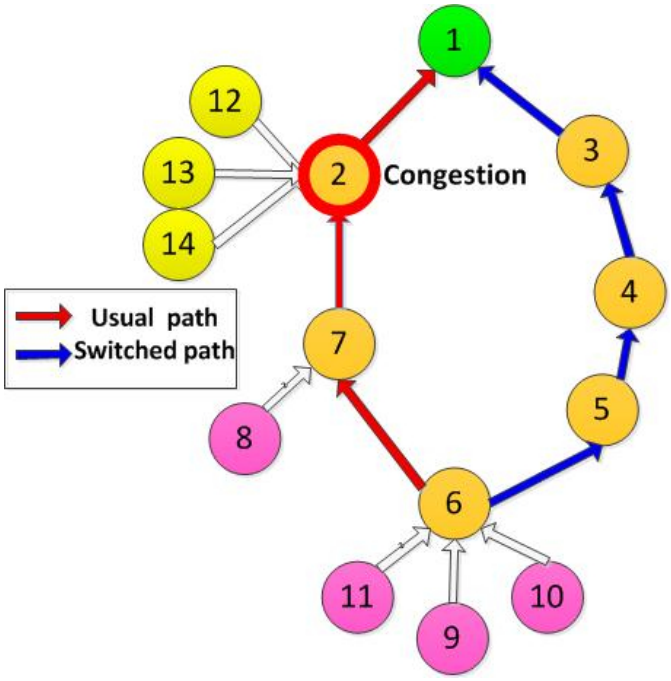


FIGURE 3.3 – Chemins choisis dans : ETX , ENERGY, NONE et FreeBW-OF

lesquels le nombre de noeuds sources varie de 3 à 10 noeuds. Les noeuds sont disposés comme illustré sur la Figure 3.1a. La portée de communication radio est de 50 m. Cinq débit de transmission de données, à savoir (1 pkt/s, 2 pkt/s, 3 pkt/s, 4 pkt/s et 5 pkt/s) ont été pris en compte dans la simulation avec une taille de données de 50 octets. Dans le deuxième scénario, nous avons varié la taille du réseau de 10 à 50 avec une taille de données de 100 octets et un débit de transmission de données de 5 pkts/s. Quand à la durée de simulation est à 300 s. Les autres paramètres de simulation sont résumés dans le tableau 3.1.

3.5.2 Métriques de performance

Nous évaluons les performances de routage des OFs par défaut du protocole RPL et de notre protocole proposé FreeBW-RPL en termes de taux de paquets délivrés (PDR), de délai de bout en bout, de débit et de consommation d'énergie.

- Taux de paquets délivrés (PDR) : Le PDR est défini comme le rapport entre le nombre de paquets reçus et le nombre de paquets envoyés.

- Délai de bout en bout : Le délai de bout en bout (délai de livraison des paquets) est une autre métrique d'évaluation utilisée pour mesurer le temps total pris par les paquets afin d'être livrés avec succès d'un noeud source au noeud récepteur (racine).

- Débit de données : Le débit est la quantité d'octets reçus par le noeud racine par rapport à la valeur totale du temps nécessaire pris par les paquets depuis le début d'envoi jusqu'à la fin de la simulation. Ces octets proviennent des paquets de données. Le débit est calculé comme suit :

Algorithm 4 Optimisation du protocole FreeBW-RPL

```
1 : Début
2 : /* Recevoir DIO */
3 : /* Traiter DIO ( obtenir les paramètres du message DIO) */
      - Candidate.path_metric = dio.path_metric
      - Candidate.parent_id = dio.node_id
4 : Si Best_parent == NULL Alors
5 :       /* Ajouter l'expéditeur DIO en tant que parent candidat */
6 :       Best_parent.path_metric = candidate.path_metric ;
7 :       Best_parent.id = candidate_parent.id
8 : Sinon
9 :       Diff = abs(Best_parent.path_metric − candidate.path_metric) ;
        /* Min_diff est utilisé pour maintenir la stabilité du choix du parent préféré */
10 :      Si (Dif f > Min_diff ) Alors
11 :            best_parent = Max(candidate.path_metric, Best_parent.path_metric) ;
12 :      Finsi
13 : Finsi
   /* Mettre à jour le paramètre DIO */
14 : dio.path_metric = M in(Best_parent.path_metric, FreeBW)
15 : dio.node_id = current_node.id
16 : Diffusion du DIO ;
17 : Fin
```

Table 3.1 – Paramètres de simulation

Paramètres	Valeurs
Simulateur de réseau	COOJA under Contiki OS (2.7)
Environnement radio	Unit disk graph medium (UDGM)
Noeuds émulés	Z1
Zone réseau	100 m × 100 m
Nombre de noeuds	10, 14, 20, 30, 40, 50
Nombre de noeuds racines	1
Nombre de noeuds sources	3, . . ., 10
Portée de transmission	50 m
Taille totale du Frame	127 bytes
Taille du paquet de données	(50, 100) bytes
Taux de trafic	1, 2, 3, 4 et 5 pkts/s
Durée de simulation	300 s

$$Throughput\ (KB/s) = \frac{\sum size\,(received_{packets}) * count\,(received_{packets})}{duration\,of\ simulation} \tag{3.2}$$

- **C**onsommation d'énergie : Afin de calculer la consommation d'énergie du réseau, nous utilisons une nouvelle technique du logiciel appelée Powertrace qui est un outil disponible dans Contiki [71]. Cet outil suit l'état de l'alimentation en estimant la consommation d'énergie pour le traitement CPU, la CPU en mode basse consommation, la transmission des paquets et l'écoute. De plus, le mécanisme de suivi de l'alimentation fournit des valeurs CPU, mode basse consommation (LPM), écoute radio et transmission radio, ce qui donne le temps total consommé dans chaque intervalle de trace de puissance. La consommation totale d'énergie est calculée selon l'équation 3.3. De plus, nous prenons le pourcentage moyen de radio représenté par la consommation d'énergie moyenne (APC) dans le temps de chaque type de noeuds (source, routeurs et serveurs) pendant toute la durée de vie du réseau selon l'équation 3.4.

$$Energy\,consumption = \sum_{i=1}^{n} (LPM + CPU + RadioListen + RadioTransmit) \tag{3.3}$$

$$APC = \frac{\sum_{i=1}^{n} (LPM + CPU + RadioListen + RadioTransmit)}{n} \tag{3.4}$$

  où n représente le nombre de noeuds.

- Énergie consommée par paquets reçus : Nous avons mesuré une nouvelle métrique d'évaluation en calculant l'énergie consommée pour la quantité totale des paquets reçus avec succès selon l'équation 3.5.

$$Energy\,consumed\,per\,packet = \frac{Power\,consumption}{Amount\,of\,packets\,succefully\,received} \tag{3.5}$$

3.5.3 Résultats de simulation et discussion

Afin d'étudier l'impact du débit de transmission de données sur le comportement du réseau, nous l'avons fait varier de 1 à 5 paquets par seconde en mesurant le PDR, le délai de bout en bout, le débit et la consommation d'énergie.

a) Taux de paquets délivrés (PDR)

Les résultats de simulation présentés par la Figure 3.4 montrent que le PDR de la nouvelle OF (FreeBW) est meilleur que celui des OFs du standard RPL (ETX, Energy et NONE). La raison principale est que le protocole FreeBW-RPL a un mécanisme plus efficace que le protocole RPL avec ses OF par défaut, dans lequel il évite le chemin encombré en commutant le chemin vers un nouveau noeud parent qui fournit un chemin

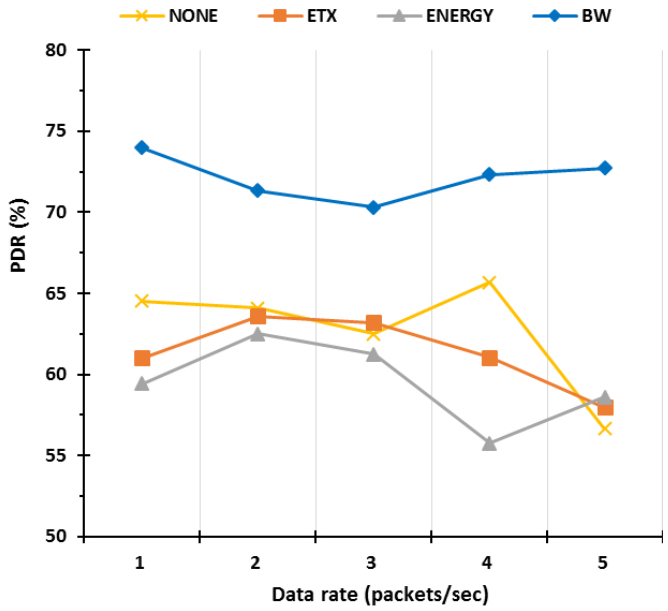


FIGURE 3.4 – Taux de livraison de paquets (PDR) vs Débit de données

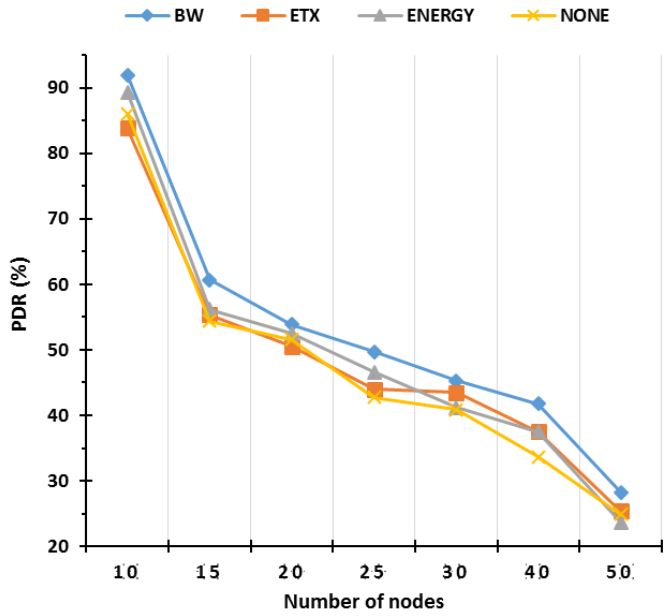


FIGURE 3.5 – Taux de livraison de paquets vs Nombre de nœuds avec débit de données = 5 pkts/s

avec un FreeBW plus élevé. Ce mécanisme permet au flux de paquets de trouver un chemin alternatif, gagner plus de chances d'être délivrés et de ne pas se chevaucher avec d'autres paquets circulant dans le chemin encombré conduisant à un taux de paquets délivrés. De plus, le protocole proposé avec FreeBW-OF est le protocole le plus efficace pour transférer des paquets avec une différence de taux PDR (11%, 12,5%, 9,5%) supérieure à ETX-OF, Energy-OF et None-OF respectivement déduisant qu'avec ce nouveau protocole FreeBW-RPL le réseau est plus fiable.

La Figure 3.5 illustre notre deuxième schéma qui comprend de 10 à 50 noeuds, en évaluant le PDR en termes de la taille du réseau (passage à l'échelle). Les OFs évaluées se comportent de la même manière en figurant par une diminution de PDR quand le nombre de noeuds augmente. Cela est dû à l'augmentation de la collision des paquets qui empruntent le même chemin. En donnant une chance aux paquets d'éviter le chemin encombré, le FreeBW-RPL fournit de meilleurs résultats en termes de PDR par rapport aux OFs par défaut.

b) Délai de bout en bout

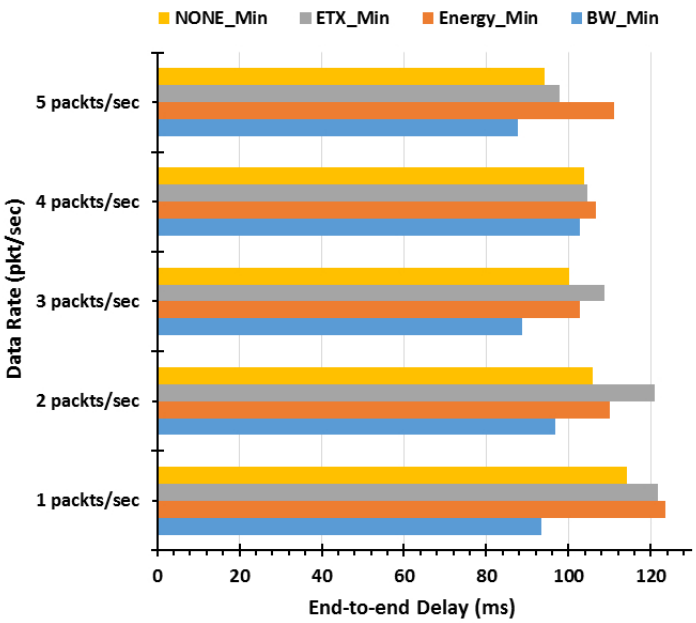


FIGURE 3.6 – Délai de bout en bout vs Débit de données

Comme illustre la Figure 3.6, le protocole RPL avec ses OFs par défaut (ETX, Energy et NONE) a le délai le plus élevé, car ils ne prennent pas en compte la BW libre, menant les paquets à parcourir le chemin encombré en prenant plus de délai dans la file d'attente afin d'être servis. Cependant, FreeBW-RPL a un délai inférieur à celui des OFs RPL par défaut, et ceci est principalement grâce au mécanisme de commutation de chemin utilisé par FreeBW-OF. Une fois que le noeud est confronté à un lien encombré, il essaie de trouver un autre parent afin de basculer le chemin vers un lien moins encombré. Par conséquent, le temps mis par un paquet source afin d'être transmis jusqu'au noeud récepteur en utilisant le protocole FreeBW-OF est inférieur à celui pris par les autres OFs. En effet, puisque toutes les OF (ETX, Energy et None) sont exécutées dans le même contexte en gardant le même chemin congestionné qui doit prendre plus de temps pour la transmission en entraînant un délai plus élevé. Dans les deux débits d'envoi (2 et 4 pkts/s), le délai de FreeBW-OF augmente, sinon le délai atteint ses valeurs minimales, ce qui fait que les débits de transmission de données (1, 3, 5 pkts/s) sont les meilleurs débits en termes de délai. Les OFs (ETX et Energy) ont le délai le plus élevé et pour les OFs globales, elles ont atteint leur délai minimum au débit de données (3 pkts/s).

c) Débit

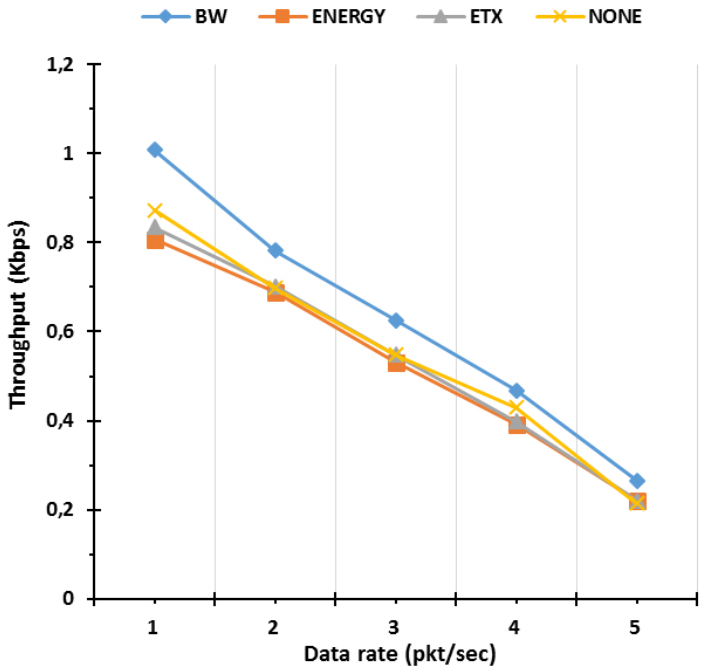


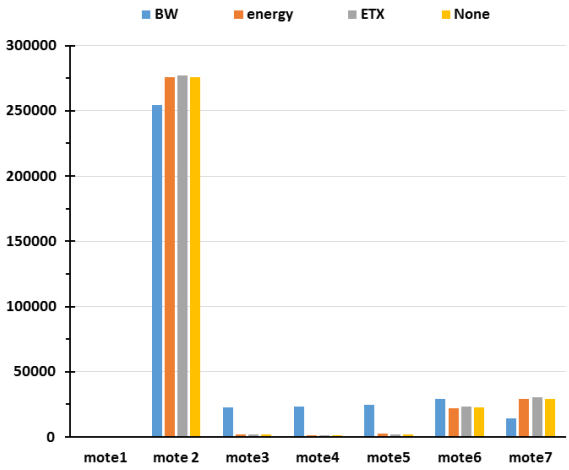
FIGURE 3.7 – Débit vs Débit de données

La Figure 3.7 montre l'un des principaux avantages de FreeBW-OF. FreeBW-OF garantit une augmentation du débit du réseau par rapport aux autres OFs (ETX, Energy et None). En effet, toutes les débits des OFs mesurées diminuent lorsque le débit de transmission des données augmente. Par conséquent, nous pouvons expliquer qu'avec l'augmentation du taux de paquets de données, il y a progressivement plus de paquets de données transmis dans le réseau, conduisant à une congestion du réseau et à une diminution du débit du réseau. Malgré cette baisse, la raison de la supériorité de l'avantage du débit donné par FreeBW-OF est que notre OF proposée soulage la congestion du réseau en trouvant un chemin alternatif moins encombré avec la bande passante libre maximale lors de l'envoi des paquets, donc il augmente le débit moyen du réseau.

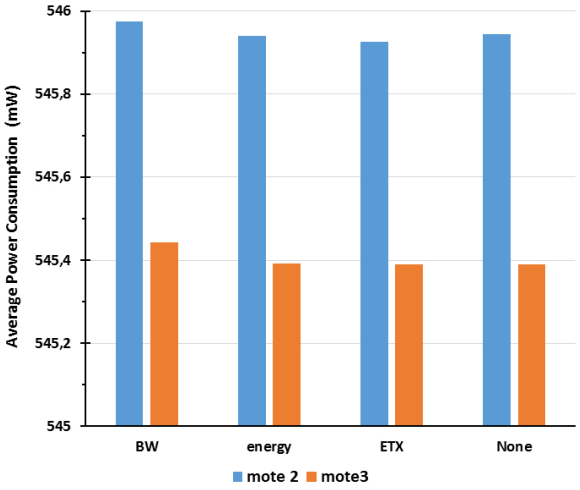
d) Consommation d'énergie

Afin d'estimer la durée de vie du réseau avec FreeBW-OF, nous avons comparé cette dernière avec ETX-OF, Energy-OF et None-OF en termes de consommation d'énergie au cours du temps dans un réseau composé d'un seul DAG.

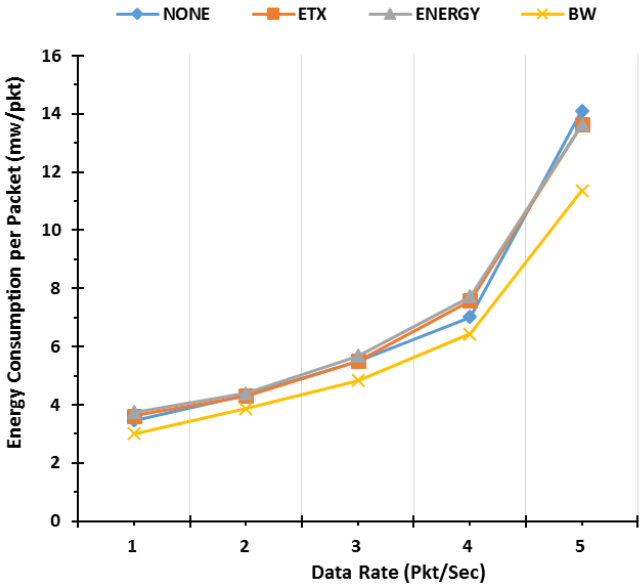
La Figure 3.8a représente la consommation d'énergie moyenne de deux noeuds distincts qui appartiennent à deux chemins différents. Le premier chemin ($6 \rightarrow 7 \rightarrow 2$) est utilisé par toutes les OFs (ETX, Energy et None) et le second ($6 \rightarrow 5 \rightarrow 4 \rightarrow 3$) est commuté dynamiquement par FreeBW-OF (nous notons que ces résultats ont été déduits à partir de la sortie de simulation). D'après les résultats, nous observons que le routage d'un paquet à travers des chemins congestionnés peut consommer plus d'énergie qu'à travers les moins congestionnés. Nous remarquons dans la Figure 3.8a que FreeBW-RPL consomme près de 50% d'énergie en moins par rapport aux OFs de RPL. La raison de la



(a) Consommation d'énergie pour le serveur et les routeurs



(b) APC pour les capteurs 2 & 3



(c) Énergie consommée par paquet

FIGURE 3.8 – Consommation d'énergie (mw)

faible consommation d'énergie de FreeBW-OF est que BW consomme plus d'énergie du processeur CPU car il nécessite plus de ressources en termes de calcul.

De même, sur la Figure 3.8b, nous mesurons l'énergie consommée par les noeuds les plus proches du racines (2 et 3) des deux chemins choisis par les différentes OFs. À partir de ces résultats et en se référant à la Figure 3.1, il est bien clair que le paquet routé prend le chemin ($6 \rightarrow 7 \rightarrow 2$) tout en utilisant les OFs du RPL (ETX, Energy, None) alors qu'il commute vers le chemin ($6 \rightarrow 5 \rightarrow 4 \rightarrow 3$) lors de l'utilisation de FreeBW-OF de RPL. Ainsi, cela pourrait être expliqué qu'une fois que le noeud (2) reçoit une surcharge de paquets, il consommera plus d'énergie et il peut être éventuellement épuisée. Par ailleurs, le protocole proposé FreeBW-RPL profite dans ce cas en commutant le chemin ce qui équilibre les frais de routage (overhead) mieux que les autres OFs du RPL.

Une autre mesure d'évaluation est illustrée sur la Figure 3.8c, dans laquelle nous avons essayé d'évaluer l'énergie consommée par les paquets reçus avec succès. Il est également démontré que FreeBW-OF consomme moins d'énergie que ETX-OF, Energy-OF et None-OF. Nous avons choisi ce type de métriques d'évaluation car notre réseau n'est pas un réseau dense (14 noeuds) et nous avons essayé de suivre le comportement de notre OF proposée quand elle se comporte différemment des autres OFs de RPL. En conséquence, FreeBW-RPL gère bien les ressources du réseau en termes d'équilibrage de charge, de CPU et de consommation d'énergie, comme le montre clairement la Figure 3.8a.

3.5.4 Comparaison de FreeBW-RPL avec d'autres travaux

En raison de l'influence à la fois du débit de transmission des données et des valeurs de densité du réseau sur les performances du réseau IoMT, nous fournissons dans cette section une comparaison entre l'OF proposée et certains travaux récents qui sont dédiés à améliorer le protocole RPL en se basant sur sa fonction d'objectif. Cette comparaison est illustrée dans le tableau 3.2.

La première série d'analyses a étudié l'impact du débit de transmission des données et de la densité du réseau sur le taux de livraison de paquets (PDR). Après avoir ajusté nos paramètres de simulation conformément à deux travaux comparatifs, le premier dans [286] où le débit de transmission des données est égal à "1 pkt/2 sec", "1 pkt/5 sec" et "1 pkt/10 sec", avec une densité de réseau égale à 20, 30, 40 noeuds pendant 900 secondes de temps de simulation. Le deuxième ajustement était similaire à celui de [287] en considérant une taille de réseau de 30 noeuds tout en conservant le même débit de transmission des données. De façon intéressante, notre FreeBW-OF proposé a révélé des résultats remarquables en termes de PDR et meilleurs que ceux des travaux précédents [286, 287]. Les auteurs de [286] ont eu tendance à se concentrer sur les performances des deux OFs de RPL (OF0 et MRHOF) en fixant la densité du réseau et en variant les intervalles de transmission, tandis que les auteurs dans [287] ont obtenu les résultats PDR à travers des expérimentations en analysant les performances de leur protocole de routage amélioré pour les réseaux faibles et à perte (ERPL). Ce protocole vise à améliorer la construction de route "peer-to-peer" et la transmission de paquets de données dans les deux modes de fonctionnement du RPL.

Dans notre deuxième comparaison, nous remarquons comment le PDR de notre FreeBW-OF proposé diminue lorsque la densité du réseau varie de 10 à 50 noeuds, par contre, il offre de meilleures performances PDR que le protocole QCOF (une extension du RPL basée sur la QoS et sensible à la congestion) proposé dans [288]. Un autre résultat a confirmé l'efficacité de notre FreeBW-OF proposé, dans lequel nous avons utilisé les mêmes paramètres de simulation considérés dans [289] tels que le débit de transmission des données variant entre 2 pkt/min, 3 pkt/min et 6 pkt/min avec une taille de charge utile de 16 octets pendant un temps de simulation de 600 secondes. Notre FreeBW-OF a un avantage en termes de taux de paquets perdus par rapport à la fonction d'objectif basée sur la logique floue (OFFL) présentée dans [289]. Dans cette comparaison, les résultats du taux de paquets perdus de FreeBW-OF reflètent des valeurs beaucoup plus élevées par rapport à celles trouvées par le protocole "OFFL". La comparaison de nos résultats avec les travaux mentionnés ci-dessus prouve que notre OF proposée "FreeBW-OF" permet une solution formelle aux exigences de QoS des réseaux IoMT tout en fournissant des performances de réseau satisfaisantes.

TABLE 3.2 – Comparaison de FreeBW-RPL avec d'autres protocoles

Protocole /OF	**Critères de performances**								
FreeBW-RPL	**Taux de perte de paquets (PDR)**								
	Taille du réseau : N=20			N=30			N=40		
	PPS=2	PPS=5	PPS=10	PPS=2	PPS=5	PPS=10	PPS=2	PPS=5	PPS=10
	80,01%	94,88%	98,86%	76,89%	89%	97,72%	68,20%	81,93%	92,05%
MRHOF + OF0 [286]	**Taux de perte de paquets (PDR)**								
	Taille du réseau : N=20			N=30			N=40		
	PPS=2	PPS=5	PPS=10	PPS=2	PPS=5	PPS=10	PPS=2	PPS=5	PPS=10
	≈39%	≈92%	≈96%	≈38%	50%	≈95%	≈18%	40%	≈82%
ERPL [287]	**Taux de perte de paquets (PDR)**								
	Résultats expérimentaux :			N=30					
				PPS=2		PPS=5		PPS=10	
				≈70%		≈75%		≈80%	
FreeBW-RPL	**Taux de livraison de paquets (PDR)**								
	Taille du réseau : N=10		N=20	N=30		N=40		N=50	
	92,01%		53.9%	45.276%		41.73%		28.225%	
QCOF [288]	**Taux de livraison de paquets (PDR)**								
	Taille du réseau : N=10		N=20	N=30		N=40		N=50	
	≈16%		≈17%	≈18%		≈20%		≈22%	
FreeBW-RPL	**Taux de perte de paquets**								
	Taille du réseau : N=50								
	PPM=2 pkts/min			PPM=3 pkts/min			PPM=6 pkts/min		
	5%			6%			8%		
OFFL [289]	**Taux de perte de paquets**								
	Taille de réseau : N=50								
	PPM=2 pkts/min			PPM=3 pkts/min			PPM=6 pkts/min		
	≈72%			60%			≈45%		

3.6 Conclusion

Dans ce chapitre, nous avons proposé un nouveau protocole de routage RPL sensible à la QoS pour l'IoMT avec une nouvelle fonction d'objectif appelée FreeBW-OF. Notre FreeBW-OF proposée permet de sélectionner le meilleur candidat de transfert en fonction de la bande passante libre maximale fournie par les noeuds ascendants. En outre, la bande passante libre réelle a lieu à chaque saut tout au long de tous les chemins, depuis le noeud source au noeud destinataire (racine). Pendant ce temps, FreeBW-OF peut réduire le problème de congestion en passant par un chemin moins encombré. Nous avons montré, sur la base d'une évaluation expérimentale en utilisant Cooja, que notre FreeBW-OF peut atteindre de meilleurs résultats par rapport aux OFs par défaut du protocole RPL en termes de taux de paquets délivrés, de délai de bout en bout, de débit et de consommation d'énergie. La plupart de ces paramètres d'évaluation satisfaits étaient auparavant considérés comme un défi essentiel dans les réseaux IoMT. Nos résultats peuvent promouvoir

les applications gourmandes telles que les applications IoMT.

Dans le chapitre suivant, en changeant de couche protocolaire, nous proposons dans une deuxième contribution qui consiste e un algorithme d'ordonnancement. Cet algorithme permet d'équilibrer le taux de perte des données en répondant à la QoS dans les réseaux IoMT.

Chapitre 4

Un algorithme d'ordonnancement équilibré pour une transmission d'un flux multimedia

Chapitre 4

Un algorithme d'ordonnancement équilibré pour une transmission d'un flux multimédia

4.1 Introduction

IoMT est généralement considéré comme un ensemble de dispositifs multimédias interconnectés qui ont la capacité d'acquérir des contenus multimédias du monde réel et de les présenter de manière attrayante [94]. De plus, avec le nombre croissant de ce type de dispositifs intelligents, le nombre d'applications IoMT a connu une croissance exponentielle. Ces applications sont utilisées dans plusieurs domaines notamment les maisons intelligentes, la santé intelligente, les véhicules intelligents, les villes intelligentes...etc. Cette riche diversité d'applications peut entraîner des exigences plus strictes que celles de l'environnement d'IoT, en raison de la croissance des contenus multimédias dans le réseau. Le contenu multimédia peut faire référence à la combinaison, en temps réel ou non, de deux ou plusieurs contenus multimédias différents tels que texte, audio, image, vidéo, etc. [94]. Par exemple, certaines caméras de surveillance dans une application d'une maison intelligente peuvent enregistrer des images et du son en même temps, et peuvent également enregistrer un scénario de vidéo complet.

Les auteurs dans [290] ont proposé un nouveau schéma de conception basé sur une infrastructure multimédia interactive dans laquelle l'information multimédia est traitée pour satisfaire les besoins du système d'informations du campus. Des recherches récentes, qui ont connu des avancées significatives dans le flux de trafic multimédia, ont rapporté que le trafic multimédia, en particulier le trafic vidéo, dominait largement le trafic des paquets de type "Internet Packet" sur Internet [50]. Ce type de trafic est connu sous le nom de "BVD" dans [268] et de communications multimédias dans l'IoMT.

Les applications IoMT sont de plus en plus utilisées. Cependant, il est important de mentionner qu'un bon nombre d'entre elles, à savoir la vidéo à la demande et la vidéo-conférence, sont confrontées à des défis de plus en plus imposants en ce qui concerne la garantie d'un certain nombre d'exigences de QoS telles que la bande passante, le délai et le taux de perte de paquets. À cet effet, dans la littérature, il existe un grand nombre de solutions proposées visant à résoudre ces défis. Par exemple, dans [275], une amélioration du protocole de routage RPL a été proposée au niveau de la couche réseau en suggérant

une nouvelle fonction d'objectif sensible à la QoS appelée FreeBW-RPL. Il convient de mentionner un autre problème qui est très susceptible de détériorer la QoS ; c'est l'incapacité de distinguer les différents types de paquets qui circulent dans un réseau. Si une distinction adéquate n'est pas établie entre les données scalaires et les données vidéos, les exigences de QoS ne seront pas entièrement satisfaites. De plus, les caractéristiques du trafic multimédia dans le réseau pourraient être hétérogènes, ce qui pourrait avoir un impact négatif sur la QoS. D'autre part, l'architecture des services différenciés, i.e. DiffServ, effectue une réservation de ressources par classe pour la différenciation entre les services qui utilisent plusieurs classes. Par la suite, ce trafic est traité selon ses classes respectives [291]. Lorsqu'un flux vidéo est diffusé via le réseau, il est important de trouver un moyen efficace d'empêcher toute perte de ces données multimédias, car ces dernières sont aussi critiques que les données *Internet Packet (IP)*. Les données multimédias passent par la couche MAC et la couche physique afin qu'elles puissent être livrées [292].

Une maison connectée à Internet, utilisant à la fois des flux IoT et non IoT, peut bénéficier de l'utilisation d'algorithmes récents de gestion active des files d'attente "Active Queue Management (AQM)", en particulier des systèmes basés sur "Fair-Queuing (FQ)" [293]. De plus, dans les applications IoT industrielles, l'ordonnancement des services d'IoT et l'ordonnancement des messages qui prennent en considération la QoS sont utilisées quand il parvient de sélectionner une direction d'ordonnancement [294]. Il existe de nombreuses politiques d'ordonnancement dans les systèmes de gestion des files d'attente ; les plus utilisées sont la file d'attente équitable (FQ), la file d'attente pondérée équitable (Weighted Fair Queuing (WFQ)), la file d'attente Round Robin pondérée (Weighted Round Robin (WRR)) et la file d'attente Round Robin pondérée par le déficit (Deficit Weighted Round Robin (DWRR)) [295]. L'algorithme d'ordonnancement DWRR [296] s'est avéré plus simple à utiliser en comparaison avec les autres algorithmes d'ordonnancement lors de la recherche d'une équité globale. L'algorithme d'ordonnancement WRR attribue à chaque connexion un poids différent, sans traiter toutes les connexions de manière égale. Cet algorithme a été utilisé dans [297] pour résoudre le problème résultant de la grande quantité de trafic de données ainsi que du changement dynamique des modèles de trafic dans la gestion des données multimédias. Les auteurs ont appliqué cet algorithme pour fournir le meilleur service demandé afin d'améliorer la qualité de la transmission multimédia.

Concernant l'architecture IoT, il est préférable d'utiliser des fonctionnalités de gestion de données simples et évolutives [298]. Pour cette raison, il a été décidé de choisir l'algorithme d'ordonnancement DWRR comme base pour l'extension souhaitée. Il est important de rappeler que cet algorithme est efficace et présente une complexité faible ($O(1)$).

D'autre part, il est largement admis que les communications sans fil sont connues pour être soumises à certaines restrictions telles que la limitation de la bande passante, le nombre limité d'unités de traitement, la consommation d'énergie...etc. [269]. De plus, les réseaux IoMT sont connus d'être des réseaux avec perte car ils gèrent d'énormes quantités de données multimédias. Ces données sont généralement volumineuses et gourmandes en termes d'espace mémoire ; d'où il y a un grand risque que ces données soient perdues, i.e., lorsqu'un paquet de données est trop volumineux et ne trouve pas assez d'espace dans une file d'attente, il y a une forte probabilité qu'il soit perdu. Mais la question qui se pose est de savoir quelle la cause qui augmente la probabilité de perte de données ? La réponse peut varier selon plusieurs causes sur lesquelles nous pouvons les classer en fonc-

tion de chaque couche protocolaire. En effet, certains chercheurs ont suggéré de traiter le problème de la perte de paquets au niveau de la couche physique [292]. Afin d'éviter toute perte de données, ils ont proposé de classer ce problème selon trois approches qui sont le codage/décodage vidéo, le codage de canal et la dissimulation d'erreur basée sur le récepteur. Dans notre cas, nous identifions ce problème sur la couche MAC, dans laquelle la fourniture des meilleures métriques de QoS est le problème important en ce qui concerne la gestion des files d'attente. En effet, le streaming multimédia prend plus de place et circule très rapidement, ce qui peut immédiatement saturer les files d'attentes. De plus, lorsqu'il n'y a pas assez d'espace pour mettre les données dans la file d'attente prévue, l'algorithme d'ordonnancement supprime instantanément le paquet. Il convient de savoir que les données multimédias peuvent être classées selon leur type. Tenant en exemple, les données multimédias réelles sont censées de satisfaire l'exigence de QoS avec un délai minimum. Ce type de données sensibles au délai doit être programmé pour quitter le système à temps, un algorithme d'ordonnancement, différent de celui de FIFO, est fortement recommandé. Pour plus d'informations, ce type de données doit être traité séparément lorsqu'il s'agit de le comparer avec un autre type de données car comme ces dernières auraient besoin de moins de temps pour être traitées. Il est utile de noter que dans ce cas, deux problèmes peuvent être identifiés : le premier survient lorsqu'une file d'attente devient saturée et commence à rejeter les paquets en excès, ce qui entraîne un taux de perte de paquets élevé. Tandis qu'au second concerne le type de paquet non défini qui peut nécessiter un algorithme d'ordonnancement avec priorité. Ces deux problèmes se posent avec l'utilisation d'un algorithme d'ordonnancement FIFO dont dépend l'IoT. Il convient de souligner que l'algorithme DWRR offre la possibilité d'avoir plusieurs files d'attente qui permettent de résoudre le problème de la gestion de différents types de données multimédias. À notre connaissance, il n'existe aucune méthode efficace pour optimiser l'algorithme DWRR, d'où il est nécessaire de prendre en compte un moyen pour équilibrer les pourcentages de perte de paquets entre les différentes files d'attente possédant différents types de données multimédias et de partitionner l'espace libre restant entre elles.

Notre deuxième contribution vise à proposer une nouvelle solution pour minimiser la probabilité de perte de données. Il s'agit d'une extension de l'algorithme d'ordonnancement DWRR ; nommé EDWRR. Fondamentalement, l'algorithme EDWRR est obtenu en introduisant un mécanisme d'équilibrage dans l'algorithme d'ordonnancement DWRR. Ce mécanisme fournit, après un certain nombre de tours, un taux de perte de paquets également équilibré entre les différentes files d'attente définies dans l'algorithme d'ordonnancement. Par exemple, après 10 tours, l'algorithme DWRR supprime un grand nombre de paquets dans la file d'attente vidéo en raison de la grande quantité de données à traiter, tandis que les autres files d'attente possèdent beaucoup d'espace libre. Il s'agit d'une gestion des files d'attente 'aprés une saturation' inéquitable. L'algorithme d'ordonnancement EDWRR proposé devrait résoudre ce problème en équilibrant le taux de perte de paquets, ainsi que l'espace libre restant entre les différentes files d'attente.

Contrairement à d'autres algorithmes, celui proposé dans notre deuxième contribution est capable de minimiser le rejet direct de paquets en cas de files d'attente surchargées en envoyant une alerte à la procédure de mise en file d'attente afin de ne plus accepter de paquets jusqu'à ce que l'algorithme réussisse à libérer suffisamment d'espace correspondant au nombre d'octets pouvant être acceptés. L'algorithme d'ordonnancement DWRR

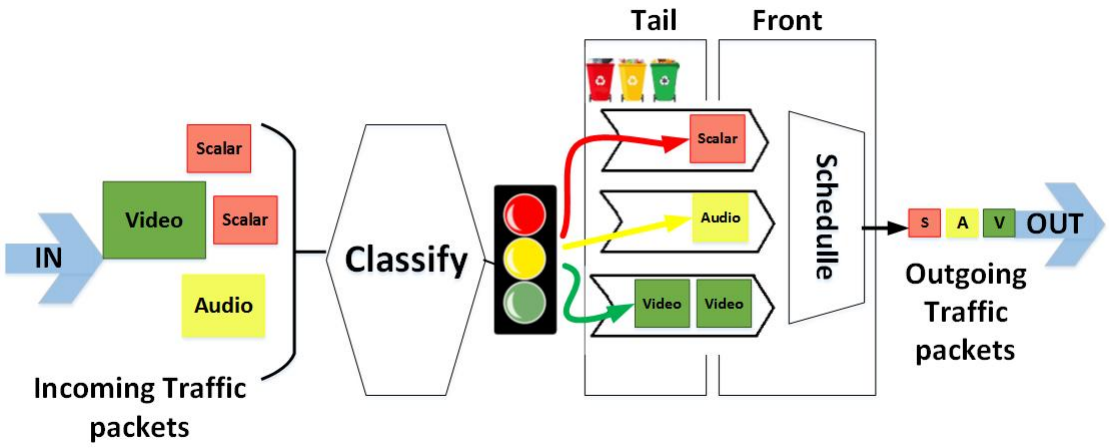


FIGURE 4.1 – Politique d'ordonnancement de l'algorithme EDWRR

a été choisi comme base de notre extension en raison de sa faible complexité, de son équité élevée et de son utilisation récente de plus en plus répandue dans un grand nombre d'applications multimédias. En plus du rôle majeur d'attribution de poids dynamiques aux files d'attente afin d'aider le réseau à fournir des services multimédias adéquats, même en présence d'un trafic en rafale, l'algorithme "EDWRR" [299] proposé garantit un taux de perte de paquets inférieur pour les scénarios à plusieurs files d'attente, et obtient également de meilleures performances en termes de taux de paquets délivrés (PDR), de délai de bout en bout et de débit. Pour conclure, on peut souligner les principales contributions comme suit :

- Arrêt de la procédure de mise en file d'attente dans le but de minimiser le nombre de paquets perdus en cas de surcharge,
- Allouer une mémoire tampon à chaque type de service ou de données,
- Classifier le trafic entrant en deux types de trafic RT (VoIP) et NRT (données scalaires), comme illustré dans la Figure 4.1,
- Différencier les différents services d'application IoMT en donnant la priorité aux données multimédias qui nécessitent certaines exigences de QoS spécifiques, telles que la période de temps limitée pour le traitement des données urgentes.

Il convient de mentionner que la solution proposée dans ce chapitre a été développée en utilisant le simulateur Cooja [92] sous le système d'exploitation Contiki [71]. Contiki fournit une pile de réseau sans fil très adéquate, appelée pile Rime [300], qui est considérée comme une pile de communication en couches légères qui a été conçue pour simplifier la mise en oeuvre des protocoles de communication complexes. En ce qui concerne la mise en file d'attente des données, Rime copie les données dans les tampons des files d'attente alloués dynamiquement.

4.2 Travaux connexes sur DWRR

Dans les systèmes multimédias, plusieurs problèmes restent ouverts pour améliorer le transfert multimédia avec QoS. Nous mentionnons la gestion des files d'attente au niveau de la couche MAC, qui représente un facteur très important aidant à minimiser la perte de données. Ainsi, le respect de certains niveaux de QoS pour les flux multimédias ne repose pas sur l'utilisation d'une seule file d'attente sans aucun niveau de priorité. Ce paradigme figure comme une tâche difficile, en particulier lors de la manipulation de données multimédias sous toutes ses formes variées. L'algorithme d'ordonnancement DWRR a été introduit par [296] pour les flux de file d'attente actifs avec un ordonnancement de type Round Robin (RR). De nombreuses extensions de DWRR visaient à améliorer ses performances à plusieurs fins. Nous présentons dans cette section une revue détaillée et une comparaison des politiques d'ordonnancement. Nous les regroupons en cinq sous-sections : optimisation des délais, optimisation de l'équité, améliorations récentes du DWRR, autres améliorations d'ordonnancement et les méthodes concurrentes dans lesquelles nous dépendons de notre comparaison.

4.2.1 Optimisation du Délai

Dans [301], les auteurs ont proposé un schéma appelé "Modified Dynamic WRR (MDWRR)" en ajoutant une procédure de transmission cellulaire basée sur la priorité du délai. MDWRR garantit le délai du trafic en temps réel et assure une transmission efficace du trafic en temps non réel. Cependant, MDWRR peut fournir plus de complexité par rapport au schéma DWRR conventionnel. Similaire à cette approche, les auteurs dans [302] ont suggéré une autre version améliorée appelée "Multi Level Dynamic Deficit Round Robin (MLDDRR)" qui soutient les applications sensibles au délai telles que les applications temps réel. Le résultat principal de MLDDRR est la possibilité d'atteindre un débit efficacement élevé et un petit délai pour les paquets de petites tailles de chaque classe de service. Dans [303], une version étendue du DWRR est fournie en tant que DRR+, ce qui lui permet de garantir une gigue à faible délai pour le trafic en rafale sensible au délai par rapport au DWRR. Le trafic sensible au délai est stocké dans une file d'attente distincte avec un quantum différent (QLC). Cependant, l'ajustement de QLC devient plus difficile et nécessite une procédure d'essai et d'erreur dans les points d'agrégation où les flux provenant de plusieurs sources se combinent et forment un modèle de trafic non déterministe.

4.2.2 Optimisation de l'équité

Une autre approche est présentée dans [304], où les auteurs ont suggéré un algorithme d'ordonnancement distribué (Distributed Deficit Round Robin (DDRR)) qui utilise une file d'attente équitable avec la valeur d'espace inter-trame pour permettre la prise en charge de la QoS pour les applications WLAN. DDRR a permis de hiérarchiser le trafic en différenciant les inter-intervalles d'espacement (Inter Frame Space (IFS)).

Le travail dans [305] présente une discipline d'ordonnancement appelée "Elastic Round Robin (ERR)", qui permet un ordonnancement équitable et efficace des paquets pour améliorer l'isolement entre les différents utilisateurs dans les réseaux de trous de ver. Les résultats obtenus prouvent que ce dernier présente une équité remarquable et relative.

Les compteurs excédentaires sont remis à zéro dès que les flux deviennent inactifs. Cela implique d'oublier tout service excédentaire reçu par des flux inactifs qui sont autorisés à concurrencer à nouveau la bande passante du canal dès le tour suivant. Une autre version améliorée du DWRR est proposée dans [306] "Airtime Deficit Round Robin (ADRR)" pour les réseaux maillés sans fil basés sur IEEE 802.11. L'algorithme d'ordonnancement ADRR prend en compte la qualité du canal du noeud émetteur en fournissant une équité de temps d'antenne intracellulaire.

Ainsi, les auteurs dans [307] ont utilisé un ordonnanceur à base de trames appelé "Loan-Grant based Round Robin (LGRR)" dans les réseaux DiffServ. LGRR est basé sur un schéma de Loan-Grant qui accorde une priorité plus élevée au flux de trafic qui demande un prêt de bande passante de l'ordonnanceur afin d'être traité rapidement. Dans [308], les auteurs ont proposé une extension nommé "Budget-based Round Robin (BRR)" qui fonctionne avec la hiérarchie de la mémoire afin d'implémenter un grand nombre de connexions actives. Son analyse théorique et ses résultats expérimentaux démontrent que BRR permet la mise en file d'attente d'une manière équitable. En outre, l'algorithme dans [309], a présenté une nouvelle extension par l'insolvabilité de l'algorithme DWRR (IDWRR) basé sur un mécanisme appelé l'insolvabilité de file d'attente (Queue Insolvency (QI)). Cette extension réduit la quantité des paquets avec un délai épuisé (overdelayed packets) qui sont envoyés par les files d'attente insolvables. Des calculs supplémentaires seraient nécessaires dans l'algorithme d'ordonnancement I-DWRR et la complexité de l'algorithme augmenterait considérablement.

4.2.3 Améliorations récentes du DWRR

Des travaux plus récents dans ce contexte avaient également fourni quelques extensions de DWRR, comme [310], où les auteurs ont utilisé un algorithme d'ordonnancement basé sur un réseau neuronal "Dynamic Weighted Round Robin (NNDWRR)" pour l'équilibrage de charge entre plusieurs machines virtuelles (VM). Cet algorithme utilise la prédiction de charge basée sur le réseau neuronal pour distribuer les demandes entrantes et ajuste un poids pour chaque machine virtuelle appropriée.

Une autre amélioration de l'algorithme RR nommée "Least Delay Dynamic Weighted Round Robin (LDDWRR) [311], qui calcule le poids des serveurs et distribue le trafic en conséquence. La stratégie proposée peut entraîner un délai important car un seul contrôleur doit calculer le poids de tous les serveurs en plus de définir des règles pour répartir le trafic. Dans [312], les auteurs ont introduit un algorithme d'ordonnancement DWRR dynamique à long terme (DLTE-DWRR) afin d'améliorer les performances d'ordonnancement de la passerelle dans l'IoT. L'algorithme évite la possibilité de congestion face aux flux de trafic en rafale en mémorisant le taux d'arrivée des paquets et des informations historiques.

Dans le même contexte, un algorithme nommé Prioritized Load Aware Weighted Round Robin (PLAWRR) est présenté dans [313], qui a pour objectif d'améliorer l'utilisation des ressources. L'algorithme PLAWRR utilise différentes priorités pour les valeurs de charge de trafic en fonction des caractéristiques du trafic et des conditions du canal ainsi que de l'historique du débit de manière à augmenter le nombre de paquets à servir. PLAWRR atteint des performances supérieures en termes de délai, de taux de perte de paquets et de débit.

4.2.4 Autres améliorations

Pour de nouvelles améliorations dans les nouveaux réseaux émergents, les auteurs dans [292] ont proposé une méthode de transmission qui améliore la QoS pour prendre en charge divers contenus multimédias de haute qualité dans le réseau de convergence de la cinquième génération. En particulier, leurs travaux proposent une méthode de protection des images clés basée sur la priorité où un trafic de données très élevé tel que le contenu "Ultra High Definition (UHD)" qui est transmis dans un réseau de convergence 5G. Un autre type d'applications appelé IoTs à bande étroite (Narrowband Internet of Things (NB-IoT)) est discuté dans [314], qui cible les dispositifs nécessitant un faible débit de données, un faible coût et une longue durée de vie de la batterie. Les auteurs identifient les problèmes d'ordonnancement des ressources radio pour les systèmes NB-IoT et évaluent les effets des paramètres essentiels sur les performances d'ordonnancement des ressources radio. Une autre approche d'ordonnancement basée sur les événements a été suggérée par [315], où les auteurs ont introduit une nouvelle expérience d'ordonnancement réseau et une approche de routage dans le réseau IoT. Le mécanisme de routage utilise les performances attendues du réseau afin de choisir le chemin le plus approprié pour le paquet donné, selon des chemins possibles vers chaque noeud.

4.2.5 Les méthodes concurrentes

L'ordonnancement des flux a été largement étudié dans les réseaux sans fil, en particulier dans les réseaux LTE. Les preuves qui nous amènent à insister sur notre étude comparative sont bien plus nombreuses sur les approches d'ordonnancement proposées dans la technologie sans fil LTE. Divers algorithmes d'ordonnancement de paquets ont été développés pour prendre en charge les services en temps réel (RT) et en temps non-réel (NRT).

Les auteurs dans [316, 317] ont présenté une approche d'ordonnancement de liaison descendante pour l'allocation de ressources pour différentes classes de trafic au niveau de la couche MAC des systèmes sans fil. Cette approche représente une modification des algorithmes d'ordonnancement "Virtual Token Modified Largest Weighted Delay First (VT-M-LWDF)" et des règles d'ordonnancement "Modified Largest Weighted Delay First (M-LWDF)". L'ordonnanceur proposé a montré une amélioration équilibrée pour les différents flux inter-classes (vidéo, VoIP et au trafic best-effort) en termes de débit, PLR et efficacité spectrale cellulaire parmi différents nombres d'utilisateurs.

Dans [318], les auteurs ont analysé les performances des trois différents mécanismes d'ordonnancement de couche MAC tels que FIFO, RED et WRED sur le réseau IEEE 802.11e. Les simulations effectuées par le simulateur QualNET 5.1 montrent que les ordonnanceurs RED et WRED surpassent FIFO lorsque la charge du trafic augmente.

Les auteurs dans [319,320], ont proposé un nouveau schéma d'ordonnancement appelé E-MQS. Ce schéma d'ordonnancement est basé sur l'extension du modèle E, en prenant en compte un nouveau facteur appelé taille maximale de file d'attente (Maximum Queue Size (MQS)) afin de réduire le taux de perte de paquets. Les résultats de simulation montrent que le schéma proposé surpasse les ordonnanceurs "Frame Level Scheduler (FLS)", "M-LWDF" et "Exponential/Proportional Fair (EXP/PF)" en termes de délai, de débit cellulaire, d'indice d'équité (FI) et efficacité spectrale (SE).

Dans [321], les auteurs ont proposé une extension pour le groupe des stratégies d'ordonnancement existantes Logrule, Linear-rule, et M-LWDF en montrant l'effet de l'utilisation des paramètres (QdS Class Identifier (QCI)) sur différents algorithmes d'ordonnancement sensibles au délai. L'évaluation des performances des algorithmes d'ordonnancement étendus a été réalisée en termes de PLR, de débit, d'équité et d'efficacité spectrale. De plus, les auteurs dans [322] ont étudié l'évaluation des performances du DRR et du SFQ dans un scénario filaire/sans fil. Cette étude s'est concentrée sur différents scénarios tels que la densité du réseau (nombre croissant de noeuds), le scénario de temps de pause et le scénario de mobilité. Ils ont évalué le DRR et le SFQ sur la base de deux métriques tels que le délai moyen de livraison des paquets et le taux moyen de perte de paquets.

Dans de nombreux cas, lorsque le trafic augmente, notamment avec le flux multimédia, les files d'attente sont surchargées puis rejetent les paquets dépassés. Par conséquent, cette situation peut entraîner plusieurs conséquences, en particulier si les données sont de type d'urgence, dans ce cas, la surcharge doit être évitée.

De nombreuses extensions visent à utiliser l'algorithme d'ordonnancement DWRR en améliorant ses performances pour un type de trafic différent tout en maintenant les exigences de QoS en utilisant diverses stratégies d'ordonnancement. Cependant, à ce jour, aucune d'entre elles ne s'est avérée capable de réduire davantage la probabilité de perte de données tout en différenciant les services d'application IoMT. De plus, aucune d'entre elles n'a tenté d'implémenter l'algorithme DWRR dans les réseaux IoT sachant que ce type de réseaux dépend, en matière de gestion de file d'attente, de la politique FIFO. Cela apparaît comme un écart de recherche majeur, car la demande de trafic RT augmente tout autant que celle du trafic NRT. À notre connaissance, ce type d'études n'a pas été abordé dans la littérature. Notre EDWRR proposé a résolu ces limitations en équilibrant le taux de perte de paquets en plus de l'espace libre restant entre les files d'attente. En plus, notre algorithme minimise la perte inutile de paquets dans le cas de files d'attente surchargées en arrêtant la procédure de mise en file d'attente des paquets jusqu'à ce que l'algorithme libère suffisamment d'espace pour les prochains paquets entrants.

Les améliorations proposées de l'algorithme d'ordonnancement DWRR et d'autres algorithmes d'ordonnancement sont résumées dans le tableau 4.1.

Table 4.1 – Comparaison des travaux connexes

Algorithme d'ordonnancement	**Type de trafic**	***Technique***	**Avantages**	**Inconvénients**
MDWRR [301],2002	RT & NRT	Utilise la priorité du délai pour la transmission	- Minimise la priorité de délai du trafic RT - Traite le trafic ABR (Available Bit Rate)	Plus complexe que DWRR
MLDDRR [302],2005	RT	Priorité élevée attribuée aux paquets ayant le plus petit poids [1]	Peut atteindre un débit élevé et un délai plus court	Favorise les paquets de petite taille

1. Le poids est calculé en fonction de la longueur du paquet et des paramètres de "Relative Differentiated Services"

TABLE 4.1 – Comparaison des travaux connexes

DRR++ [303],2000-2002	RT & best-effort traffic	Utilise un mécanisme de priorité pour favoriser les paquets des flux critiques en termes de latence	Garantit une latence réduite	- Incapable de planifier le trafic critique en terme de latence dans les réseaux multi-sauts - Ne gère pas les longues rafales transitoires en raison de sa configuration statique
DDRR [304],2003	RT & NRT trafic	Attribue des IFS et des intervalles backoff plus courts aux paquets de priorité supérieure	Fournit une prise en charge de la QoS et une différenciation des services dans les WLAN	- Ne convient pas pour un débit de données élevé et une application RT - Atteint un faible débit sous une charge élevée à un conflit de canal excessif
ERR [305],2002	Flux RT	- Les flux ne sont pas desservis pour un quantum fixe à chaque tour - À chaque tour, ERR détermine le nombre de flits [2] autorisés à être envoyés dans un flux	Bonne équité de la bande passante entre les flux	- Ne fournit pas des limites de performances satisfaisantes dans le pire des cas - N'atteint pas une bonne équité à court terme que la plupart des ordonnanceurs - Un flux peut subtiliser la bande passante de ses concurrents
ADRR [306],2008	RT & NRT	- Exploite ETT [3] pour transmettre un paquet sur un lien - Prend en compte la qualité du canal - Les trames de données entrantes sont classées en fonction de leur prochain saut avant d'être déposées dans la file d'attente	- Améliore le DRR en tenant compte de la qualité du canal - Propose une solution pour les réseaux maillés sans fil en exploitant les métriques de routage afin d'assurer l'équité	- Ne prend pas en compte des poids différents pour chaque file d'attente - Ne sert que les paquets dont "ETT" est inférieur au compteur de déficit

2. Flit : le plus petit morceau de paquet
3. ETT : temps de transmission estimé

Table 4.1 – Comparaison des travaux connexes

LGRR [307],2009	EF [4], BE [5] (Poisson & Pareto traffic)	- Étendre OCGRR en fonction d'une politique de prêt de bande passante qui manipule la saturation du trafic - Permet à un flux de prêter une certaine bande passante à l'ordonnanceur pour passer ses rafales	Permet une équité aux différents flux	L'ordonnancement des paquets au sein de la classe EF ne concerne pas la façon dont l'ordonnancement inter-classe
BRR [308],2010	Flux de données en temps réel	- Utilise une hiérarchie de mémoire pour bien fonctionner dans le cas d'un nombre élevé de connexions actives - S'appuie sur plusieurs structures de file d'attente	- Un algorithme d'approximation pour l'équité de la mise en file d'attente - Résout la complexité temporelle	Spécifie pour deux cas particuliers d'allocation de mémoire : statique dans la DRAM, dynamique dans la SRAM
I-DWRR [309],2011	Paquets ordinaires ayant des TTL différents	Identifie les files d'attente insolvables qui ont envoyé des paquets dans les délais	- Réduit le nombre de violations des délais - PDR réduit pour les scénarios à plusieurs files d'attente	Maintient la latence survenue égale à DWRR
NNDWRR [310],2014	Trafic Web réel	- Envoie un grand nombre de tâches à différentes VMs - Combine les métriques de charge des VMs : utilisation du processeur, de la mémoire, de la bande passante et des E/S sur disque - Prédit la charge d'un réseau de neurones pour ajuster le poids de chaque VM	Bénéficie des avantages de l'architecture décentralisée : passage à l'échelle et capacités de disponibilité plus élevées pour gérer les utilisateurs du Cloud	En cas de grande variation d'entrée, le réseau neuronal peut ne pas bien apprendre

4. EF :Expedited Forwarding
5. BE : Best-Effort

TABLE 4.1 – Comparaison des travaux connexes

LDDWRR [311],2017	Trafic Web	- Attribue un délai à chaque lien entre le serveur et le commutateur en fonction de la vitesse - Le poids est attribué en fonction du délai	Améliore l'algorithme de RR en attribuant un poids dynamique aux serveurs et en répartissant le trafic	- Un seul contrôleur centralisé peut être un point de défaillance unique - Messages de contrôle et délais de traitement importants, car un seul contrôleur qui calcule le poids des serveurs et définit la règle de distribution du trafic
DLTE-DWRR [312],2018	Trafic en rafale (modèle de poisson)	Historique des délais et le taux d'arrivée des paquets sont utilisés pour calculer le compteur de déficit	- Satisfait la demande de transmission multiservice dans les réseaux Mine IoT - Assure l'équité à long terme	Certaines files d'attente ont une exigence sur le délai comparé à DWRR
PLAWRR [313],2019	RT(UGS, rtPS et ertPS) et NRT(FTP et BE)	Priorité calculée en fonction du trafic, des conditions du canal et de l'historique du débit afin de hiérarchiser les trafics	Fournit une utilisation efficace des ressources	Manque d'évaluation de l'énergie consommée
Queue-HOLM-LWDF [316, 317],2013	RT & NRT	Prend en considération la taille de la file d'attente et les délais des paquets	Satisfait les utilisateurs RT et NRT offrant une efficacité spectrale plus élevée, un débit plus élevé et un taux de perte de paquets plus faible	Distribue la plupart des ressources radio aux trafics RT au détriment des trafics NRT
FIFO, RED & WRED [318],2015	Trafic multimédia interactif : voix, vidéo et best effort	- Analyse des performances de FIFO, RED et WRED sur le réseau IEEE802.11e en faisant varier le taux d'arrivée du trafic - WRED inclut le mécanisme de différenciation des services et de priorité IP afin d'améliorer les performances du réseau pour les applications IMM en temps réel	RED et WRED fonctionnent mieux que FIFO sous de fortes charges de trafic	Certains des ordonnanceurs analysés présentent un caractère aléatoire

TABLE 4.1 – Comparaison des travaux connexes

E-MQS [319],2016	Trafic RT (flux VoIP et vidéo)	- Les décisions d'ordonnancement sont basées sur les paramètres de perception de l'utilisateur ainsi que sur les paramètres sensibles au canal et à la QoS - Les paramètres de perception de l'utilisateur sont obtenus à partir du modèle E	Répond aux exigences de QoS en temps réel	- Évalue uniquement le trafic VoIP - La file d'attente maximale n'identifie pas la demande de l'utilisateur et ne prédit pas la modification du débit de données de l'utilisateur
QCI-Delay-LOG-PLR, QCI-Delay-LINEAR-PLR et QCI-MLWDF [321],2018	Trafic RT et NRT (vidéo, voix et CBR)	Introduit le paramètre QCI sur la règle Log-rule, la règle linéaire et M-LWDF	Des algorithmes d'ordonnancement étendus prennent en charge et équilibrent les flux RT et NRT	Le débit moyen du trafic VoIP des schémas proposés et l'indice de référence sont des résultats proches (le débit de MLWDF surpasse à la fois QCI-Delay-LINEAR-PLR et QCI-MLWDF)
DRR et SFQ [322],2018	Modèle de trafic dans un réseau sans fil (trafic en rafale avec un débit constant)	Évalue les performances de DRR et de SFQ	Observe la technique surperformante une fois que la métrique d'évaluation a changé	- Aucune variation du modèle de trafic lors de l'analyse des techniques AQM -Ne prend pas en considération l'exigence de QoS du trafic RT et NRT

4.3 Présentation de l'algorithme d'ordonnancement DWRR

DWRR [296] a été proposé comme une solution à plusieurs problèmes d'algorithmes d'ordonnancement existants, notamment, les problèmes ayant une complexité élevée et qui sont inéquitables à cause des longueurs de paquets éventuellement différentes. Dans ce qui suit, nous présentons brièvement l'algorithme DWRR et nous mettons en évidence les points les plus importants qui nous ont motivés à proposer l'extension du DWRR (une version équilibrée de DWRR).

La file d'attente DWRR permet de regrouper le trafic en classes où chaque classe reçoit un traitement distinct dans la file d'attente correspondante. DWRR utilise un compteur de déficit $DeficitCounter$[i] pour chaque file d'attente active i dans le processus d'ordonnancement. Il spécifie la quantité maximale d'octets autorisée à être transmise par la file d'attente qui est incrémentée par le quantum à chaque fois que la file d'attente est visitée par l'ordonnanceur. Chaque type de flux est configuré avec un quantum Q[i], une

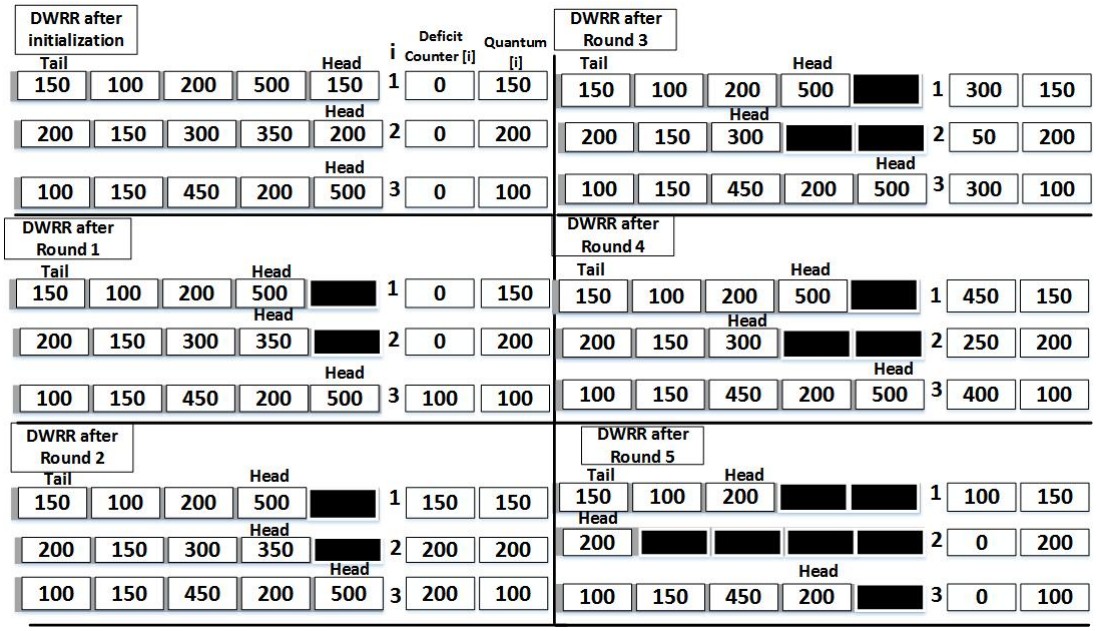


FIGURE 4.2 – Exemple de DWRR

valeur constante qui est proportionnelle au poids de la file d'attente exprimée en octets. Le poids attribué peut donner une sorte de priorité à la file d'attente qui gère un type spécifique de classe. Lors du démarrage du processus DWRR, les compteurs de déficit sont initialisés à zéro et les paquets sont mis en file d'attente selon les classes affectées.

L'idée globale est qu'à chaque tour k, la file d'attente active (file non vide) i reçoit un certain quantum d'octets $Quantum[i]$ qui est ajouté au compteur de déficit ($DeficitCounter$[i] = $DeficitCounter$[i] + $Quantum[i]$). Ensuite, le DeficitCounter [i] ne peut être envoyé que si sa valeur est supérieure ou égale à $PacketSize : Head$[i], qui est la taille du paquet de la tête de file d'attente i. Après cela, la valeur du compteur est décrémentée de la taille du paquet jusqu'à ($DeficitCounter[i] < PacketSize : Head[i]$) ou jusqu'à ce que la file d'attente devienne vide. Une fois la file d'attente est vide, la valeur du compteur de déficit est remise à 0.

Dans la Figure 4.2, un exemple illustratif est utilisé pour décrire brièvement la progression du comportement de l'algorithme d'ordonnancement DWRR. Comme on peut le constater en haut de la Figure 4.2, chaque file d'attente i possède différentes valeurs du $Quantum$[i] pour $i = 1, 2, 3$. Après le premier tour, le premier paquet est traité dans la première file d'attente car le $Quantum$[1] ajouté correspond exactement au $PacketSize : Head$[1]. Cela est également vrai pour la deuxième file d'attente qui dessert son $PacketSize : Head$[2]. Contrairement à la troisième file d'attente, qui a la quantité de $DeficitCounter$[3] < $PacketSize : Head$[3].

Pendant le tour 2, aucune des files d'attente n'est servie. Au tour 3, seul le premier paquet de la deuxième file d'attente est traité. De la même manière qu'au tour 2, au tour 4, aucun paquet n'est traité. Pendant le tour 5, un paquet de la première file d'attente ainsi que deux paquets (1^{ier} et $2^{ième}$) de la deuxième file d'attente sont traités et enfin la troisième file d'attente traite son premier paquet en tête de la file d'attente. Après le tour 6, la deuxième file d'attente est servie complètement et le $DeficitCounter$[2] est mis à zéro.

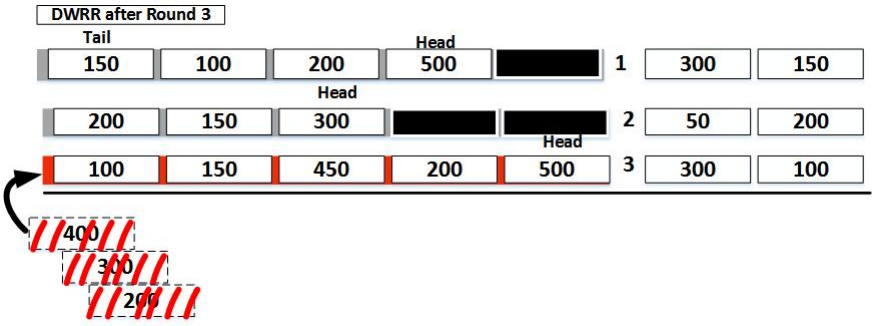


FIGURE 4.3 – Exemple de paquets surchargés dans DWRR

La Figure 4.3 illustre l'état des files d'attente i ainsi que les deux valeurs de *DeficitCounter[i]* et *Quantum[i]*. Comme on peut le remarquer, il est à noter que toutes les files d'attente ne peuvent pas être desservies au cours du tour 4 et cela est principalement dû à la valeur du *DeficitCounter[i]* ajoutée avec *Quantum[i]* qui est inférieure au *PacketSize : Head[i]* pour chaque File d'attente i. Cependant, après le tour 5, chaque file d'attente est desservie. Considérons, par exemple, qu'après le $3^{\text{ième}}$ tour, plus de paquets sont mis en file d'attente dans la file d'attente 3 (voir les rectangles barrés en rouge dans la Figure 4.3), ces paquets seront malheureusement supprimés en raison de la file d'attente surchargée alors qu'il y a beaucoup d'espace libre disponible dans les deux files d'attente 1 & file d'attente 2 qui pourraient être partagées avec la file d'attente 3. Le gaspillage de cet espace libre tout en perdant les paquets de données représente la vraie perte, surtout si ces paquets ont une QoS restreinte. En prenant un exemple de temps réel, comme le streaming vidéo, le trafic qui nécessite un faible taux de perte de données, ce problème peut entraîner une corruption des données. Par conséquent, la réduction du nombre total de paquets rejetés est une bonne solution. Néanmoins, le partage d'espace libre restant dans chaque file d'attente, en d'autres termes, le partage du nombre d'octets restant dans chaque file d'attente tout en réduisant le taux de perte de paquets par les files d'attente avec un rapport équilibré entre eux à l'aide de DWRR serait la solution la plus adéquate. Cette solution est offerte par notre algorithme d'ordonnancement DWRR équilibré décrit dans la section suivante.

4.4 EDWRR

La réduction du nombre total de paquets rejetés par les files d'attente surchargées est un défi majeur pour les algorithmes d'ordonnancement. Comme connu dans plusieurs algorithmes d'ordonnancement basés sur les classes, DWRR est celui qui fonctionne de manière équitable, efficace et avec une faible complexité. Cet algorithme est caractérisé par la communication des flux restants au cycle suivant, ce qui conduit à un débit de données minimum à long terme. Pour ces raisons, nous avons choisi DWRR comme plate-forme pour notre extension équilibrée. Dans cette section, nous discutons de notre amélioration EDWRR en donnant plus de détails sur l'algorithme d'ordonnancement proposé et sa complexité.

4.4.1 L'algorithme d'ordonnancement EDWRR

La perte des paquets se produit lorsqu'un flux de paquets arrive dans une file d'attente déjà saturée (pleine). À ce moment, la file d'attente n'a pas d'autre solution que de rejeter ces paquets nouvellement arrivés car ils n'ont pas beaucoup d'espace pour s'en occuper. En disséquant la problématique de la perte totale de paquets, nous avons compris que dans chaque file d'attente, nous pouvons formuler en utilisant un calcul mathématique la perte totale des paquets en termes des paquets de données et la valeur du quantum en plus de l'espace libre restant à chaque tour où il est traité.

Nous désignons le paquet de données mis en file d'attente dans chaque file d'attente i par A_i et nous différencions le type de données en trois types : scalaire, audio et vidéo. Q_i est la valeur du quantum affectée à chaque file d'attente et $Free$ est l'espace libre restant à l'espace tampon alloué pour chaque file d'attente. L'équation (4.1) peut être déduite de l'étape 3 de l'organigramme de l'algorithme EDWRR illustré dans la Figure 4.4. Avant la procédure de mise en file d'attente, lorsque différentes sources de trafic arrivent dans les files d'attente, elles seront classées en deux types de trafic : "real time (RT)" et "non-real time (NRT)" en se réunissant en entrée A_i, représentant la somme de tous les paquets arrivés. Sachant que le nombre total de l'ensemble des paquets perdus est calculé pour les trois files d'attente, il concerne la somme de tous les paquets de données notés $SumA_i$ calculés dans l'équation (4.1).

$$SumAi = \sum_{i=1}^{3} A_i \tag{4.1}$$

Si nous supposons que toutes les files d'attente sont saturées et n'ont pas d'espace libre, cela prouvera que tous les paquets sont rejetés en raison de la taille de tous les paquets ($SumA_i$) qui sont supérieurs au $Quantum$. Ainsi, nous supposons que toutes les files d'attente peuvent supprimer un certain nombre de paquets, nous pouvons écrire le $TotalDrop$ comme :

$$TD = \begin{cases} SumA_i - \sum_{i=1}^{3} Q_i & \text{if the queues are full} \\ SumA_i - \left(\sum_{i=1}^{3} Q_i + Free\right) & \text{if the queues are not full} \end{cases} \tag{4.2}$$

Dans le cas de files d'attente pleines, nous avons des paquets rejetés($TD > 0$) lorsque $A_i > Q_i$ et nous n'avons pas de paquets rejetés ($TD = 0$) lorsque $A_i = Q_i$. Alors que, dans le cas de files d'attente non pleines, nous avons des paquets rejetés lorsque $A_i > Q_i + free$ et nous n'avons pas de paquets rejetés($TD = 0$) lorsque $A_i = Q_i + free$.

Afin de calculer la perte de chaque file d'attente dénommée $Drop_i$ (calculée en 4.9) plusieurs étapes ont été effectuées. Nous avons fait comme hypothèse que la perte totale est égale à la somme de la perte de chaque file d'attente ($Drop_1$ pour Queue1, $Drop_2$ pour Queue2 et $Drop_3$ pour Queue3). De plus, nous avons supposé que chaque type de trafic (qu'il soit scalaire, audio ou vidéo) puisse avoir une priorité pour être servi. Ces priorités (notées α, β et γ) sont attribuées à la phase initiale de l'algorithme EDWRR en fonction du type de trafic (par exemple, nous avons utilisé pour donner une priorité élevée pour la vidéo et l'audio et moins de priorité pour le scalaire).

Comme illustré dans l'équation (4.3a), nous avons comme hypothèse la somme des pertes de toutes les files d'attente est égale à une valeur constante (TD) et nous supposons

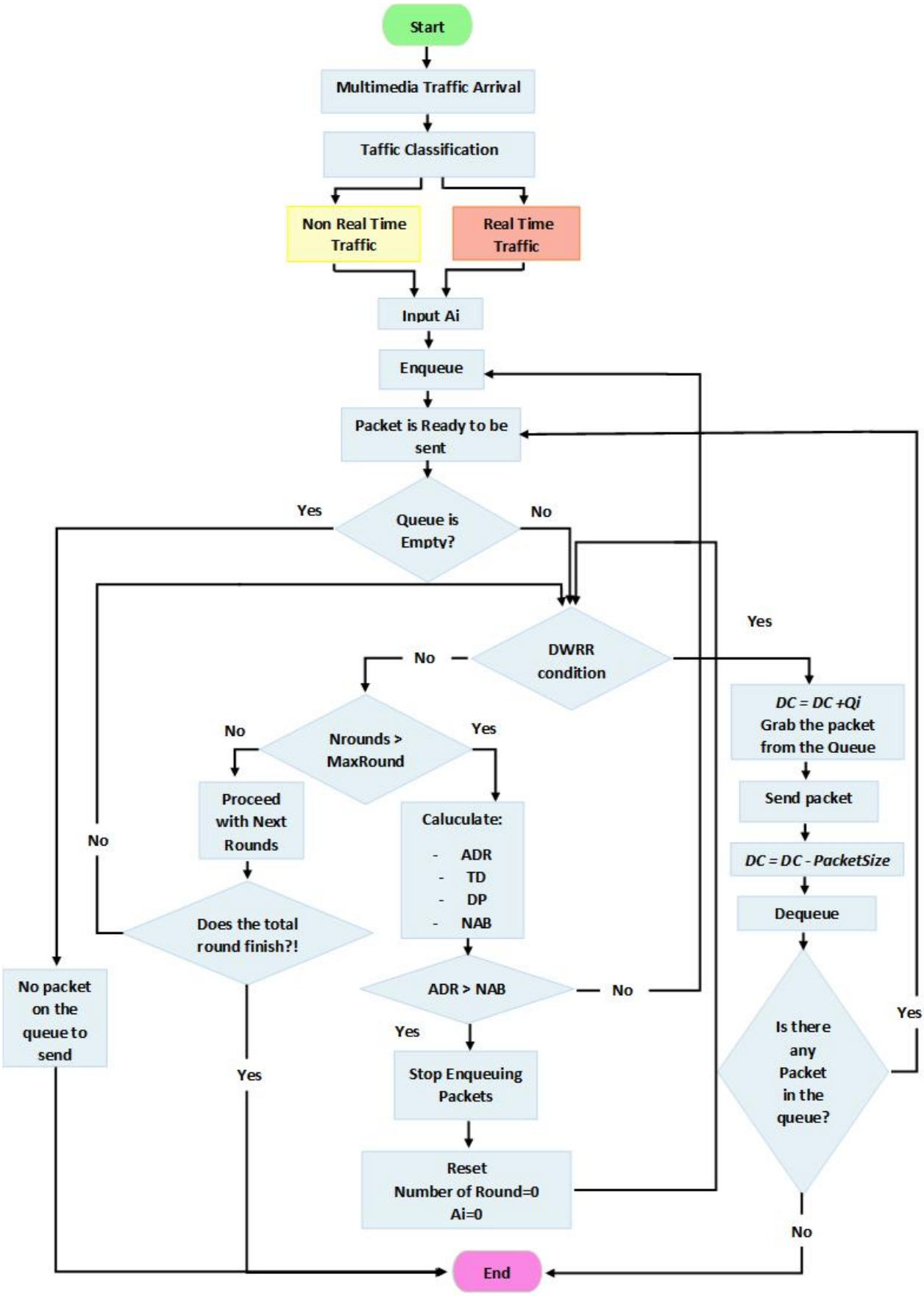


FIGURE 4.4 – Organigramme du processus EDWRR

que α, β et γ représentent respectivement les priorités de perte scalaire, audio et vidéo :

$$Drop_1 + Drop_2 + Drop_3 = TD \tag{4.3a}$$
$$\alpha + \beta + \gamma = 1 \tag{4.3b}$$

avec $0 \leq \{\alpha, \beta, \gamma\} \leq 1$.

Maintenant, la condition nécessaire et suffisante pour un pourcentage équilibré de paquets perdus est la suivante :

$$\alpha \frac{Drop_1}{A_1} = \beta \frac{Drop_2}{A_2} = \gamma \frac{Drop_3}{A_3} \tag{4.4}$$

En récupérant les deux valeurs de $Drop_2$ et $Drop_3$ respectivement dans l'équation (4.4) et en les remplaçant dans l'équation (4.3a), nous obtenons :

$$Drop_1 + \frac{\alpha}{\beta}\frac{A_2 * Drop_1}{A_1} + \frac{\alpha}{\gamma}\frac{A_3 * Drop_1}{A_1} = TD \tag{4.5}$$

On obtient ainsi :

$$Drop_1 \left(1 + \frac{\alpha}{\beta}\frac{A_2}{A_1} + \frac{\alpha}{\gamma}\frac{A_3}{A_1}\right) = TD \tag{4.6}$$

Notre objectif est d'atteindre un pourcentage équilibré de paquets perdus entre toutes les files d'attente après un certain nombre de tours. A cet effet, nous avons fixé $\alpha = \beta = \gamma$, résultant :

$$Drop_1 = \frac{TD}{1 + \frac{A_2}{A_1} + \frac{A_3}{A_1}} = \frac{TD}{\frac{A_1 + A_2 + A_3}{A_1}} = \frac{A_1 * TD}{\sum_{i=1}^{3} A_i} \tag{4.7}$$

On déduit le même résultat pour $Drop_2$ et $Drop_3$, pour obtenir en résultat le groupe d'équations (4.8) :

$$\begin{cases} Drop_1 = \frac{A_1 * TD}{\sum_{i=1}^{3} A_i} \\ Drop_2 = \frac{A_2 * TD}{\sum_{i=1}^{3} A_i} \\ Drop_3 = \frac{A_3 * TD}{\sum_{i=1}^{3} A_i} \end{cases} \tag{4.8}$$

Enfin, nous obtenons la forme générale :

$$Drop_i = \frac{A_i * TD}{\sum_{i=1}^{3} A_i} \tag{4.9}$$

Notre objectif n'est pas seulement de savoir combien l'ensemble de files d'attente a rejeté mais de calculer le nombre d'octets à accepter (NAB)) par chaque file d'attente après avoir perdu un certain pourcentage de données au cours d'un certain nombre de tours. Avant de calculer NAB, nous devons d'abord calculer le DP selon l'équation 4.10.

$$DP = \frac{Drop_i}{A_i} \tag{4.10}$$

Après avoir obtenu le pourcentage équilibré de paquets perdus, nous pouvons maintenant déduire la valeur de APB selon l'équation 4.11

$$APB = 1 - DP \tag{4.11}$$

Enfin, nous dérivons NAB selon l'équation 4.12

$$NAB = A_i - Drop_i \tag{4.12}$$

Les exigences pour l'extension équilibrée peuvent être divisées en trois parties :

1. Détection d'une éventuelle perte ;
2. Calcul du taux de perte de paquets après un certain nombre de tours et
3. Estimation du nombre d'octets à accepter dans le tour suivant.

Ces exigences sont prises en compte dans le mécanisme équilibré décrit ci-dessous. Pour détecter une éventuelle perte, le mécanisme équilibré calcule, après un certain nombre de tours, le TD suivant les équations obtenues ci-dessus. Ensuite, après avoir estimé la quantité de données que chaque file d'attente peut accepter du prochain paquet entrant, le NAB est calculé. De même, l'une des étapes les plus importantes du mécanisme équilibré consiste à suspendre momentanément la mise en file d'attente des paquets.

L'algorithme EDWRR peut être divisé en trois procédures principales. Ces procédures dominent le processus de l'algorithme d'ordonnancement. L'idée sous-jacente est la suivante : une fois que le flux de paquets de données arrive dans la file d'attente, il sera classé en fonction de son type puis mis dans la file d'attente correspondante. Dans notre cas, nous choisissons trois types de données : scalaire, audio et vidéo. Une fois que la couche application donne un ordre d'envoi, l'algorithme EDWRR récupère le premier paquet de la file d'attente et l'envoie. Le processus n'est pas encore terminé, l'ordonnanceur retirera de la file d'attente (comme c'est illustré dans l'algorithme 3) des paquets afin de libérer de l'espace pour les prochains paquets entrants. Les pseudo-codes de la fonction améliorée de dépôt de paquets dans les files d'attente et de première capture de l'algorithme d'ordonnancement EDWRR sont donnés respectivement dans l'algorithme 1 et l'algorithme 2 .

En outre, un organigramme du processus de l'algorithme d'ordonnancement EDWRR est illustré dans la Figure 4.4.

Dans l'algorithme 1, EDWRR récupère le type des paquets de données entrants (communication inter-couches). Une fois la mémoire allouée aux paquets, l'algorithme vérifiera son type afin de l'ajouter dans la file d'attente appropriée. Par conséquent, il y a deux cas qui se présentent :

Si la file d'attente est vide, le paquet prendra la première place, sinon l'algorithme récupérera la file d'attente appropriée pour le type du paquet de données. Une fois que le paquet est prêt à être envoyé, il sera renvoyé de la file d'attente appropriée, comme illustré dans l'algorithme 2. Une fois que la liste des files d'attente n'est pas vide, l'ordonnanceur met à jour la valeur $DeficitCounter$ en ajoutant la valeur du quantum.

Ensuite, l'ordonnanceur détermine s'il faut calculer : $AADR$, TD et NAB ou bien passer au tour suivant quand la condition nécessaire de l'algorithme EDWRR n'est pas

Algorithm 1 Enqueue() of Equilibrated-DWRR

Input : Données A_i à mettre en file d'attente pour type : QHS, QHA and QHV
/* Après avoir placé chaque type de données dans la file d'attente correspondante, on calcule la somme des A_i correspondant à chaque type de paquet */
1 : Type = PBA(PACKETBUF_TYPE_DATA) ;
2 : SumA[Type] = SumA[Type] + PacketBufDatalen ; /* SumA selon l'équation 4.1 */
/* On vérifie si les données entrantes ne dépassent pas la condition estimée NAB */
/* Critère d'arrêt de la procédure de mise en file d'attente en testant ToTalDrop calculé selon First-Grab ()*/
3 : **if** $(A[Type] > NAB[Type])$ **and** $(TTDrop \neq 0)$ **then**
4 : Return ;
5 : **end if**
6 : Memory_Alloc(item) ; /* Allouer un bloc de mémoire pour contenir le paquet "item"*/
/* Si la file d'attente est vide, "item" sera le premier à être mis en file d'attente */
7 : **if** Queue is empty **then**
8 : **if** (Type == DATA_TYPE_SCALAR) **then**
9 : Ajouter "item" à QHS
10 : **end if**
11 : **if** (Type == DATA_TYPE_AUDIO) **then**
12 : Ajouter "item" à QHA
13 : **end if**
14 : **if** (Type == DATA_TYPE_VIDEO) **then**
15 : Ajouter "item" à QHV
16 : **end if**
/* sinon le paquet sera mis à la fin de la file d'attente */
17 : **else**
18 : Récupérer le dernier élément de la queue de chaque file d'attente
/* Insérer le nouvel élément entrant */
19 : **if** (Type == DATA_TYPE_SCALAR) **then**
20 : Ajouter l'élément de QHS en queue
21 : **end if**
22 : **if** (Type == DATA_TYPE_AUDIO) **then**
23 : Ajouter l'élément de QHA en queue
24 : **end if**
25 : **if** (Type == DATA_TYPE_VIDEO) **then**
26 : Ajouter l'élément de QHV en queue
27 : **end if**
28 : **end if**
29 : **End**

accomplie. Lors du calcul de ($AADR$, TD et NAB) l'ordonnanceur vérifie (comme mentionné au début de l'algorithme 1) en attendant s'il y a un paquet arrivant dans la file d'attente avec un ADR supérieur au NAB, à ce moment, il suspend momentanément l'algorithme 3) de mise en file d'attente. Après cela, le nombre de tours et le paquet de données d'application de chaque file d'attente sont remis à zéro afin d'accueillir les nouveaux paquets entrants tandis que le paquet qui doit être envoyé est prêt à être retiré

de la file d'attente. Dans l'algorithme 3, l'ordonnanceur vérifie d'abord si la file d'attente n'est pas vide afin de retirer le paquet qui est en tête de liste de la file d'attente. Enfin, le paquet est supprimé, le tampon de la file d'attente est libéré et la valeur $DeficitCounter$ est mise à jour.

Algorithm 2 First_Grab() of Equilibrated-DWRR

Input : File d'attente qui contient le paquet à récupérer Q_i
Output : Premier élément extrait de la file d'attente actuelle "item"
/* On Vérifie si la file d'attente contient des paquets ou non*/
1 : **if** Queue is empty **then** /* On Vérifie si la file d'attente n'est pas vide */
2 : Retourner NULL ;
3 : **elseif** (DC $<$ HS) **then** /* Update the DC value */
4 : $DC = DC + Quantum$;
5 : **else**
6 : **while** (DC $<$ HS) and (LS(CQ) $\neq 0$) **do**
/* On vérifie la file d'attente actuelle, si le tour est terminé, on passe au tour suivant*/
7 : $CQ = (CQ + 1)\%3 + 1$;
8 : **if** (CQ == SQ) **then**
9 : $NRound = NRound + 1$
10 : **end if**
/* Procéder aux tours suivants une fois que la condition n'est pas vérifiée */
11 : **if** (NRound $>$ MaxRound) **then**
12 : **for** i from 1 to NQueue **do**
/* Calculer le taux d'application moyen des trois files d'attente*/
13 : $ADR = A_i/MaxRound$;
14 : $AADR = AADR + ADR$;
15 : **end for**
/* Calculer à la fois TTDrop et le Drop de chaque file d'attente */
/* Free est l'espace libre restant dans chaque file d'attente */
16 : $TTDrop = AADR-(Free+\sum Quantum)$; /* $\sum Q = Q[Queue_1]+Q[Queue_2]+Q[Queue_3]$ */
17 : **for** (i from 1 to NQueue) **do**
18 : $Drop_i = (ADR_i * TTDrop)/AADR$; /* $Drop_i$ selon l'équation 4.9 */
19 : $NAB_i = ADR_i - Drop_i$; /* NAB selon l'équation 4.12 */
20 : **end for**
/* Réinitialiser le nombre de tours et les données d'application */
21 : NRound = 0 ;
22 : **for** (i from 1 to NQueue) **do**
23 : $A_i = 0$;
24 : **end for**
25 : **end if**
26 : **if** (DC $<$ HS) **then**
27 : $DC = DC + Q$;
28 : **end if**
29 : **end while**
30 : Retourner item ; /* Récupérer le paquet de la file d'attente actuelle et le renvoyer */

Algorithm 3 Dequeue() of Equilibrated-DWRR

Input : Élément (paquet) qui sera retiré de la file d'attente " item "
/* Vérifier s'il y a un élément à retirer depuis la file d'attente */
1 : **if** item $\neq$ NULL **then**
/* Mettre à jour les champs de l'ordonnanceur */
2 : DC =DC – Queue_Buffer_Datalen(item) ;
/* Espace libre de la file d'attente actuelle qui vient de retirer le paquet */
3 : QueueBuffer_Free(item) ;
/* Libérer le bloc mémoire */
4 : Memory_Free (item) ;
5 : **end if**

4.4.2 Complexité de l'algorithme EDWRR

La complexité de l'algorithme EDWRR peut être définie comme suit :

Lorsque le taux de paquets et/ou le nombre de paquets augmente, cela n'affectera pas la complexité de l'algorithme qui est $O(1)$.

Lorsque la taille du paquet augmente, nous avons deux cas qui se présentent :

- Lorsque la taille du paquet en tête d'une file d'attente est inférieure à la valeur du quantum, la complexité reste la même ($O(1)$).
- Lorsque la taille du paquet en tête d'une file d'attente est supérieure à la valeur quantum (qui représente le pire des cas), le temps d'exécution varie linéairement proportionnellement à N. Ainsi, nous obtenons une complexité d'ordre $O(N)$, où N est le rapport entre la taille du paquet et la valeur quantum.

4.5 Résultats de simulation et discussion

Dans cette section, les résultats les plus significatifs d'une étude de simulation de la politique d'ordonnancement EDWRR sont présentés.

4.5.1 Environnement de travail

Les performances de l'algorithme EDWRR sont comparées aux performances des deux algorithmes d'ordonnancement DWRR et FIFO sous le simulateur de réseau COOJA [92]. COOJA est considéré comme un émulateur car il teste exactement le code binaire d'une classe qui s'exécuterait sur une plateforme réelle de capteurs IoT connus sous le nom de motes Z1 sous le système d'exploitation Contiki [71]. De plus, cela nous donne une flexibilité totale dans l'évaluation des environnements radio et des topologies. Pour le modèle de propagation radio, nous utilisons le modèle Unit Disk Graph Model : Distance Loss [285]. Dans notre espace carré de réseau de simulation (100m x 100m), le noeud 1 est un noeud Sink (racine) situé sur le bord du réseau. La portée de la communication radio est de 50 m. Six niveaux de débit de trafic, i.e. 2 ; 4 ; 6 ; 8 ; 10 et 12 pkt/seconde, ont été pris en compte dans les simulations avec une taille de données de 50 à 100 octets.

Pour les deux files d'attente audio et vidéo qui contiennent comme type de trafic RT, le débit de trafic a été défini avec le débit binaire VoIP. La simulation a duré 300 secondes. Les autres paramètres de simulation sont résumés dans le tableau 4.2.

TABLE 4.2 – Paramètres de simulation

Paramètre	***Valeur***
Couche MAC	802.14.5
Simulateur	COOJA sous Contiki OS (3.0)
Environnement radio	UDGM (Unit Disk Graph Medium)
Type de capteurs	$Z1$
Zone de déploiement	$100m \times 100m$
Nombre de noeuds	[10, 40]
Nombre de noeuds racines	1
Portée de transmission	$50m$
Taille des paquets	$10 - 100\,bytes$
Taux de trafic	2, 4, 6, 8, 10 et $12 Pkt/second$
Débit VoIP (audio et vidéo)	$8.4 kbps$
Temps de simulation	$300s$

Nous avons effectué une large série de mesures dans lesquelles nous faisons varier l'ensemble de l'intervalle de génération de paquets (Packet generation Interval (PI)) ou le débit de données (le nombre de paquets par seconde), le nombre de noeuds et la taille des données en octets ainsi que la valeur de $Quantum[i]$. Afin d'évaluer l'impact de l'utilisation de la nouvelle politique d'ordonnancement EDWRR sur différents aspects des systèmes IoMT. Dans cette section, les résultats de quatre scénarios importants sont présentés et discutés.

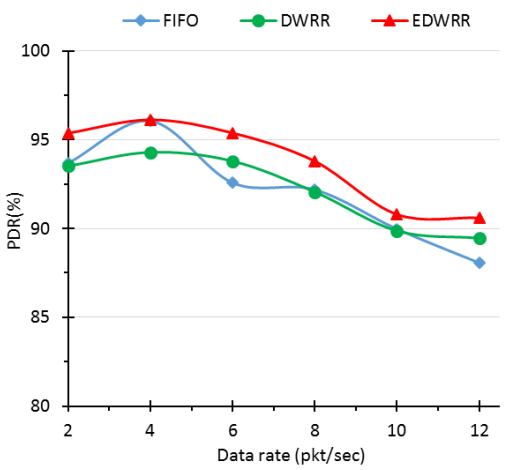
Dans le premier scénario, les résultats sont obtenus en faisant varier la valeur de *PI* tout en utilisant une valeur fixe de densité de réseau. Le second montre les résultats obtenus en faisant varier le nombre de noeuds dans un intervalle de 10 à 40 noeuds pour une valeur fixe de *PI*. Pour le troisième scénario, nous avons effectué des séries de mesures tout en variant la taille des paquets et en utilisant une valeur fixe de *PI* car c'est un facteur crucial pour analyser le comportement de l'algorithme EDWRR. Le quatrième scénario montre les résultats obtenus en faisant varier la valeur du $Quantum[i]$ pour une valeur fixe de *PI*. Chaque type de paquet a une durée de vie différente, car cela semble plus réaliste et principalement en raison de sa taille. Il devient évident que, par exemple, une seule file d'attente contenant des paquets volumineux tels que le streaming vidéo conduit rapidement à la saturation de la file d'attente, empêchant la gestion des autres types de paquets. Ainsi, la perte totale de paquets (TD) augmentera et influencera toutes les ressources et les exigences des systèmes IoMT telles que le délai, le taux des paquets délivrés...etc.

4.5.2 Les métriques de performances

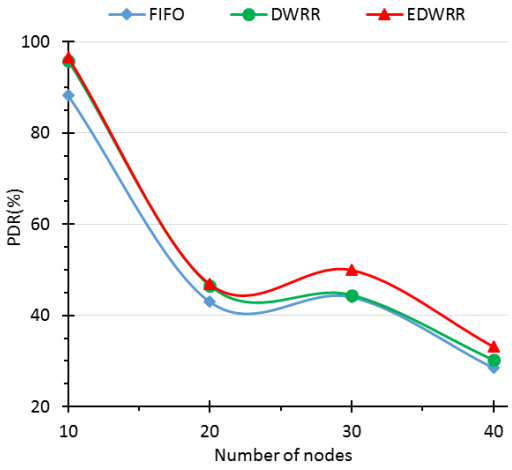
Afin d'illustrer l'impact du type de paquets communiqués par la couche application sur le comportement des différentes politiques de mise en file d'attente et leur degré d'équité,

nous avons augmenté la charge du canal en variant la vitesse de génération des données de 2 à 12 pps (pps : nombre de paquets par seconde). En outre, nous avons évalué les métriques de performance (PDR, délai de bout en bout et débit) en termes du nombre de noeuds et de la taille des données. Ces deux paramètres peuvent augmenter la charge de trafic dans la file d'attente, ce qui peut entraîner des problèmes de saturation.

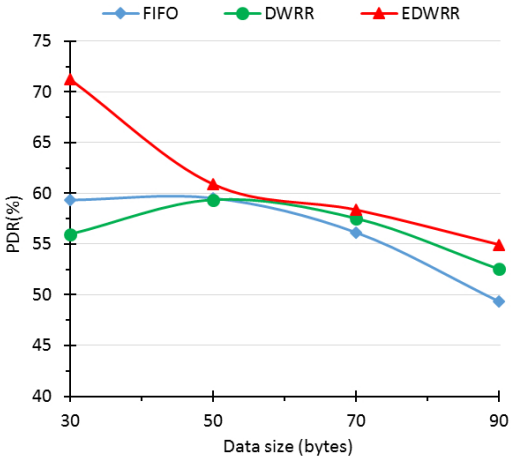
a) Taux de paquets délivrés (PDR)



(a) PDR vs. Débit de données



(b) PDR vs. Nombre de noeuds



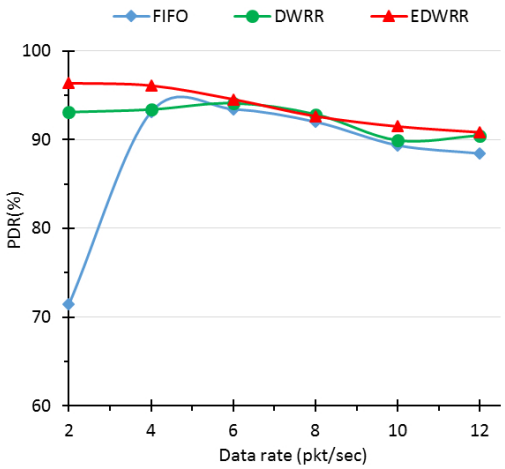
(c) PDR vs. Taille des données

FIGURE 4.5 – Taux de livraison des paquets pour la transmission de données multimédias

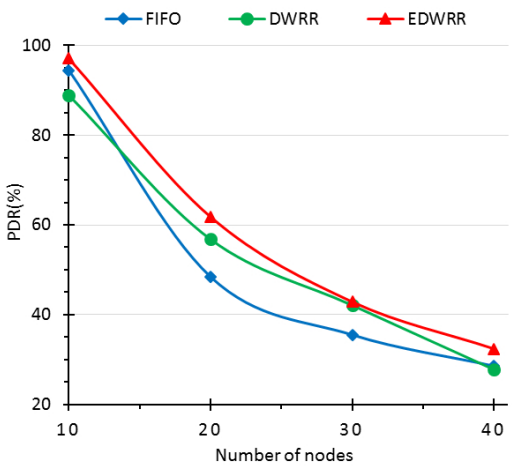
Dans la Figure 4.5, nous observons le PDR des trames multimédias avec diverses politiques de mise en file d'attente utilisant différents paramètres de mesure. Techniquement, la variation du débit de données (Figure 4.5a) et de la taille des données (Figure 4.5c) a le même impact sur la gestion des files d'attente car les deux peuvent surcharger rapidement les files d'attente. En commençant par la Figure 4.5a, une légère augmentation de 2 à 4 pps suivie d'une diminution du PDR peut être observé.

EDWRR atteint de meilleurs résultats que DWRR et FIFO lorsque le taux de paquets augmente. Cela est principalement dû au concept d'équilibration qui tend à équilibrer

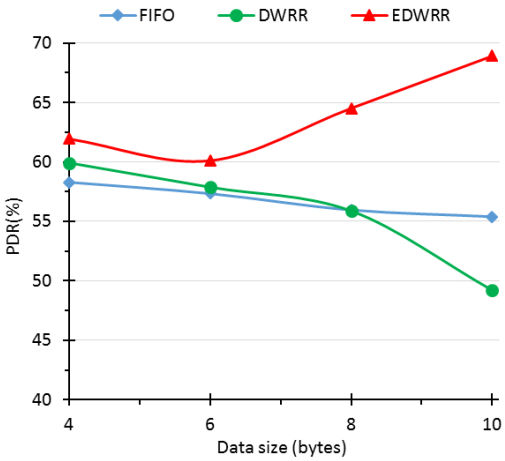
le rapport des paquets perdus entre toutes les files d'attente en partageant leur espace libre restant. De plus, lorsque le nombre de noeuds augmente dans le réseau, la collision des paquets augmente également, ce qui peut affecter le PDR comme représenté dans la Figure 4.5b.



(a) PDR vs. Débit de données



(b) PDR vs. Nombre de noeuds



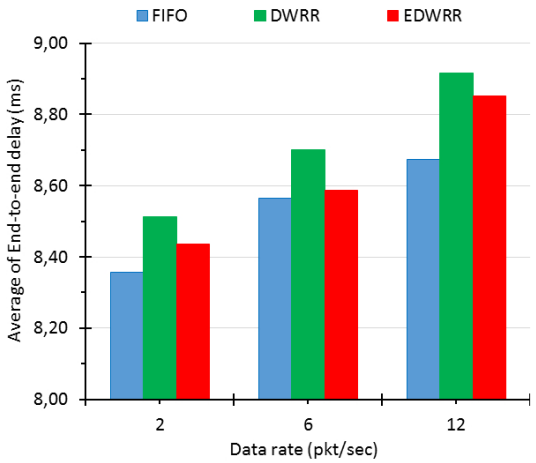
(c) PDR vs. Taille des données

FIGURE 4.6 – Taux de livraison des paquets pour la transmission de données scalaires

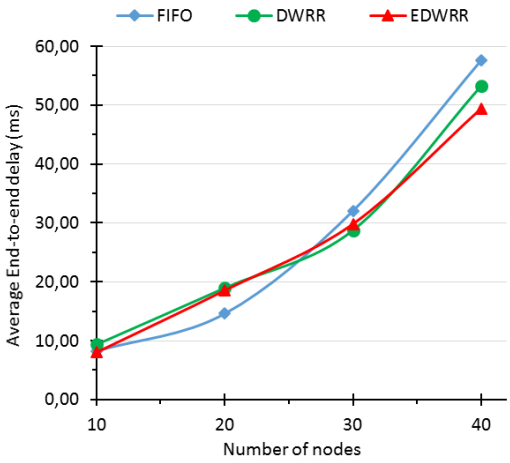
En ce qui concerne le PDR de transmission de données scalaires représenté dans la Figure 4.6, il a largement les mêmes performances que le PDR multimédia. En commençant par la Figure 4.6a, le PDR de EDWRR est plus élevé de 25% par rapport à celui du FIFO et DWRR lorsque la vitesse de transmission est comprise entre 2 et 4 pps. Contrairement au DWRR et au FIFO, EDWRR montre une diminution constante tout au long de la variation de débit tout en donnant de meilleurs résultats que les deux autres algorithmes. Cela est dû à sa politique d'ordonnancement qui tend à résoudre le problème de file d'attente unique dans le cas de FIFO et également l'absence de priorité. Dans la Figure 4.6b, les trois politiques d'ordonnancement illustrent une diminution du PDR lorsque la densité du réseau augmente et EDWRR fournit les meilleurs résultats. La Figure 4.6c présente différents tracés du PDR de la politique d'ordonnancement proposée par rapport aux DWRR et FIFO dans l'intervalle de taille de données [4 octets ; 10 octets]

pour les données scalaires et [30 octets ; 90 octets] pour les données multimédias. Nous observons qu'une fois que le flux multimédia diminue, il fournira plus d'espace pour le flux scalaire et son PDR augmentera comme illustré dans la Figure 4.6c.

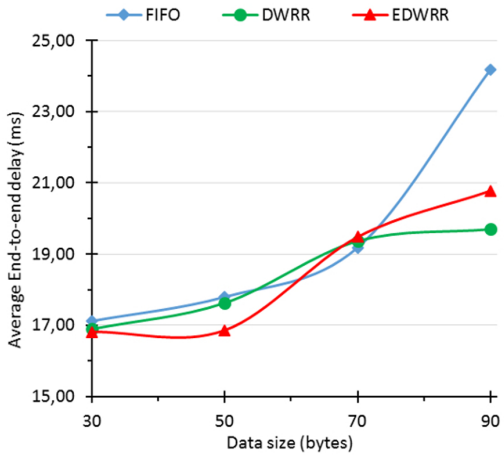
b) Délai de bout en bout



(a) Délai vs. Débit de données



(b) Délai vs. Nombre de noeuds



(c) Délai vs. Taille des données

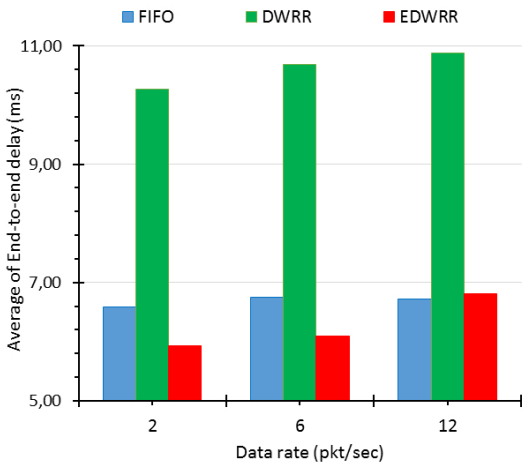
FIGURE 4.7 – Délai pour la transmission de données multimédias

EDWRR implique une limitation de la perte des données de manière équilibrée par rapport à DWRR conventionnel. Malgré l'inclusion de plusieurs étapes supplémentaires dans EDWRR, il consomme toujours moins de temps lors de la livraison des paquets par rapport à DWRR. Néanmoins, il reste toujours plus lent que FIFO qui n'intègre aucune gestion de file d'attente. Cela peut être clairement vu dans la Figure 4.7, qui contient une comparaison entre ces algorithmes. Dans cette comparaison, nous avons utilisé différents paramètres de mesures telles que la vitesse de transmission des paquets, la taille des données et le nombre de noeuds. Les trois cas d'évaluation montrent une augmentation significative du délai chaque fois que la valeur des paramètres considérés est augmentée. Dans la Figure 4.7a, EDWRR atteint un délai inférieur à celui de DWRR mais supérieur à celui de FIFO.

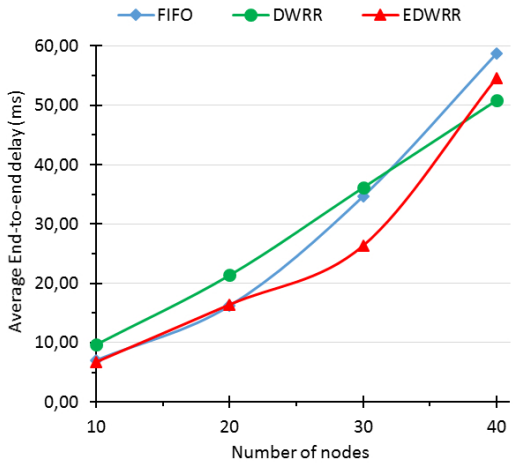
Nous expliquons ces résultats par le fait que la politique de mise en file d'attente de "EDWRR" fournit de bonnes performances dans la gestion de la file d'attente multimédia lorsque la charge de trafic augmente en comparant avec DWRR. Ainsi pour avoir un délai plus élevé que FIFO, cela est principalement dû au fait qu'il n'y a qu'une seule file d'attente partagée dans FIFO tandis que DWRR et EDWRR prennent du temps pour gérer le système multi-files d'attente. Cependant, dans le cas d'un réseau dense, FIFO montre un comportement différent après avoir été le premier a consommé moins de délai par rapport à DWRR et EDWRR, en consommant plus de délai comme le montre la Figure 4.7b. Cela illustre que, lorsque le réseau devient plus dense ($>$ 25 noeuds), la file d'attente FIFO est progressivement saturée. En effet, FIFO ne différencie pas et ne donne pas la priorité aux types de flux en plus des caractéristiques des données multimédias qui sont intermittentes et en rafale et cela entraîne un délai de mise en file d'attente important. La Figure 4.7c montre comment le délai du trafic multimédia varie lorsque la taille du flux multimédia augmente. Les deux stratégies de mise en file d'attente basées sur DWRR affichent un délai nettement inférieur à FIFO, ainsi, après que le flux vidéo atteint plus de 70 octets, FIFO consomme plus de temps. Cela peut être dû au fait que les données en temps non réel occupent la première place dans la file d'attente et que les données sont plus privilégiées (par exemple un contenu multimédia), ce qui peut entraîner des paquets livrés avec un délai épuisé dans les files d'attente. Cependant, DWRR et EDWRR prennent en considération la priorité du flux multimédia et le servent avec le bon quantum.

Nous observons que DWRR prend le pire des cas en consommation de délai dans les deux types de données scalaires et multimédias en ce qui concerne la variation de la vitesse de transmission (en pps), comme est illustré dans les Figures 4.7a et 4.8a. Contrairement aux résultats présentés dans la Figure 4.7, EDWRR atteint le délai minimum lorsqu'il s'agit du type scalaire comme illustré dans la Figure 4.8. Intuitivement, cela montre comment EDWRR donne aux données scalaires la chance d'accéder à la file d'attente. Dans la Figure 4.8b, le délai des politiques d'ordonnancement augmente quand le nombre de noeuds augmente. En règle générale, lorsque les noeuds saturent le réseau par leurs paquets, les algorithmes d'ordonnancement prennent beaucoup de temps pour gérer toutes les files d'attente, en particulier pour celles qui ont des stratégies de mise en file d'attente multiple (dans notre cas DWRR et EDWRR). De plus, la transmission multimédia prend beaucoup plus de temps par rapport au scalaire car elle est caractérisée par une grande taille de données et cela est visible à la fois sur les Figures 4.7c et 4.8c.

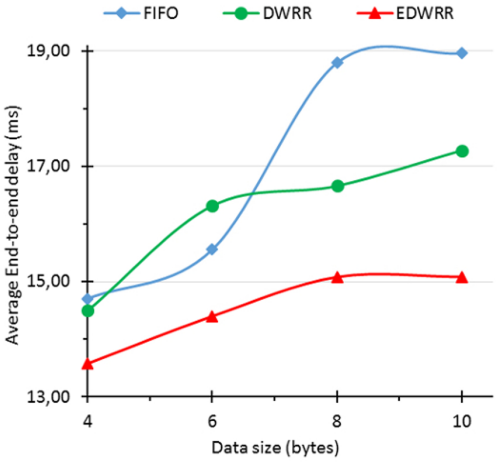
Dans la Figure 4.9, une valeur de 6 pps pour PI est utilisée et la valeur de $Quantum[i]$ varie. Les résultats montrent l'impact de diverses valeurs de quantums sur les techniques de gestion des files d'attente DWRR et EDWRR sur le délai moyen de bout en bout. Sur la même figure, nous pouvons observer une légère diminution du délai moyen dans l'intervalle quantum des deux scalaires [10 octets ; 20 octets] et multimédia [50 octets ; 70 octets] respectivement suivis d'une augmentation lorsque le quantum varie entre [20 octets ; 40 octets] pour les données scalaires et [70 octets ; 120 octets] pour le flux multimédia. Comme on peut le constater sur les résultats obtenus, EDWRR fonctionne mieux que DWRR en termes de délai. Cela peut être expliqué que DWRR ne fonctionne pas conformément aux délais et à la gestion active des paquets.



(a) Délai vs. Débit de données



(b) Délai vs. Nombre de noeuds



(c) Délai vs. Taille des données

FIGURE 4.8 – Délai pour la transmission de données scalaires

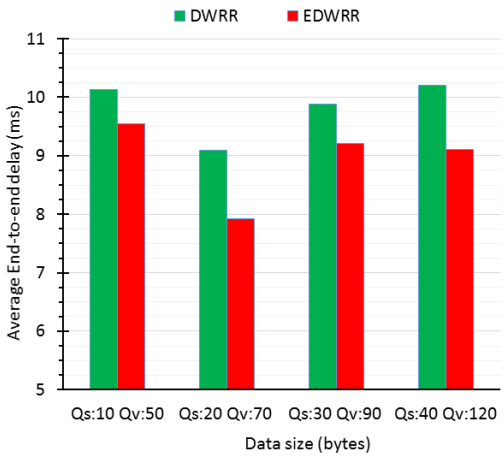
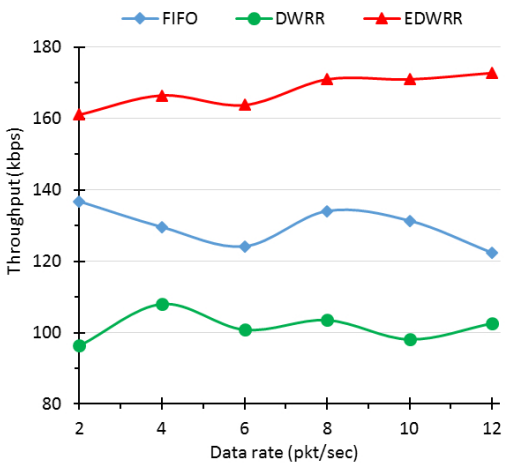
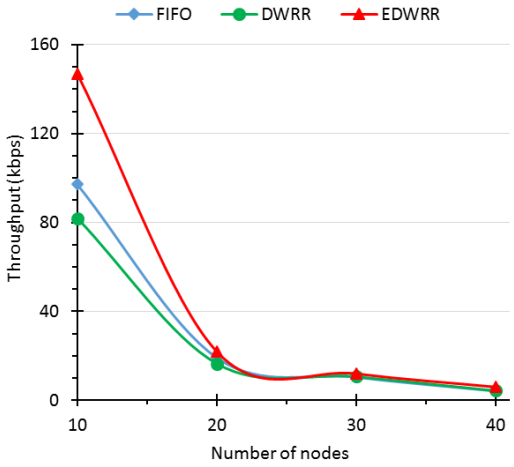


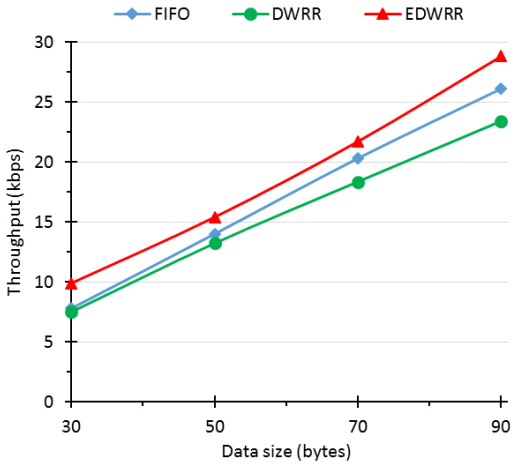
FIGURE 4.9 – Délai moyen de bout en bout en fonction de différents quantums pour un trafic mixte : scalaire et multimédia (bytes)



(a) Débit vs. Débit de données



(b) Débit vs. Nombre de noeuds



(c) Débit vs. Taille des données

FIGURE 4.10 – Débit pour la transmission de données multimédias

c) Débit de données

La Figure 4.10 est une représentation du débit expérimenté par les flux d'application à travers les deux techniques de gestion de file d'attente et FIFO, où le débit est représenté en fonction de la vitesse de transmission des données, de la taille des données et du nombre de noeuds. Par ailleurs, le débit résultant concerne le trafic scalaire ainsi que le flux multimédia. Dans les trois cas de politiques d'ordonnancement donnés sur les Figures 4.10a, 4.10b et 4.10c, nous pouvons remarquer un débit significativement plus élevé pour EDWRR que pour FIFO et DWRR lorsque le nombre de noeuds augmente.

En ce qui concerne le graphe du débit représenté dans la Figure 4.10a, nous observons clairement que le débit reste presque le même lorsque la vitesse de transmission des données augmente. Les résultats expliquent dans quelle mesure la gestion des files d'attente gère cette vitesse du trafic multimédia. Dans ce cas, le meilleur débit a été atteint par EDWRR dans lequel l'ordonnanceur FlowQueue permet un partage équitable de l'espace libre restant entre les files d'attente.

Dans la Figure 4.10b, la diminution du débit est justifiée lorsque le trafic surcharge la

bande passante partagée. Dans le cas d'une taille volumineuse des données illustrée dans la Figure 4.10c, le débit des trois algorithmes a été sensiblement amélioré. Logiquement, lorsque la taille des données traversant le réseau augmente, le débit calculé pour ce type de données augmente également. Ainsi, lorsque la taille des paquets augmente, la différence entre les performances de débit FIFO et DWRR augmente tandis que celle de l'algorithme EDWRR reste toujours supérieure et l'avantage de notre algorithme proposé EDWRR devient évident.

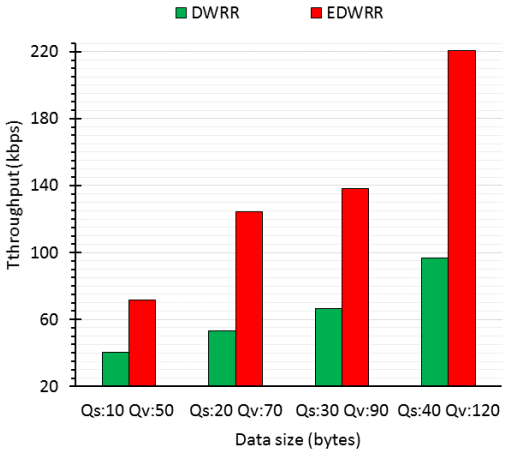


FIGURE 4.11 – Débit en fonction de différents quantums pour un trafic mixte : scalaire et multimédia (bytes)

La Figure 4.11 montre l'impact des différentes valeurs quantums sur le débit du réseau dans les techniques de gestion des files d'attente DWRR et EDWRR . Dans ce scénario, lorsque la valeur du quantum augmente, l'algorithme EDWRR devient plus avantageux que celui de DWRR. Ce résultat prouve l'efficacité de la politique de gestion de file d'attente EDWRR en matière de données multimédias.

4.5.3 Résultats comparatifs de "EDWRR" avec les travaux connexes

Une analyse plus approfondie a été examinée dans cette sous-section afin de comparer nos résultats avec les travaux antérieurs rapportés dans la littérature et cela est illustré dans le tableau 4.3. Les résultats comparatifs ont eu tendance à se concentrer sur la comparaison de nos travaux avec les approches d'ordonnancement dans les réseaux LTE, ceci est en raison du manque d'optimisation d'ordonnancement dans les réseaux IoMT.

La première série d'analyses a mis en évidence l'impact des flux VoIP sur le débit moyen. Nous avons ajusté nos paramètres de simulation à la suite de cinq travaux comparatifs, le premier est en [316] où le flux VoIP généré est codé à un taux de 8,4 kbps avec une densité de réseau égale à 10, 20, 30, 40, 50 et 60 utilisateurs pendant 30 secondes de temps de simulation. Notre ordonnanceur EDWRR montre une amélioration significative pour tous les flux impliqués par rapport à l'ordonnanceur Queue-HOLM LWDF, même lorsque le réseau est chargé de 60 utilisateurs. Le deuxième ajustement était similaire à celui de [318] en considérant 31 noeuds comme une taille de réseau tandis que la charge de trafic varie de 200 à 1000 kbps pendant 100 secondes de temps de simulation. Comme fait intéressant, notre algorithme d'ordonnancement EDWRR a révélé des résultats re-

marquables que FIFO, RED et WRED en termes de délai moyen de bout en bout, de débit moyen et de taux moyen de livraison de paquets. Dans notre troisième comparaison qui était avec [319], nous avons défini le modèle de trafic du débit binaire VoIP à 8,4 kbps sur 25 utilisateurs VoIP (de 5 à 25) pendant 100 secondes. Les résultats de simulation ont montré que EDWRR ne répond pas seulement aux exigences de QoS pour les services en temps réel (application VoIP) mais surpasse également E-MQS et les ordonnanceurs FLS, M-LWDF, EXP/PF en termes de délai, de taux de perte de paquets et de débit et indice d'équité de Jain calculés en fonction de [323]. D'autres résultats ont confirmé l'efficacité de "EDWRR", dans lequel nous avons utilisé les mêmes paramètres de simulation supposés dans [321] tels que le nombre d'utilisateurs (UE) qui a varié entre 10 et 60 utilisateurs avec le même débit binaire du VoIP utilisé dans une durée de 30 secondes. L'évaluation des performances de "EDWRR" montre un meilleur débit moyen par rapport à celui de l'extension de l'algorithme QCI.

Dans une dernière comparaison avec [322], EDWRR montre un net avantage en termes de délai moyen de livraison des paquets et de taux de perte de paquets par rapport aux deux algorithmes de gestion active de file d'attente (AQM) DRR et SFQ lors de l'augmentation du nombre de noeuds 5 à 15.

La comparaison de nos résultats avec ceux des travaux susmentionnés a été très prometteuse. L'algorithme d'ordonnancement EDWRR ne traite clairement pas les caractéristiques vidéo, néanmoins, il prend en compte le trafic en temps réel (RT) et en temps non réel (NRT). Nous pensons que "EDWRR" pourrait être une solution formelle aux exigences de QoS des réseaux IoMT en fournissant des performances de réseau satisfaisantes.

TABLE 4.3 – Comparaison entre EDWRR avec d'autres algorithmes d'ordonnancement

Paramètre de performance	Débit moyen (bit/s) pour un flux VoIP					
Nombre d'utilisateurs/Algorithme	10	20	30	40	50	60
Queue-HOLM-LWDF [316]	≈ 9400	≈ 9000	≈ 9400	≈ 8800	≈ 9001	≈ 8500
VT-M-LWDF [316]	≈ 9000	≈ 8600	≈ 9000	≈ 9001	≈ 9000	≈ 9000
M-LWDF [316]	≈ 9000	≈ 9000	≈ 8700	≈ 9000	≈ 9000	≈ 8900
EDWRR	76320	50400	38160	21600	18720	16560

Paramètre de performance	Délai moyen de bout en bout (sec)				
Charge de trafic (kbps)/Algorithme	200	400	600	800	1000
FIFO [318]	≈ 0.2	≈ 6.5	≈ 4.1	≈ 3.5	≈ 3.5
RED [318]	≈ 0.8	≈ 0.5	≈ 2.5	≈ 1.5	≈ 2.7
WRED [318]	≈ 0.7	≈ 3.4	≈ 1.3	≈ 1.4	≈ 4
EDWRR	0.425	0.431	0.442	0.393	0.446
Paramètre de performance	Débit Moyen (bit/s)				
Charge de trafic (kbps)/Algorithme	200	400	600	800	1000
FIFO [318]	≈ 60000	≈ 205000	≈ 260000	≈ 100000	≈ 24000
RED [318]	≈ 110000	≈ 215000	≈ 240000	≈ 130000	≈ 135000
WRED [318]	≈ 112000	≈ 190000	≈ 255000	≈ 140000	≈ 147000
EDWRR	102960	235440	258480	216000	232560
Paramètre de performance	PDR moyen (%)				
Charge de trafic (kbps)/Algorithme	200	400	600	800	1000
FIFO [318]	≈ 30%	≈ 43%	≈ 33%	≈ 11%	≈ 3%

TABLE 4.3 – Comparaison entre EDWRR avec d'autres algorithmes d'ordonnancement

RED [318]	≈ 51%	≈ 45%	≈ 35%	≈ 15%	≈ 12%
WRED [318]	≈ 55%	≈ 45%	≈ 34%	≈ 14.5%	≈ 13%
EDWRR	81.05%	71.84%	59.39%	55.05%	51.06%

Paramètre de performance	Taux de perte de paquets vs. nombre d'utilisateurs VoIP				
Nombre d'utilisateurs/Algorithme	5	10	15	20	25
FLS [319]	≈ 0.38	≈ 0.12	≈ 0.05	≈ 0.04	≈ 0.1
MLWDF [319]	≈ 0.65	≈ 0.47	≈ 0.35	≈ 0.3	≈ 0.3
EXP/PF [319]	≈ 0.5	≈ 0.47	≈ 0.3	≈ 0.24	≈ 0.19
E-MQS [319]	≈ 0.4	≈ 0.31	≈ 0.2	≈ 0.15	≈ 0.12
EDWRR	0.02	0.03	0.007	0.017	0.0245
Paramètre de performance	Délai vs. nombre d'utilisateurs VoIP (ms)				
Nombre d'utilisateurs/Algorithme	5	10	15	20	25
FLS [319]	≈ 10.5	≈ 9.4	≈ 8.1	≈ 7.8	≈ 7.5
MLWDF [319]	≈ 1.6	≈ 1.7	≈ 1.75	≈ 1.8	≈ 1.95
EXP/PF [319]	≈ 1.6	≈ 1.65	≈ 1.75	≈ 1.65	≈ 1.75
E-MQS [319]	≈ 1.6	≈ 1.7	≈ 1.75	≈ 1.8	≈ 1.95
EDWRR	0.08	0.3	0.5	0.7	0.8
Paramètre de performance	Débit (bps) vs. nombre d'utilisateurs VoIP				
Nombre d'utilisateurs/Algorithme	5	10	15	20	25
FLS [319]	≈ 57000	≈ 95000	≈ 128000	≈ 165000	≈ 191000
MLWDF [319]	≈ 58000	≈ 91000	≈ 126000	≈ 161000	≈ 200000
EXP/PF [319]	≈ 57500	≈ 96000	≈ 121000	≈ 160000	≈ 198000
E-MQS [319]	≈ 57500	≈ 93000	≈ 130000	≈ 163000	≈ 200000
EDWRR	294480	308160	224640	196560	269280
Paramètre de Performance	Indice d'Équité vs nombre d'utilisateurs VoIP				
Utilisateurs VoIP/Algorithme	5	10	15	20	25
E-MQS [319]	≈ 0.59	≈ 0.48	≈ 0.53	≈ 0.48	≈ 0.51
EDWRR	0.8	0.9	0.93	0.95	0.96

Paramètre de performance	Débit moyen (bit/s) pour un flux VoIP					
Nombre d'utilisateurs/Algorithme	10	20	30	40	50	60
QCI-Delay -LOG-PLR [321]	≈ 9100	≈ 8500	≈ 9100	≈ 8800	≈ 9000	≈ 9100
QCI-Delay-LINEAR-PLR [321]	≈ 8500	≈ 9200	≈ 8900	≈ 8900	≈ 8500	≈ 8800
QCI-MLWDF [321]	≈ 8300	≈ 9000	≈ 9100	≈ 8800	≈ 8600	≈ 8800
EDWRR	76320	50400	38160	21600	18720	16560

Paramètre de performance	Délai moyen (ms)			Taux de perte de paquets (pkt/s)		
Nombre d'utilisateurs/Algorithme	5	10	15	5	10	15
DDR [322]	15.2	15.21	15.52	0.1	0.17	0.2
SFQ [322]	11.92	12.43	12.46	0.2	0.18	0.17
EDWRR	2.8	8.9	11.63	0.033	0.083	0.11

4.6 Conclusion et perspectives

Dans ce chapitre, un algorithme d'ordonnancement EDWRR (Equilibrated Deficit Weighted Round Robin) est proposé pour la transmission multimédia dans une infrastructure IoMT. L'algorithme proposé prend en compte les exigences de QoS et les priorités de contexte de diverses applications IoMT afin de les mapper à des classes de trafic distinctes en fournissant une allocation de ressources équilibrée. EDWRR équilibre le pourcentage de perte en surveillant les trois files d'attente en utilisant une limitation de l'excès des paquets qui est exprimée en nombre d'octets à accepter.

De plus, EDWRR équilibre progressivement la quantité d'espace libre entre les files d'attente dédiées aux trafics RT et NRT afin de donner plus de chance aux nouveaux paquets entrants tout en les insérant dans les files d'attente correspondantes. L'algorithme est comparé avec l'algorithme DWRR, FIFO, ainsi, une comparaison supplémentaire a été effectuée avec certains algorithmes d'ordonnancement les plus récents. Les résultats montrent des améliorations remarquables de notre proposition EDWRR en offrant un taux de perte de paquets plus faible et de meilleures performances en termes de PDR, de délai de bout en bout et de débit moyen par rapport aux autres politiques d'ordonnancement.

Conclusion Générale

Conclusion Générale

Vu que le protocole de routage est l'un des principaux piliers de l'architecture de réseau, et prévoyant avec confiance sa nécessité pour les réseaux LLN, le protocole de routage IPv6 pour les LLN (RPL) est rapidement devenu le protocole de routage de facto pour IoT. Par conséquent, le protocole RPL a tendance de jouer un rôle clé pour soutenir l'infrastructure d'un nombre énorme d'applications IoT potentielles, dans des environnements réguliers et difficiles, y compris les applications en temps réel dans des zones inaccessibles avec une distribution uniforme et non uniforme des noeuds dans les réseaux à grande échelle. Cependant, RPL souffre toujours de certains problèmes qui peuvent avoir des conséquences rigoureuses sur la fiabilité des réseaux, tels que l'incapacité d'être une solution de routage rentable pour prendre en charge les exigences de QoS des applications multimédias.

L'objectif principal de cette thèse est d'améliorer les performances des protocoles de routage standards actuels de l'IoT, à savoir le protocole de routage RPL et l'adapter dans un contexte plus exigeant en particulier dans le paradigme d'IoMT en tenant compte de la croissance aiguë des protocoles et d'applications au sein du paradigme IoT. Cependant, parmi ces protocoles, le protocole de routage RPL qui a été particulièrement l'objet de cette thèse. Par la suite, la connotation IoT, les applications et l'évolution de la pile protocolaire d'IoT ont été discutées. Par ailleurs, nous avons détaillé tous les protocoles de la pile IoT afin de montrer comment les efforts cumulés ont contribué progressivement aux protocoles LLN pour aboutir à cette pile. En outre, nous avons discuté les outils et méthodes actuels d'IoT, en mettant en évidence les principales caractéristiques du système d'exploitation IoT et ses différentes installations de communication. Ainsi, nous avons surligné les vrais dispositifs utilisés lors d'une expérimentation d'un environnement IoT, à côté de l'émulateur COOJA qui est largement utilisé et représente le simulateur choisi pour mener les expériences de cette étude.

Dans le cadre de la maîtrise de l'état de l'art, nous avons proposé une classification des différents protocoles de routage conçu dans l'écosystème IoT en étudiant dans chaque classe une variété de protocoles de routage. Le protocole RPL étant le thème principal de cette thèse, plus de détails et de discussion ont été donnés afin d'ouvrir la voie à une meilleure compréhension des problèmes de recherche dans cette thèse. Subséquemment, nous avons examiné une variété de travaux et de solutions proposés pour des améliorations du protocole RPL, en révélant les conséquences significatives des problèmes traités sur RPL, ainsi que les pistes potentielles des différents travaux connexes afin de mettre en lumière certains défis non résolus.

Les applications IoMT nécessitent la conception de protocoles de communication efficaces offrant un certain niveau de QoS. Ce n'est pas une tâche triviale compte tenu des défis et contraintes uniques imposés par le paradigme des IoMT et les exigences de com-

munication multimédia. Ainsi, dans l'IoMT, la communication multimédia est basée sur la distribution de contenus multimédias (vidéo, photos, sons, texte) via différents dispositifs connectés. Ce type de réseaux 'IoMT' est beaucoup plus restreint en ressources que les réseaux IoT.

Dans cette thèse, nous avons discuté de plusieurs problèmes de communication dans le domaine IoT ainsi qu'à leur infaisabilité dans le domaine IoMT en mettant l'accent sur le problème de routage. En général, ces protocoles doivent prendre en charge une ou plusieurs contraintes de QoS imposées par les applications IoMT. Parmi ces contraintes, nous citons les contraintes d'énergie, de bande passante, de délai et de la probabilité de perte de données. Le problème de base est donc de trouver un chemin qui satisfasse les multiples contraintes de routage des données multimédias qui sont caractérisées par leur contenu volumineux. Cependant, les protocoles de routage conçu pour les systèmes IoT garanties une QoS pour les données scalaires, ce qui est complètement différent lorsque les flux multimédia (image/audio/vidéo) sont pris en compte. En fait, ils doivent traiter de grandes tailles de données (rafales de données) ayant des exigences de QoS différentes. Cependant, ces protocoles doivent être repensés pour convenir aux différentes exigences des flux multimédia.

Par conséquent, cette thèse a contribué à une étape triviale vers ce problème en proposant dans notre première contribution une amélioration du protocole de routage RPL pour les IoMTs appelée Free BandWidth RPL (FreeBW-RPL). Ainsi, une nouvelle OF à charge équilibrée appelée FreeBW pour le protocole RPL basée sur le calcul de la bande passante (BD) libre au niveau de la couche réseau en fonction du débit de données circulant tout au long du chemin de routage. Cette OF à charge équilibrée utilise une technique du noeud parent préféré lors de la surcharge d'un chemin de routage tout en permutant le chemin encombré afin de garantir une meilleure répartition de la charge des flux multimédias entre tous les noeuds du réseau et une durée de vie de la batterie prospérant pour une survie plus longue. La fonction d'objectif (OF) implémentée a été testée à l'aide d'un ensemble de métriques sur un réseau de noeuds à sauts multiples. Par conséquent, cette contribution répondait aux questions de recherche présentées au Chapitre 1. En effet, nous avons considéré un protocole de routage avec QoS : (i) visant à fournir une nouvelle métrique de routage envisageable pour un routage satisfaisant une QoS d'un trafic multimédia, (ii) prenant en charge les données en temps réel (image/audio/vidéo) et (iii) maximisant la fiabilité et la qualité des données multimédias.

En changeant de couche protocolaire dans la pile d'IoT depuis la couche réseau vers la couche MAC, notre deuxième contribution consiste à traiter la gestion d'ordonnancement des flux RT et non RT. Comme nous avons surligné auparavant, parmi les contraintes de QoS imposées par les applications IoMT est le taux de perte des données. La perte de paquets peut entraîner une dégradation de la QoS dans les applications multimédias car les données peuvent avoir différents niveaux d'importance et la perte aléatoire peut affecter éventuellement des données plus importantes. D'ou provient la nécessité de différencier le trafic des applications IoMT en fonction de leurs contextes environnementaux variant dynamiquement.

L'objectif du système de gestion de données multimédias est de permettre un stockage et une manipulation efficace en utilisant des données multimédias sous toutes leurs formes variées. Cette hétérogénéité du trafic peut nécessiter un type de priorité spécifique entre chaque type de trafic, i.e. les files d'attente sont allouées en fonction du type de

trafic multimédia afin d'attribuer une priorité à chacun. Par conséquent, le trafic avec la priorité la plus élevée peut consommer plus de ressources mémoire que les autres types, provoquant un taux élevé de perte de paquets. Le type de paquet de données est communiqué par la couche application. Deux modèles de trafic sont traités : le trafic RT (VoIP comme audio) et le trafic NRT (scalaire). Après un certain nombre de tours, certaines files d'attente seront surchargées, notamment les files d'attente qui sont allouées pour le trafic RT, lorsque certaines d'entre elles seront libérées d'espace. Ce dernier provoque une gestion inéquitable des différentes files d'attente en augmentant le taux élevé de perte des nouveaux paquets entrants et en gaspillant l'espace libre restant des files d'attente allouées au trafic NRT qui nécessite moins d'exigences que le trafic RT.

Cependant, la politique de rejet des paquets lors d'une surcharge d'une des files d'attente, i.e. les données de grande importance peuvent être rejetées alors que d'autres ne le sont pas, peut avoir un impact sur la QoS des flux multimédias en particulier la vidéo. En effet, ce problème se pose en premier lieu avec l'utilisation d'un algorithme d'ordonnancement FIFO dont l'écosystème IoT dépend dans sa gestion d'ordonnancement. Afin de répondre à cette problématique nous avons proposé une nouvelle extension équilibrée de l'algorithme d'ordonnancement DWRR, nommée EDWRR.

L'algorithme d'ordonnancement EDWRR introduit un mécanisme d'équilibrage dans l'algorithme d'ordonnancement DWRR en fournissant, après un certain nombre de tours, un taux de perte de paquets également équilibré entre les différentes files d'attente définies dans l'algorithme d'ordonnancement. EDWRR gère les différentes files d'attente d'une manière équitable en donnant une chance aux paquets arrivants dans une file d'attente surchargée de ne pas être rejetés par l'ordonnanceur. Cette technique consiste à estimer une probabilité de taux de perte durant un nombre de tours, afin d'attribuer à chaque file d'attente un pourcentage équilibré de taux de rejet de données dans les prochains tours qui viennent. Nous avons contribué à cet espace en évaluant l'impact de : FIFO, DWRR conventionnel et EDWRR sur les performances des flux de type IoMT en termes de taux de paquets délivrés, de délai de bout en bout et de débit. Notre algorithme proposé EDWRR révèle ses avantages en fournissant une gestion équitable des différentes files d'attentes en ajustant l'espace libre restant dans chacune d'elles.

Nous prévoyons d'étendre nos contributions dans plusieurs directions. Tout d'abord, dans notre première contribution, nous prévoyons d'évaluer les performances de notre algorithme de routage en tenant compte d'une nouvelle combinaison de métriques de routage en particulier le nombre de saut pris par les multiples chemins de routage. En fait, nos expériences de simulation ont été menées sur une topologie uniforme et scalable. Malgré cela, nous prévoyons d'exploiter nos simulations sous un réseau très dense tout en respectant les caractéristiques des données multimédias (vidéo et image) dans la tâche de communication. Dans notre deuxième contribution, nous envisageons d'intégrer de nouvelles algorithmes de compression afin de réduire la taille de la vidéo tout en permettant aux dispositifs IoMT de prendre en charge l'envoi et la réception d'un type de trafic très volumineux.

Références Bibliographiques

Bibliographie

[1] G. geek, "Liste des capteurs | La Fabrique DIY." http ://www.lafabriquediy.com/tutoriel/liste-des-capteurs-229/, Accessed November 2019.

[2] "Les technologies utilisées dans l'IoT." https ://wikimemoires.net/2019/09/les-technologies-utilisees-dans-l-iot/, Accessed November 2019.

[3] "Global Radio Frequency Identification (RFID) Industry, Market Revenue." https ://www.kenresearch.com/blog/2020/02/global-radio-frequency-identification-industry/, Accessed December 2019.

[4] "Meaning of RFID (Radio Frequency Identification), RFID Tag." https ://www.techferal.com/meaning-of-rfid-radio-frequency-identification-rfid-tags-423/, Accessed January 2020.

[5] S. Ray, "RFID Explained. Radio Frequency Identification (RFID)... | by Shaan Ray | Lansaar | Medium." https ://medium.com/lansaar/rfid-explained-970e9e0b13d4, Accessed January 2020.

[6] "Internet of Things | opentechdiary." https ://opentechdiary.wordpress.com/tag/internet-of-things/, Accessed November 2019.

[7] E. Siow, *Efficient querying for analytics on Internet of Things databases and streams*. PhD thesis, University of Southampton, UK, 2018.

[8] L. Atzori, A. Iera, and G. Morabito, "The internet of things : A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[9] M. Friedli, L. Kaufmann, F. Paganini, and R. Kyburz, "Energy efficiency of the Internet of Things," tech. rep., Technology and Energy Assessment Report prepared for IEA 4E EDNA. Lucerne University of Applied Sciences, Switzerland, 2016.

[10] R. Kotian, G. Exarchakos, and A. Liotta, "Reliable low-power wireless networks over unstable transmission power," in *Proceedings of the 14th IEEE International Conference on Networking, Sensing and Control (ICNSC)*, pp. 801–806, 2017.

[11] J. Soldatos, *Building Blocks for IoT Analytics*. River Publishers, 2016.

[12] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the internet of (important) things," *IEEE communications surveys & tutorials*, vol. 15, no. 3, pp. 1389–1406, 2012.

[13] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things : A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[14] N. Alhakbani, M. M. Hassan, and M. Ykhlef, "An effective semantic event matching system in the internet of things (IoT) environment," *Sensors*, vol. 17, no. 9, p. p2014, 2017.

[15] Y. Krytska, I. Skarga-Bandurova, and A. Velykzhanin, "IoT-based situation awareness support system for real-time emergency management," in *Proceedings of the 9^{th} IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems : Technology and Applications (IDAACS)*, vol. 2, pp. 955–960, 2017.

[16] H. Lin and N. W. Bergmann, "IoT privacy and security challenges for smart home environments," *Information*, vol. 7, no. 3, p. Article44, 2016.

[17] Z. Sheng, S. Yang, Y. Yu, A. V. Vasilakos, J. A. McCann, and K. K. Leung, "A survey on the IETF protocol suite for the internet of things : Standards, challenges, and opportunities," *IEEE wireless communications*, vol. 20, no. 6, pp. 91–98, 2013.

[18] M. O. Farooq and T. Kunz, "Operating systems for wireless sensor networks : A survey," *Sensors*, vol. 11, no. 6, pp. 5900–5930, 2011.

[19] "Installateur Vidéosurveillance Reconnaissance Faciale." http ://www.videosafe.fr/services/installation/videosurveillance-reconnaissance-faciale, Accessed February 2020.

[20] "ZKAccess BioCam 300 Standalone HD IP Camera with Long Range Facial Recognition." https ://www.surveillance-video.com/camera-biocam-300.html, Accessed January 2020.

[21] A. Yadav, "Machine learning in Healthcare." https ://medium.com/ai-techsystems/machine-learning-in-healthcare-2c1111a3558c, Accessed November 2019.

[22] "A Japanese medical device manufacturer is seeking a distribution partner to bring their electronic fetal monitor for remote prenatal check-ups to the EU | EEN." https ://www.een-japan.eu/jp-profile/fetal-monitor, Accessed January 2020.

[23] Y. Verma, "9 Best Smartwatch under 10000 Rs in India." https ://topbestof.com/top-list/best-smartwatch-under-10000/, Accessed May 2020.

[24] "The Importance of Data Collection in Healthcare." https ://www.sam-solutions.com/blog/the-importance-of-data-collection-in-healthcare/, Accessed March 2020.

[25] "MySignals - eHealth and Medical IoT Development Platform." http ://www.my-signals.com/, Accessed January 2020.

[26] R. Blog, "smart-homes-iot-2." https ://blog.radware.com/security/2018/02/smart-homes-iot-2/attachment/smart-homes-iot-2-2/, Accessed January 2020.

[27] Biz4Intelia, "5 IoT Applications in Agriculture Industry | Smart Farming Solutions." https ://www.biz4intellia.com/blog/5-applications-of-iot-in-agriculture/, Accessed January 2020.

[28] A. Nauman, Y. A. Qadri, M. Amjad, Y. B. Zikria, M. K. Afzal, and S. W. Kim, "Multimedia Internet of Things : A Comprehensive Survey," *IEEE Access*, vol. 8, pp. 8202–8250, 2020.

[29] H. Lamaazi and N. Benamar, "A comprehensive survey on enhancements and limitations of the RPL protocol : A focus on the objective function," *Ad Hoc Networks*, vol. 96, p. Article 102001, 2020.

[30] S. Li, L. Da Xu, and S. Zhao, "The internet of things : a survey," *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, 2015.

[31] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, "Vision and challenges for realising the Internet of Things," *Cluster of European Research Projects on the Internet of Things, European Commision*, vol. 3, no. 3, pp. 34–36, 2010.

[32] J. Pan, S. Paul, and R. Jain, "A survey of the research on future internet architectures," *IEEE Communications Magazine*, vol. 49, no. 7, pp. 26–36, 2011.

[33] N. Srinidhi, S. D. Kumar, and K. Venugopal, "Network optimizations in the Internet of Things : A review," *Engineering Science and Technology, an International Journal*, vol. 22, no. 1, pp. 1–21, 2019.

[34] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks : a survey," *Computer networks*, vol. 38, no. 4, pp. 393–422, 2002.

[35] L. Mottola and G. P. Picco, "Programming wireless sensor networks : Fundamental concepts and state of the art," *ACM Computing Surveys (CSUR)*, vol. 43, no. 3, pp. 1–51, 2011.

[36] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare : A survey," *Computer networks*, vol. 54, no. 15, pp. 2688–2710, 2010.

[37] D. Basu, G. Moretti, G. S. Gupta, and S. Marsland, "Wireless sensor network based smart home : Sensor selection, deployment and monitoring," in *Proceedings of IEEE International Symposium on Sensors Applications*, pp. 49–54, IEEE, 2013.

[38] M. S. Jamil, M. A. Jamil, A. Mazhar, A. Ikram, A. Ahmed, and U. Munawar, "Smart environment monitoring system by employing wireless sensor networks on vehicles for pollution free smart cities," *Procedia Engineering*, vol. 107, pp. 480–484, 2015.

[39] L. Mainetti, L. Patrono, and A. Vilei, "Evolution of wireless sensor networks towards the internet of things : A survey," in *Proceedings of the 19th IEEE International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2011)*, pp. 1–6, 2011.

[40] K. Evangelos A, T. Nikolaos D, and B. Anthony C, "Integrating RFIDs and smart objects into a UnifiedInternet of Things architecture," *Advances in Internet of Things*, vol. 1, pp. 5–12, 2011.

[41] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things : perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.

[42] K. Ashton *et al.*, "That 'internet of things' thing," *RFID journal*, vol. 22, no. 7, pp. 97–114, 2009.

[43] D. L. Brock, "The electronic product code (epc)," tech. rep., Auto-ID Center White Paper MIT-AUTOID-WH-002, (21 pages), 2001.

[44] L. Yang, S.-H. Yang, and L. Plotnick, "How the internet of things technology enhances emergency response operations," *Technological Forecasting and Social Change*, vol. 80, no. 9, pp. 1854–1867, 2013.

[45] L. Tan and N. Wang, "Future internet : The internet of things," in *Proceedings of 3rd IEEE International Conference on Advanced Computer Theory and Engineering (ICACTE)*, vol. 5, pp. V5–376, 2010.

[46] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer, *et al.*, "Internet of things strategic research roadmap," *Internet of things-global technological and societal trends*, vol. 1, no. 2011, pp. 9–52, 2011.

[47] P. Guillemin, P. Friess, *et al.*, "Internet of things strategic research roadmap," tech. rep., The Cluster of European Research Projects, 2009.

[48] P. P. Ray, "A survey on Internet of Things architectures," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 291–319, 2018.

[49] Y. B. Zikria, H. Yu, M. K. Afzal, M. H. Rehmani, and O. Hahm, "Internet of things (IoT) : Operating system, applications and protocols design, and validation techniques," *Future Generation Computer Systems*, vol. 88, pp. 699–706, 2018.

[50] S. A. Alvi, B. Afzal, G. A. Shah, L. Atzori, and W. Mahmood, "Internet of multimedia things : Vision and challenges," *Ad Hoc Networks*, vol. 33, pp. 87–111, 2015.

[51] O. Vermesan, P. Friess, *et al.*, *Internet of things-from research and innovation to market deployment*, vol. 29. River publishers Aalborg, 2014.

[52] B. Al Nahas, "Multichannel Communication in Contiki's Low-power IPv6 Stack," tech. rep., Department of Information Technology, Uppsala University, 2013.

[53] Z. Shelby, K. Hartke, C. Bormann, and B. Frank, "Constrained application protocol (coap) draft-ietf-core-coap-18," tech. rep., IETF work in progress, 2013.

[54] B. Shala, P. Wacht, U. Trick, A. Lehmann, B. Ghita, and S. Shiaeles, "Framework for automated functional testing of p2p-based m2m applications," in *Proceedings of the 9th IEEE International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 916–921, 2017.

[55] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (CoAP)," tech. rep., RFC 7252 , Internet Engineering Task Force (IETF), 2014.

[56] J. Postel *et al.*, "User datagram protocol," tech. rep., RFC 768, IETF, August 1980.

[57] B. Billet, *Système de gestion de flux pour l'Internet des objets intelligents*. PhD thesis, Université de VersaillesSaint-Quentin-En-Yvelines, France, 2015.

[58] E. Rescorla and N. Modadugu, "Datagram transport layer security version 1.2," tech. rep., RFC 6347, Internet Engineering Task Force (IETF), January 2012.

[59] A. Conta, S. Deering, and M. Gupta, "Internet control message protocol (ICMPv6) for the internet protocol version 6 (IPv6) specification," tech. rep., RFC 2463, Internet Engineering Task Force (IETF), December 1998.

[60] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT) : A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[61] J. Vasseur and D. Culler, "Routing over low power and lossy networks (roll)," tech. rep., Internet Engineering Task Force (IETF), 2008.

[62] T. Winter, P. Thubert, A. Brandt, J. W. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J.-P. Vasseur, and R. K. Alexander, "RPL : IPv6 Routing Protocol for Low-Power and Lossy Networks," tech. rep., RFC 6550, IETF, (157 pages), 2012.

[63] D. Culler, S. Chakrabarti, and I. Infusion, "6LoWPAN : Incorporating IEEE 802.15. 4 into the IP architecture," tech. rep., White paper, Internet Protocol for Smart Objects (IPSO) Alliance, January 2009.

[64] N. Kushalnagar, G. Montenegro, C. Schumacher, *et al.*, "IPv6 over low-power wireless personal area networks (6LoWPANs) : overview, assumptions, problem statement, and goals," tech. rep., RFC 4919 (Informational), Internet Engineering Task Force (IETF), 2007.

[65] J. Hui, P. Thubert, *et al.*, "Compression format for IPv6 datagrams over IEEE 802.15. 4-based networks," tech. rep., RFC 6282, Internet Engineering Task Force (IETF), September 2011.

[66] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, *et al.*, "Transmission of IPv6 packets over IEEE 802.15. 4 networks," tech. rep., Internet proposed standard RFC (vol. 4944 :130 pages), 2007.

[67] G. Mulligan, "The 6LoWPAN architecture," in *Proceedings of the 4th Workshop on Embedded networked sensors*, pp. 78–82, 2007.

[68] I. C. Msadaa and A. Dhraief, "Internet of Things in support of public safety networks : opportunities and challenges," in *Wireless Public Safety Networks 2*, pp. 1–23, Elsevier, 2016.

[69] E. Callaway, P. Gorday, L. Hester, J. A. Gutierrez, M. Naeve, B. Heile, and V. Bahl, "Home networking with IEEE 802.15. 4 : a developing standard for low-rate wireless personal area networks," *IEEE Communications magazine*, vol. 40, no. 8, pp. 70–77, 2002.

[70] J.-P. Vasseur and A. Dunkels, *Interconnecting smart objects with ip : The next internet*. Morgan Kaufmann, 2010.

[71] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki-a lightweight and flexible operating system for tiny networked sensors," in *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks*, pp. 455–462, 2004.

[72] A. Dunkels, O. Schmidt, T. Voigt, and M. Ali, "Protothreads : Simplifying event-driven programming of memory-constrained embedded systems," in *Proceedings of the 4th International Conference on Embedded networked sensor systems*, pp. 29–42, 2006.

[73] A. Dunkels, F. Osterlind, N. Tsiftes, and Z. He, "Software-based on-line energy estimation for sensor nodes," in *Proceedings of the 4th Workshop on Embedded networked sensors*, pp. 28–32, 2007.

[74] A. Dunkels, J. Eriksson, N. Finne, and N. Tsiftes, "Powertrace : Network-level power profiling for low-power wireless networks," tech. rep., Swedish Institute of Computer Science, 2011.

[75] M. Durvy, J. Abeillé, P. Wetterwald, C. O'Flynn, B. Leverett, E. Gnoske, M. Vidales, G. Mulligan, N. Tsiftes, N. Finne, *et al.*, "Making sensor networks ipv6 ready," in *Proceedings of the 6th ACM Conference on Embedded network sensor systems*, pp. 421–422, 2008.

[76] A. Dunkels, F. Österlind, and Z. He, "An adaptive communication architecture for wireless sensor networks," in *Proceedings of the 5th International Conference on Embedded networked sensor systems*, pp. 335–349, 2007.

[77] S. Kalyoncu, "Wireless solutions and authentication mechanisms for Contiki based Internet of things networks," tech. rep., Halmstad University, School of Information Science, Computer and Electrical Engineering (IDE), 2013.

[78] A. Dunkels, "The contikimac radio duty cycling protocol," tech. rep., Swedish Institute of Computer Science, 2011.

[79] J. Kabara and M. Calle, "MAC protocols used by wireless sensor networks and a general method of performance evaluation," *International Journal of Distributed Sensor Networks*, vol. 8, no. 1, p. Article834784, 2012.

[80] M. Orell, "Performance Evaluation of MAC protocols in Wireless Sensor Networks," tech. rep., Mälardalen University, School of Innovation, Design and Engineering, 2016.

[81] M. Buettner, G. V. Yee, E. Anderson, and R. Han, "X-MAC : a short preamble MAC protocol for duty-cycled wireless sensor networks," in *Proceedings of the 4th International Conference on Embedded networked sensor systems*, pp. 307–320, 2006.

[82] M.-P. Uwase, M. Bezunartea, J. Tiberghien, J.-M. Dricot, and K. Steenhaut, "Experimental comparison of radio duty cycling protocols for wireless sensor networks," *IEEE sensors journal*, vol. 17, no. 19, pp. 6474–6482, 2017.

[83] V. C. Thang, "A Comparative Study of Network Performance between ContikiMAC and XMAC Protocols in Data Collection Application with ContikiRPL," *Int. J. Comput. Netw. Inf. Secur*, vol. 11, no. 8, pp. 1–32, 2019.

[84] M. Bezunartea, M.-P. Uwase, J. Tiberghien, J.-M. Dricot, and K. Steenhaut, "Demonstrating the versatility of a low cost measurement testbed for Wireless Sensor Networks with a case study on Radio Duty Cycling protocols," in *International Internet of Things Summit*, pp. 222–230, Springer, 2015.

[85] C. Pinola, "Evaluating the performance of synchronous and asynchronous media access control protocols in the contiki operating system," tech. rep., Worcester Polytechnic Institute, 2013.

[86] F. Österlind, "A sensor network simulator for the Contiki OS," tech. rep., 2006.

[87] H.-S. Kim, J. Ko, D. E. Culler, and J. Paek, "Challenging the IPv6 routing protocol for low-power and lossy networks (RPL) : A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2502–2525, 2017.

[88] J. Eriksson, A. Dunkels, N. Finne, F. Osterlind, and T. Voigt, "Mspsim–an extensible simulator for msp430-equipped sensor boards," in *Proceedings of the European Conference on Wireless Sensor Networks (EWSN), Poster/Demo session*, vol. 118, 2007.

[89] J. Eriksson, F. Österlind, N. Finne, N. Tsiftes, A. Dunkels, T. Voigt, R. Sauter, and P. J. Marrón, "COOJA/MSPSim : interoperability testing for wireless sensor networks," in *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, pp. 1–7, 2009.

[90] B. Titzer, D. K. Lee, and J. Palsberg, "SYS1 : Avrora : Scalable Sensor Network Simulation with Precise Timing," tech. rep., Center for Embedded Network Sensing, 2005.

[91] R. de Paz Alberola and D. Pesch, "AvroraZ : extending Avrora with an IEEE 802.15.4 compliant radio chip model," in *Proceedings of the 3nd ACM Workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks*, pp. 43–50, 2008.

[92] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with cooja," in *Proceedings. 2006 31st IEEE International Conference on Local Computer Networks*, pp. 641–648, 2006.

[93] A. Floris and L. Atzori, "Managing the quality of experience in the multimedia internet of things : A layered-based approach," *Sensors*, vol. 16, no. 12, p. Article2057, 2016.

[94] A. Floris and L. Atzori, "Quality of Experience in the Multimedia Internet of Things : Definition and practical use-cases," in *Proceedings of IEEE International Conference on Communication Workshop (ICCW)*, pp. 1747–1752, 2015.

[95] C. G. C. Index, "Cisco Global Cloud Index : Forecast and Methodology, 2015–2020," tech. rep., June 2016.

[96] A. Gynnild, "The Robot Eye Witness : Extending visual journalism through drone surveillance," *Digital journalism*, vol. 2, no. 3, pp. 334–343, 2014.

[97] M. Bojarski, D. Del Testa, D. Dworakowski, B. Firner, B. Flepp, P. Goyal, L. D. Jackel, M. Monfort, U. Muller, J. Zhang, Z. Xin, Z. Jake, and K. Zieba, "End to End Learning for Self-Driving Cars," *Journal : arXiv preprint arXiv :1604.07316*, pp. 1–9, 2016.

[98] S. A. Alvi, G. A. Shah, and W. Mahmood, "Energy efficient green routing protocol for internet of multimedia things," in *Proceedings of the 10th IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, pp. 1–6, 2015.

[99] S. Boll, J. Meyer, and N. E. O'Connor, "Health media : From multimedia signals to personal health insights," *IEEE MultiMedia*, vol. 25, no. 1, pp. 51–60, 2018.

[100] A. Ruiz-Zafra, K. Benghazi, C. Mavromoustakis, and M. Noguera, "An IoT-aware architectural model for smart habitats," in *Proceedings of the 16th IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, pp. 103–110, 2018.

[101] I. U. Rehman, M. M. Nasralla, A. Ali, and N. Philip, "Small cell-based ambulance scenario for medical video streaming : A 5G-health use case," in *Proceedings of the 15th IEEE International Conference on Smart Cities : Improving Quality of Life Using ICT & IoT (HONET-ICT)*, pp. 29–32, 2018.

[102] M. K. Ishak and N. M. Kit, "Design and implementation of robot assisted surgery based on Internet of Things (IoT)," in *Proceedings of IEEE International Conference on Advanced Computing and Applications (ACOMP)*, pp. 65–70, 2017.

[103] F. Al-Alem, M. A. Alsmirat, and M. Al-Ayyoub, "On the road to the internet of biometric things : a survey of fingerprint acquisition technologies and fingerprint databases," in *Proceedings of the 13th IEEE/ACS International Conference of Computer Systems and Applications (AICCSA)*, pp. 1–6, 2016.

[104] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4900–4913, 2018.

[105] A. Boles and P. Rad, "Voice biometrics : Deep learning-based voiceprint authentication system," in *Proceedings of the 12th IEEE International Conference on System of Systems Engineering Conference (SoSE)*, pp. 1–6, 2017.

[106] Y. Meng, W. Zhang, H. Zhu, and X. S. Shen, "Securing consumer IoT in the smart home : Architecture, challenges, and countermeasures," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 53–59, 2018.

[107] H. Hamidi, "An approach to develop the smart health using Internet of Things and authentication based on biometric technology," *Future generation computer systems*, vol. 91, pp. 434–449, 2019.

[108] A. H. Basri, S. N. Ibrahim, N. A. Malik, and A. Asnawi, "Integrated surveillance system with mobile application," in *Proceedings of the 7th IEEE International Conference on Computer and Communication Engineering (ICCCE)*, pp. 218–222, 2018.

[109] L.-W. Chen, C.-R. Chen, and D.-E. Chen, "VIPS : A video-based indoor positioning system with centimeter-grade accuracy for the IoT," in *Proceedings of IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 63–65, 2017.

[110] M. I. Al-Saleh, M. A. Alsmirat, Y. Jararweh, and I. Obaidat, "A unified key distribution and session management protocol for mobile video surveillance systems," in *Proceedings of the 9th IEEE International Conference on Internet of Things : Systems, Management and Security*, pp. 234–238, 2018.

[111] C.-Y. Hsu, L.-W. Kang, H.-Y. Lin, R.-H. Fu, C.-Y. Lin, M.-F. Weng, and D.-Y. Chen, "Depth-based feature extraction-guided automatic identification tracking of steel products for smart manufacturing in steel 4.0," in *Proceedings of IEEE International Conference on Applied System Invention (ICASI)*, pp. 145–146, 2018.

[112] C.-Y. Hsu, H.-Y. Lin, L.-W. Kang, M.-F. Weng, C.-M. Chang, and T.-Y. You, "3D modeling for steel billet images," in *Proceedings of IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*, pp. 5–6, 2017.

[113] R. N. Gore, H. Kour, and M. Gandhi, "IoT based equipment identification and location for maintenance in large deployment industrial plants," in *Proceedings of the 10th IEEE International Conference on Communication Systems & Networks (COMSNETS)*, pp. 461–463, 2018.

[114] K. Sornalatha and V. Kavitha, "IoT based smart museum using Bluetooth Low Energy," in *Proceedings of the 3rd IEEE International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-informatics (AEEICB)*, pp. 520–523, 2017.

[115] A. S. Rao, A. V. Sharma, and C. S. Narayan, "A context aware system for an IoT-based smart museum," in *Proceedings of the 2nd IEEE International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*, pp. 1–5, 2017.

[116] I. Plaksina, G. Chistokhina, and D. Topolskiy, "Development of a transport robot for automated warehouses," in *Proceedings of IEEE International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, pp. 1–4, 2018.

[117] G. Nisha and J. Megala, "Wireless sensor network based automated irrigation and crop field monitoring system," in *Proceedings of the 6th IEEE International Conference on Advanced Computing (ICoAC)*, pp. 189–194, 2014.

[118] K. Yanai, T. Maruyama, and Y. Kawano, "A cooking recipe recommendation system with visual recognition of food ingredients," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 8, no. 2, pp. 28–34, 2014.

[119] G. Witjaksono, A. S. Rabih, N. Yahya, and S. Alva, "IoT for agriculture : food quality and safety," in *IOP Conference Series : Materials Science and Engineering (ICEAMM 2017). IOP Publishing*, vol. 343, pp. 1–7, 2018.

[120] D. Goel, N. Pahal, P. Jain, and S. Chaudhury, "An ontology-driven context aware framework for smart traffic monitoring," in *Proceedings of IEEE Region 10 Symposium (TENSYMP)*, pp. 1–5, 2017.

[121] A. Celesti, A. Galletta, L. Carnevale, M. Fazio, A. Ĺay-Ekuakille, and M. Villari, "An IoT cloud system for traffic monitoring and vehicular accidents prevention based on mobile sensor data processing," *IEEE Sensors Journal*, vol. 18, no. 12, pp. 4795–4802, 2017.

[122] C. Chellaswamy, H. Famitha, T. Anusuya, and S. Amirthavarshini, "IoT based humps and pothole detection on roads and information sharing," in *Proceedings of IEEE International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC)*, pp. 084–090, IEEE, 2018.

[123] E. Türk and M. Challenger, "An android-based IoT system for vehicle monitoring and diagnostic," in *Proceedings of the 26th IEEE International Conference on Signal Processing and Communications Applications (SIU)*, pp. 1–4, 2018.

[124] N. S. Rajput, A. Mishra, A. Sisodia, I. Makarov, *et al.*, "A novel autonomous taxi model for smart cities," in *Proceedings of 4th IEEE World Forum on Internet of Things (WF-IoT)*, pp. 625–628, 2018.

[125] D. Pašalić, B. Cvijić, D. Bundalo, Z. Bundalo, and R. Stojanović, "Vehicle toll payment system based on Internet of Things concept," in *Proceedings of the 5th IEEE Mediterranean Conference on Embedded Computing (MECO)*, pp. 485–488, 2016.

[126] A. Dhumane and R. Prasad, "Routing challenges in internet of things," in *Proceedings of International Conference on CSI Communications*, pp. 19–20, 2015.

[127] O. Bello and S. Zeadally, "Intelligent device-to-device communication in the internet of things," *IEEE Systems Journal*, vol. 10, no. 3, pp. 1172–1182, 2014.

[128] Y. Tian and R. Hou, "An improved AOMDV routing protocol for internet of things," in *Proceedings of IEEE International Conference on Computational Intelligence and Software Engineering*, pp. 1–4, IEEE, 2010.

[129] G. Maalouf, "A study of AODV and DSR protocols : A meta-analysis of AODV and DSR protocols," tech. rep., Mid Sweden University, Faculty of Science, Technology and Media, Department of Information and Communication systems, 2016.

[130] D. Sasidharan and L. Jacob, "Energy and bandwidth efficient multipath-enhanced loadng routing protocol," in *Proceedings of Twenty Second IEEE National Conference on Communication (NCC)*, pp. 1–6, 2016.

[131] S. Sankaran and R. Sridhar, "Modeling and analysis of routing in iot networks," in *Proceedings of IEEE International Conference on Computing and Network Communications (CoCoNet)*, pp. 649–655, 2015.

[132] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd IEEE Annual Hawaii International Conference on System Sciences*, pp. 10–pp, 2000.

[133] T. Qiu, X. Liu, L. Feng, Y. Zhou, and K. Zheng, "An efficient tree-based self-organizing protocol for internet of things," *IEEE Access*, vol. 4, pp. 3535–3546, 2016.

[134] T. Muhammed, R. Mehmood, A. Albeshri, and A. Alzahrani, "HCDSR : A hierarchical clustered fault tolerant routing technique for IoT-based smart societies," in *Smart Infrastructure and Applications*, pp. 609–628, Springer, 2020.

[135] J. Yim, W.-S. Jung, and Y.-B. Ko, "Link quality based geographic routing resilient to location errors," in *Proceedings of 7th IEEE International Conference on Ubiquitous and Future Networks*, pp. 95–96, 2015.

[136] C. H. Barriquello, G. W. Denardin, and A. Campos, "A geographic routing approach for IPv6 in large-scale low-power and lossy networks," *Computers & Electrical Engineering*, vol. 45, pp. 182–191, 2015.

[137] M.-S. Pan and S.-W. Yang, "A lightweight and distributed geographic multicast routing protocol for IoT applications," *Computer Networks*, vol. 112, pp. 95–107, 2017.

[138] R. K. Poluru and S. Naseera, "A Literature Review on Routing Strategy in the Internet of Things," *Journal of Engineering Science & Technology Review*, vol. 10, no. 5, pp. 50–60, 2017.

[139] A. Dhumane, R. Prasad, and J. Prasad, "Routing issues in internet of things : a survey," in *Proceedings of the international multiconference of engineers and computer scientists*, vol. 1, pp. 16–18, 2016.

[140] Z. Chen, H. Wang, Y. Liu, F. Bu, and Z. Wei, "A context-aware routing protocol on internet of things based on sea computing model," *Journal of Computers*, vol. 7, no. 1, pp. 96–105, 2012.

[141] T. Qiu, Y. Lv, F. Xia, N. Chen, J. Wan, and A. Tolba, "ERGID : An efficient routing protocol for emergency response Internet of Things," *Journal of Network and Computer Applications*, vol. 72, pp. 104–112, 2016.

[142] S. M. Oteafy, F. M. Al-Turjman, and H. S. Hassanein, "Pruned adaptive routing in the heterogeneous Internet of Things," in *Proceedings of IEEE Global Communications Conference (GLOBECOM)*, pp. 214–219, 2012.

[143] S. J. Borah, S. K. Dhurandher, I. Woungang, and V. Kumar, "A game theoretic context-based routing protocol for opportunistic networks in an iot scenario," *Computer Networks*, vol. 129, pp. 572–584, 2017.

[144] S. Debroy, P. Samanta, A. Bashir, and M. Chatterjee, "SpEED-IoT : spectrum aware energy efficient routing for device-to-device IoT communication," *Future Generation Computer Systems*, vol. 93, pp. 833–848, 2019.

[145] S. Hamrioui, C. A. M. Hamrioui, J. Lioret, and P. Lorenz, "Smart and self-organised routing algorithm for efficient IoT communications in smart cities," *IET Wireless Sensor Systems*, vol. 8, no. 6, pp. 305–312, 2018.

[146] D. Kothandaraman, C. Chellappan, P. Sivasankar, and S. N. Pasha, "Context-Aware Energy Conserving Routing Algorithm for Internet of Things," *International Journal of Computer Networks & Communications (IJCNC) Vol*, vol. 11, pp. 15–32, 2019.

[147] W. Sun, M. Tang, L. Zhang, Z. Huo, and L. Shu, "A Survey of Using Swarm Intelligence Algorithms in IoT," *Sensors*, vol. 20, no. 5, pp. 1–27, 2020.

[148] S. A. Chelloug *et al.*, "Energy-efficient content-based routing in internet of things," *Journal of Computer and Communications*, vol. 3, no. 12, p. 9, 2015.

[149] K. Machado, D. Rosário, E. Cerqueira, A. A. Loureiro, A. Neto, and J. N. De Souza, "A routing protocol based on energy and link quality for internet of things applications," *Sensors*, vol. 13, no. 2, pp. 1942–1964, 2013.

[150] N. Nasser, L. Karim, A. Ali, and N. Khelifi, "Multiple Base station and Packet Priority-based clustering scheme in Internet of Things," in *Proceedings of IEEE International Conference on Computing, Management and Telecommunications (ComManTel)*, pp. 58–61, 2014.

[151] S.-H. Park, S. Cho, and J.-R. Lee, "Energy-efficient probabilistic routing algorithm for internet of things," *Journal of Applied Mathematics*, vol. 2014, pp. Article ID 213106, 7 pages, 2014.

[152] M. Zhao, A. Kumar, P. H. J. Chong, and R. Lu, "A reliable and energy-efficient opportunistic routing protocol for dense lossy networks," *IEEE Wireless Communications Letters*, vol. 6, no. 1, pp. 26–29, 2016.

[153] M. Vellanki, S. Kandukuri, and A. Razaque, "Node level energy efficiency protocol for internet of things," *Journal of Theoretical and Computational Science*, vol. 3, pp. 1–5, 2016.

[154] Z. Zhou, B. Yao, R. Xing, L. Shu, and S. Bu, "E-CARP : An energy efficient routing protocol for UWSNs in the internet of underwater things," *IEEE Sensors Journal*, vol. 16, no. 11, pp. 4072–4082, 2015.

[155] K. Kumar and S. Kumar, "Energy efficient link stable routing in internet of things," *International Journal of Information Technology*, vol. 10, no. 4, pp. 465–479, 2018.

[156] P. K. Reddy and R. Babu, "An evolutionary secure energy efficient routing protocol in internet of things," *International Journal of Intelligent Engineering and Systems*, vol. 10, pp. 337–346, 2017.

[157] B. R. Al-Kaseem and H. S. Al-Raweshidy, "Scalable M2M routing protocol for energy efficient IoT wireless applications," in *Proceddings 8th IEEE International Conference on Computer Science and Electronic Engineering (CEEC)*, pp. 30–35, 2016.

[158] X. Zhong, L. Li, S. Zhang, and R. Lu, "ECOR : An Energy Aware Coded Opportunistic Routing for Cognitive Radio Social Internet of Things," *Wireless Personal Communications*, vol. 110, no. 1, pp. 1–20, 2020.

[159] H. S. Bazzi, A. M. Haidar, and A. Bilal, "Classification of routing protocols in wireless sensor network," in *Proceedings of IEEE International Conference on Computer Vision and Image Analysis Applications*, pp. 1–5, 2015.

[160] M. Sepulcre, J. Gozalvez, and B. Coll-Perales, "Multipath QoS-driven routing protocol for industrial wireless networks," *Journal of network and computer applications*, vol. 74, pp. 121–132, 2016.

[161] T. D. Nguyen, J. Y. Khan, and D. T. Ngo, "A distributed energy-harvesting-aware routing algorithm for heterogeneous IoT networks," *IEEE Transactions on Green Communications and Networking*, vol. 2, no. 4, pp. 1115–1127, 2018.

[162] M. Zhao, A. Kumar, P. H. J. Chong, and R. Lu, "A comprehensive study of RPL and P2P-RPL routing protocols : Implementation, challenges and opportunities," *Peer-to-Peer Networking and Applications*, vol. 10, no. 5, pp. 1232–1256, 2017.

[163] W.-T. Sung and Y.-C. Chiang, "Improved particle swarm optimization algorithm for android medical care IoT using modified parameters," *Journal of medical systems*, vol. 36, no. 6, pp. 3755–3763, 2012.

[164] S. Luo, L. Cheng, and B. Ren, "Practical Swarm Optimization based Fault-Tolerance Algorithm for the Internet of Things," *KSII Transactions on Internet & Information Systems*, vol. 8, no. 3, pp. 1178–1191, 2014.

[165] M. Z. Hasan and F. Al-Turjman, "Optimizing multipath routing with guaranteed fault tolerance in internet of things," *IEEE Sensors Journal*, vol. 17, no. 19, pp. 6463–6473, 2017.

[166] S. Hamrioui and P. Lorenz, "Bio inspired routing algorithm and efficient communications within IoT," *IEEE Network*, vol. 31, no. 5, pp. 74–79, 2017.

[167] M. Frey, F. Große, and M. Günes, "Energy-aware ant routing in wireless multi-hop networks," in *Proceedings of IEEE International Conference on Communications (ICC)*, pp. 190–196, 2014.

[168] G. Hatzivasilis, I. Papaefstathiou, and C. Manifavas, "SCOTRES : secure routing for IoT and CPS," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2129–2141, 2017.

[169] G. Hatzivasilis and C. Manifavas, "Building trust in ad hoc distributed resource-sharing networks using reputation-based systems," in *Proceedings of 16th IEEE Panhellenic Conference on Informatics*, pp. 416–421, 2012.

[170] R. Hummen, H. Wirtz, J. H. Ziegeldorf, J. Hiller, and K. Wehrle, "Tailoring end-to-end IP security protocols to the Internet of Things," in *Proceedings of 21st IEEE International Conference on Network Protocols (ICNP)*, pp. 1–10, 2013.

[171] S. Gali and V. Nidumolu, "Multi-Context Trust Aware Routing For Internet of Things," *International Journal of Intelligent Engineering and Systems*, vol. 12, pp. 189–200, 2019.

[172] D. K. Shende and S. Sonavane, "CrowWhale-ETR : CrowWhale optimization algorithm for energy and trust aware multicast routing in WSN for IoT applications," *Wireless Networks*, vol. 26, pp. 1–19, 2020.

[173] A. Tabassum, S. Sadaf, D. Sinha, and A. K. Das, "Secure Anti-Void Energy-Efficient Routing (SAVEER) Protocol for WSN-Based IoT Network," in *Advances in Computational Intelligence*, pp. 129–142, Springer, 2020.

[174] P. L. R. Chze and K. S. Leong, "A secure multi-hop routing for IoT communication," in *IEEE World forum on internet of things (WF-IoT)*, pp. 428–432, 2014.

[175] D. Shin, V. Sharma, J. Kim, S. Kwon, and I. You, "Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks," *IEEE Access*, vol. 5, pp. 11100–11117, 2017.

[176] T. Mick, R. Tourani, and S. Misra, "LASeR : Lightweight authentication and secured routing for NDN IoT in smart cities," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 755–764, 2017.

[177] B. Deebak and F. Al-Turjman, "A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks," *Ad Hoc Networks*, vol. 97, p. Paper102022, 2020.

[178] J. Vasseur, M. Kim, K. Pister, N. Dejean, and D. Barthel, "Routing metrics used for path calculation in low-power and lossy networks," tech. rep., RFC 6551, IETF, (30 pages), 2012.

[179] H. Kharrufa, H. A. Al-Kashoash, and A. H. Kemp, "RPL-based routing protocols in IoT applications : A Review," *IEEE Sensors Journal*, vol. 19, no. 15, pp. 5952–5967, 2019.

[180] A. Brandt, J. Buron, and G. Porcu, "Home automation routing requirements in low-power and lossy networks," tech. rep., RFC5826, Internet Engineering Task Force (IETF), 2010.

[181] J. Martocci, P. De Mil, N. Riou, and W. Vermeylen, "Building automation routing requirements in low-power and lossy networks," in *Industrial routing requirements : Internet Engineering Task Force (IETF), 27 pages*, p. 27 pages, 2010.

[182] K. Pister, P. Thubert, S. Dwars, and T. Phinney, "Industrial routing requirements in low-power and lossy networks," tech. rep., RFC5673, Internet Engineering Task Force (IETF), 2009.

[183] M. Dohler, T. Watteyne, T. Winter, and D. Barthel, "Routing requirements for urban low-power and lossy networks," tech. rep., RFC 5548, IETF, 2009.

[184] O. Gaddour, A. Koubaa, S. Chaudhry, M. Tezeghdanti, R. Chaari, and M. Abid, "Simulation and performance evaluation of DAG construction with RPL," in *Proceedings of the 3rd IEEE International Conference on Communications and Networking*, pp. 1–8, 2012.

[185] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko, "The trickle algorithm," tech. rep., Internet Engineering Task Force, RFC6206, 2011.

[186] O. Gaddour, A. Koubäa, R. Rangarajan, O. Cheikhrouhou, E. Tovar, and M. Abid, "Co-RPL : RPL routing for mobile low power wireless sensor networks using Corona mechanism," in *Proceedings of the 9th IEEE International Symposium on Industrial Embedded Systems (SIES 2014)*, pp. 200–209, 2014.

[187] P. Thubert *et al.*, "Objective function zero for the routing protocol for low-power and lossy networks (RPL)," tech. rep., RFC 6552, Internet Engineering Task Force, March 2012.

[188] O. Gnawali and P. Levis, "The minimum rank with hysteresis objective function," tech. rep., RFC 6719, Internet Engineering Task Force, 2012.

[189] J. Ko, J. Jeong, J. Park, J. Jun, N. Kim, and O. Gnawali, "RPL Routing Pathology In a Network With a Mix of Nodes Operating in Storing and Non-Storing Modes," tech. rep., Internet Engineering Task Force, 2014.

[190] O. Iova, F. Theoleyre, and T. Noel, "Stability and efficiency of RPL under realistic conditions in wireless sensor networks," in *Proceedings of the 24th IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 2098–2102, 2013.

[191] D. S. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," in *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking*, pp. 134–146, 2003.

[192] P. Sanmartin, A. Rojas, L. Fernandez, K. Avila, D. Jabba, and S. Valle, "Sigma routing metric for RPL protocol," *Sensors*, vol. 18, no. 4, p. Article1277, 2018.

[193] P. Karkazis, P. Trakadas, H. C. Leligou, L. Sarakis, I. Papaefstathiou, and T. Zahariadis, "Evaluating routing metric composition approaches for QoS differentiation in low power and lossy networks," *Wireless networks*, vol. 19, no. 6, pp. 1269–1284, 2013.

[194] W. Gan, Z. Shi, C. Zhang, L. Sun, and D. Ionescu, "MERPL : A more memory-efficient storing mode in RPL," in *Proceedings of the 19th IEEE International Conference on Networks (ICON)*, pp. 1–5, 2013.

[195] B. Ghaleb, A. Y. Al-Dubai, E. Ekonomou, A. Alsarhan, Y. Nasser, L. M. Mackenzie, and A. Boukerche, "A survey of limitations and enhancements of the ipv6 routing protocol for low-power and lossy networks : A focus on core operations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1607–1635, 2018.

[196] J. V. Sobral, J. J. Rodrigues, R. A. Rabêlo, J. Al-Muhtadi, and V. Korotaev, "Routing Protocols for Low Power and Lossy Networks in Internet of Things Applications," *Sensors*, vol. 19, no. 9, p. Article 2144, 2019.

[197] A. J. Witwit and A. K. Idrees, "A Comprehensive Review for RPL Routing Protocol in Low Power and Lossy Networks," in *International Conference on New Trends in Information and Communications Technology Applications*, pp. 50–66, Springer, 2018.

[198] Y. B. Zikria, M. K. Afzal, F. Ishmanov, S. W. Kim, and H. Yu, "A survey on routing protocols supported by the Contiki Internet of things operating system," *Future Generation Computer Systems*, vol. 82, pp. 200–219, 2018.

[199] O. Iova, P. Picco, T. Istomin, and C. Kiraly, "RPL : The routing standard for the internet of things... or is it ?," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 16–22, 2016.

[200] P. O. Kamgueu, E. Nataf, and T. D. Ndie, "Survey on RPL enhancements : a focus on topology, security and mobility," *Computer Communications*, vol. 120, pp. 10–21, 2018.

[201] O. Gaddour and A. Koubâa, "RPL in a nutshell : A survey," *Computer Networks*, vol. 56, no. 14, pp. 3163–3178, 2012.

[202] J. Tripathi, J. C. de Oliveira, and J.-P. Vasseur, "A performance evaluation study of RPL : Routing protocol for low power and lossy networks," in *Proceedings of the 44th IEEE Annual Conference on Information Sciences and Systems (CISS)*, pp. 1–6, 2010.

[203] M. O. Farooq, C. J. Sreenan, K. N. Brown, and T. Kunz, "RPL-based routing protocols for multi-sink wireless sensor networks," in *Proceedings of the 11th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 452–459, 2015.

[204] N. Accettura, L. A. Grieco, G. Boggia, and P. Camarda, "Performance analysis of the RPL routing protocol," in *Proceedings of IEEE International Conference on Mechatronics*, pp. 767–772, 2011.

[205] E. Ancillotti, R. Bruno, and M. Conti, "RPL routing protocol in advanced metering infrastructures : An analysis of the unreliability problems," in *Proceedings of IEEE International Conference on Sustainable Internet and ICT for Sustainability (SustainIT)*, pp. 1–10, 2012.

[206] X. Liu, Z. Sheng, C. Yin, F. Ali, and D. Roggen, "Performance analysis of routing protocol for low power and lossy networks (RPL) in large scale networks," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2172–2185, 2017.

[207] W. Mardini, M. Ebrahim, and M. Al-Rudaini, "Comprehensive performance analysis of RPL objective functions in iot networks," *International Journal of Communication Networks and Information Security*, vol. 9, no. 3, pp. 323–332, 2017.

[208] H. Kermajani and C. Gomez, "On the network convergence process in RPL over IEEE 802.15. 4 multihop networks : Improvement and trade-offs," *Sensors*, vol. 14, no. 7, pp. 11993–12022, 2014.

[209] C. Cobarzan, J. Montavont, and T. Noel, "Analysis and performance evaluation of RPL under mobility," in *IEEE Symposium on Computers and Communications (ISCC)*, pp. 1–6, 2014.

[210] H. Lamaazi, N. Benamar, M. I. Imaduddin, and A. J. Jara, "Performance assessment of the routing protocol for low power and lossy networks," in *IEEE International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pp. 1–8, 2015.

[211] N. M. Shakya, M. Mani, and N. Crespi, "SEEOF : Smart energy efficient objective function : Adapting RPL objective function to enable an IPv6 meshed topology solution for battery operated smart meters," in *IEEE International Conference on Global Internet of Things Summit (GIoTS)*, pp. 1–6, 2017.

[212] P. O. Kamgueu, E. Nataf, T. D. Ndié, and O. Festor, "Energy-based routing metric for RPL," tech. rep., Research Report N° 8208, Project-Team Madynes (14 pages), June 2012.

[213] O. Iova, F. Theoleyre, and T. Noel, "Using multiparent routing in RPL to increase the stability and the lifetime of the network," *Ad Hoc Networks*, vol. 29, pp. 45–62, 2015.

[214] M. M. Khan, M. A. Lodhi, A. Rehman, A. Khan, and F. B. Hussain, "Sink-to-sink coordination framework using RPL : Routing protocol for low power and lossy networks," *Journal of Sensors*, vol. 2016, p. Article ID 2635429, 2016.

[215] M. Banh, N. Nguyen, K.-H. Phung, L. Nguyen, N. H. Thanh, and K. Steenhaut, "Energy balancing RPL-based routing for Internet of Things," in *Proceedings of the 6th IEEE International Conference on Communications and Electronics (ICCE)*, pp. 125–130, 2016.

[216] A. Riker, M. Curado, and E. Monteiro, "Neutral operation of the minimum energy node in energy-harvesting environments," in *IEEE Symposium on Computers and Communications (ISCC)*, pp. 477–482, 2017.

[217] J. Ko, J. Jeong, J. Park, J. A. Jun, O. Gnawali, and J. Paek, "DualMOP-RPL : Supporting multiple modes of downward routing in a single RPL network," *ACM Transactions on Sensor Networks (TOSN)*, vol. 11, no. 2, pp. 1–20, 2015.

[218] H.-S. Kim, H. Cho, H. Kim, and S. Bahk, "DT-RPL : Diverse bidirectional traffic delivery through RPL routing protocol in low power and lossy networks," *Computer Networks*, vol. 126, pp. 150–161, 2017.

[219] S. Taghizadeh, H. Bobarshad, and H. Elbiaze, "CLRPL : context-aware and load balancing RPL for IoT networks under heavy and highly dynamic load," *IEEE Access*, vol. 6, pp. 23277–23291, 2018.

[220] C. Kiraly, T. Istomin, O. Iova, and G. P. Picco, "D-RPL : Overcoming memory limitations in RPL point-to-multipoint routing," in *Proceedings of the 40th IEEE Conference on Local Computer Networks (LCN)*, pp. 157–160, 2015.

[221] B. Ghaleb, A. Al-Dubai, E. Ekonomou, and I. Wadhaj, "A new enhanced RPL based routing for Internet of Things," in *Proceedings of IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 595–600, 2017.

[222] H. Bouzebiba and M. Lehsaini, "Opt-RPL : Optimized routing for Internet of Things," in *International Conference on Defense systems : Architectures and Technologies (DAT'2020)*, p. Accepted paper, 2020.

[223] O. Gnawali and P. Levis, "The ETX objective function for RPL," tech. rep., 2010.

[224] S. Capone, R. Brama, N. Accettura, D. Striccoli, and G. Boggia, "An energy efficient and reliable composite metric for RPL organized networks," in *Proceedings of the 12th IEEE International Conference on Embedded and Ubiquitous Computing*, pp. 178–184, 2014.

[225] O. Gaddour, A. Koubâa, N. Baccour, and M. Abid, "OF-FL : QoS-aware fuzzy logic objective function for the RPL routing protocol," in *Proceedings of the 12th IEEE International symposium on Modeling and Optimization in mobile, Ad hoc, and Wireless Networks (WiOpt)*, pp. 365–372, 2014.

[226] H. Lamaazi and N. Benamar, "RPL enhancement using a new objective function based on combined metrics," in *Proceedings of the 13th IEEE International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 1459–1464, 2017.

[227] P.-O. Kamgueu, E. Nataf, and T. N. Djotio, "On design and deployment of fuzzy-based metric for routing in low-power and lossy networks," in *Proceedings of the 40th IEEE Conference Workshops on Local Computer Networks (LCN Workshops)*, pp. 789–795, 2015.

[228] H. D. S. Araújo, J. J. Rodrigues, R. D. A. Rabelo, N. D. C. Sousa, C. José Filho, J. V. Sobral, *et al.*, "A proposal for IoT dynamic routes selection based on contextual information," *Sensors (Basel)*, vol. 18, no. 2, p. 353, 2018.

[229] Y. Chen, J.-P. Chanet, K.-M. Hou, H. Shi, and G. De Sousa, "A scalable context-aware objective function (SCAOF) of routing protocol for agricultural low-power and lossy networks (RPAL)," *Sensors*, vol. 15, no. 8, pp. 19507–19540, 2015.

[230] N. Gozuacik and S. Oktug, "Parent-aware routing for IoT networks," in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, pp. 23–33, Springer, 2015.

[231] A. Hassan, S. Alshomrani, A. Altalhi, and S. Ahsan, "Improved routing metrics for energy constrained interconnected devices in low-power and lossy networks," *Journal of communications and networks*, vol. 18, no. 3, pp. 327–332, 2016.

[232] H. Bouzebiba and M. Lehsaini, "Combination of two primary routing metrics of RPL protocol for Internet of Things," in *First International Conference on Embedded & Distributed Systems (EDiS'2017)*, pp. 1–4, 2017.

[233] B. Tian, K. M. Hou, H. Shi, X. Liu, X. Diao, J. Li, Y. Chen, and J.-P. Chanet, "Application of modified RPL under VANET-WSN communication architecture," in *IEEE International Conference on Computational and Information Sciences*, pp. 1467–1470, 2013.

[234] F. Gara, L. B. Saad, R. B. Ayed, and B. Tourancheau, "RPL protocol adapted for healthcare and medical applications," in *Proceedings of IEEE International wireless communications and mobile computing conference (IWCMC)*, pp. 690–695, 2015.

[235] H. Fotouhi, D. Moreira, and M. Alves, "mRPL : Boosting mobility in the Internet of Things," *Ad Hoc Networks*, vol. 26, pp. 17–35, 2015.

[236] M. R. Anand and M. P. Tahiliani, "mRPL++ : Smarter-HOP for optimizing mobility in RPL," in *Proceedings of IEEE Region 10 Symposium (TENSYMP)*, pp. 36–41, 2016.

[237] M. Barcelo, A. Correa, J. L. Vicario, A. Morell, and X. Vilajosana, "Addressing mobility in RPL with position assisted metrics," *IEEE Sensors Journal*, vol. 16, no. 7, pp. 2151–2161, 2015.

[238] H. Kharrufa, H. Al-Kashoash, Y. Al-Nidawi, M. Q. Mosquera, and A. H. Kemp, "Dynamic RPL for multi-hop routing in IoT applications," in *Proceedings of the 13th IEEE Annual Conference on wireless on-demand network systems and services (WONS)*, pp. 100–103, 2017.

[239] H. Kharrufa, H. Al-Kashoash, and A. H. Kemp, "A game theoretic optimization of RPL for mobile Internet of Things applications," *IEEE Sensors Journal*, vol. 18, no. 6, pp. 2520–2530, 2018.

[240] Y. Tahir, S. Yang, and J. McCann, "BRPL : Backpressure RPL for high-throughput and mobile IoTs," *IEEE Transactions on Mobile Computing*, vol. 17, no. 1, pp. 29–43, 2017.

[241] L. Tassiulas and A. Ephremides, "Stability properties of constrained queueing systems and scheduling policies for maximum throughput in multihop radio networks," in *Proceedings of the 29th IEEE Conference on Decision and Control*, pp. 2130–2132, 1990.

[242] M. Bouaziz, A. Rachedi, A. Belghith, M. Berbineau, and S. Al-Ahmadi, "EMA-RPL : Energy and mobility aware routing for the Internet of Mobile Things," *Future Generation Computer Systems*, vol. 97, pp. 247–258, 2019.

[243] M. Bouaziz, A. Rachedi, and A. Belghith, "EKF-MRPL : Advanced mobility support routing protocol for internet of mobile things : Movement prediction approach," *Future Generation Computer Systems*, vol. 93, pp. 822–832, 2019.

[244] J. Kniess and V. de Figueiredo Marques, "MARPL : A crosslayer approach for Internet of things based on neighbor variability for mobility support in RPL," *Transactions on Emerging Telecommunications Technologies*, vol. e3931, pp. 1–17, 2020.

[245] B. Mohamed and F. Mohamed, "QoS routing RPL for low power and lossy networks," *International Journal of Distributed Sensor Networks*, vol. 11, no. 11, p. Article 971545, 2015.

[246] N. Khelifi, S. Oteafy, H. Hassanein, and H. Youssef, "Proactive maintenance in RPL for 6LowPAN," in *Proceedings of IEEE International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 993–999, 2015.

[247] K. Q. Abdel Fadeel and K. El Sayed, "ESMRF : enhanced stateless multicast RPL forwarding for IPv6-based low-power and lossy networks," in *Proceedings of the Workshop on IoT challenges in Mobile and Industrial Systems*, pp. 19–24, 2015.

[248] G. G. Lorente, B. Lemmens, M. Carlier, A. Braeken, and K. Steenhaut, "BMRF : Bidirectional multicast RPL forwarding," *Ad Hoc Networks*, vol. 54, pp. 69–84, 2017.

[249] M. Barcelo, A. Correa, J. L. Vicario, and A. Morell, "Cooperative interaction among multiple RPL instances in wireless sensor networks," *Computer Communications*, vol. 81, pp. 61–71, 2016.

[250] E. Ancillotti, R. Bruno, and M. Conti, "Reliable data delivery with the IETF routing protocol for low-power and lossy networks," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 3, pp. 1864–1877, 2014.

[251] J. Nassar, M. Berthomé, J. Dubrulle, N. Gouvy, N. Mitton, and B. Quoitin, "Multiple instances QoS routing in RPL : Application to smart grids," *Sensors*, vol. 18, no. 8, p. 2472, 2018.

[252] A. Charles and K. Palanisamy, "QoS measurement of RPL using cooja simulator and wireshark network analyser," *International Journal of Computer Sciences and Engineering*, vol. 6, pp. 283–291, 2018.

[253] A. Zier, A. Abouaissa, and P. Lorenz, "E-RPL : A routing protocol for IoT networks," in *Proceedings of IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, 2018.

[254] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson, "A security threat analysis for the routing protocol for low-power and lossy networks (RPLs)," tech. rep., 2015.

[255] P. Pongle and G. Chavan, "A survey : Attacks on RPL and 6LoWPAN in IoT," in *Proceedings of IEEE International conference on pervasive computing (ICPC)*, pp. 1–6, 2015.

[256] A. Kamble, V. S. Malemath, and D. Patil, "Security attacks and secure routing protocols in RPL-based Internet of Things : Survey," in *Proceedings of IEEE International Conference on Emerging Trends & Innovation in ICT (ICEI)*, pp. 33–39, 2017.

[257] S. Mangelkar, S. N. Dhage, and A. V. Nimkar, "A comparative study on RPL attacks and security solutions," in *Proceedings of IEEE International Conference on Intelligent Computing and Control (I2C2)*, pp. 1–6, 2017.

[258] Z. A. Almusaylim, A. Alhumam, and N. Jhanjhi, "Proposing a Secure RPL based Internet of Things Routing Protocol : A Review," *Ad Hoc Networks*, vol. 101, p. 102096, 2020.

[259] J. Hui and J. Vasseur, "The routing protocol for low-power and lossy networks (RPL) option for carrying rpl information in data-plane datagrams," tech. rep., RFC 6553, IETF, March 2012.

[260] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "Mitigation of topological inconsistency attacks in rpl-based low-power lossy networks," *International Journal of Network Management*, vol. 25, no. 5, pp. 320–339, 2015.

[261] S. Raza, L. Wallgren, and T. Voigt, "SVELTE : Real-time intrusion detection in the Internet of Things," *Ad hoc networks*, vol. 11, no. 8, pp. 2661–2674, 2013.

[262] A. Mayzaud, R. Badonnel, and I. Chrisment, "A distributed monitoring strategy for detecting version number attacks in RPL-based networks," *IEEE Transactions on Network and Service Management*, vol. 14, no. 2, pp. 472–486, 2017.

[263] B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani, and L. Mackenzie, "Addressing the DAO Insider Attack in RPL's Internet of Things networks," *IEEE Communications Letters*, vol. 23, no. 1, pp. 68–71, 2018.

[264] P. Thulasiraman and Y. Wang, "A Lightweight Trust-Based Security Architecture for RPL in Mobile IoT Networks," in *Proceedings of the 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1–6, 2019.

[265] M. Conti, P. Kaliyar, M. M. Rabbani, and S. Ranise, "SPLIT : A Secure and Scalable RPL routing protocol for Internet of Things," in *Proceedings of the 14th IEEE*

International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 1–8, 2018.

[266] H.-D. Ma, "Internet of things : Objectives and scientific challenges," *Journal of Computer science and Technology*, vol. 26, no. 6, pp. 919–924, 2011.

[267] C. C. Aggarwal, N. Ashish, and A. Sheth, "The internet of things : A survey from the data-centric perspective," in *Managing and mining sensor data*, pp. 383–428, Springer, 2013.

[268] Q. Wang, Y. Zhao, W. Wang, D. Minoli, K. Sohraby, H. Zhu, and B. Occhiogrosso, "Multimedia IoT systems and applications," in *Proceedings of IEEE Global Internet of Things Summit (GIoTS)*, pp. 1–6, 2017.

[269] J. Wang, Z. Liu, Y. Shen, H. Chen, L. Zheng, H. Qiu, and S. Shu, "A distributed algorithm for inter-layer network coding-based multimedia multicast in Internet of Things," *Computers & Electrical Engineering*, vol. 52, pp. 125–137, 2016.

[270] O. Said, Y. Albagory, M. Nofal, and F. Al Raddady, "IoT-RTP and IoT-RTCP : Adaptive protocols for multimedia transmission over Internet of Things environments," *IEEE access*, vol. 5, pp. 16757–16773, 2017.

[271] X. Huang, K. Xie, S. Leng, T. Yuan, and M. Ma, "Improving Quality of Experience in multimedia Internet of Things leveraging machine learning on big data," *Future Generation Computer Systems*, vol. 86, pp. 1413–1423, 2018.

[272] A. Elshafeey, N. S. A. Elkader, and M. Zorkany, "Compressed sensing video streaming for internet of multimedia things," *International Journal of Cyber-Security and Digital Forensics*, vol. 6, no. 1, pp. 44–54, 2017.

[273] P. Zhao, X. Yang, W. Yu, C. Dong, S. Yang, and S. Bhattarai, "Toward efficient estimation of available bandwidth for IEEE 802.11-based wireless networks," *Journal of network and computer applications*, vol. 40, pp. 116–125, 2014.

[274] S. S. Chaudhari and R. C. Biradar, "Survey of bandwidth estimation techniques in communication networks," *Wireless Personal Communications*, vol. 83, no. 2, pp. 1425–1476, 2015.

[275] H. Bouzebiba and M. Lehsaini, "FreeBW-RPL : A New RPL Protocol Objective Function for Internet of Multimedia Things," *Wireless Personal Communications*, vol. 112, no. 2, p. 1003–1023, 2020.

[276] F. Mortazavi and M. Khansari, "An energy-aware rpl routing protocol for internet of multimedia things," in *Proceedings of the International Conference on smart cities and internet of things*, pp. 1–6, 2018.

[277] S. Rani, S. H. Ahmed, R. Talwar, J. Malhotra, and H. Song, "IoMT : A reliable cross layer protocol for internet of multimedia things," *IEEE Internet of things Journal*, vol. 4, no. 3, pp. 832–839, 2017.

[278] W. E. Castellanos, J. C. Guerri, and P. Arce, "A QoS-aware routing protocol with adaptive feedback scheme for video streaming for mobile networks," *Computer Communications*, vol. 77, pp. 10–25, 2016.

[279] J. Zhou, L. Liu, Y. Deng, and S. Huang, "A QoS routing protocol with bandwidth allocation in multichannel ad hoc networks," *Wireless personal communications*, vol. 75, no. 1, pp. 273–291, 2014.

[280] H. Zhu and I. Chlamtac, "Admission control and bandwidth reservation in multi-hop ad hoc networks," *Computer Networks*, vol. 50, no. 11, pp. 1653–1674, 2006.

[281] C. Sarr, C. Chaudet, G. Chelius, and I. G. Lassous, "Bandwidth estimation for IEEE 802.11-based ad hoc networks," *IEEE transactions on Mobile Computing*, vol. 7, no. 10, pp. 1228–1241, 2008.

[282] H. Xu, L. Huang, C. Qiao, Y. Zhang, and Q. Sun, "Bandwidth-power aware cooperative multipath routing for wireless multimedia sensor networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 4, pp. 1532–1543, 2012.

[283] H.-S. Kim, J. Paek, D. E. Culler, and S. Bahk, "Do not lose bandwidth : Adaptive transmission power and multihop topology control," in *Proceedings of the 13th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 99–108, 2017.

[284] H. Zhu and I. Chlamtac, "Performance analysis for IEEE 802.11 e EDCF service differentiation," *IEEE Transactions on wireless Communications*, vol. 4, no. 4, pp. 1779–1788, 2005.

[285] B. N. Clark, C. J. Colbourn, and D. S. Johnson, "Unit disk graphs," *Annals of Discrete Mathematics*, vol. 48, pp. 165–177, 1991.

[286] W. Mardini, S. Aljawarneh, A. Al-Abdi, and H. Taamneh, "Performance evaluation of RPL objective functions for different sending intervals," in *Proceedings of the 6th IEEE International Symposium on Digital Forensic and Security (ISDFS)*, pp. 1–6, 2018.

[287] M. O. Farooq and D. Pesch, "Reduced Overhead Routing in Short-Range Low-Power and Lossy Wireless Networks," *Sensors*, vol. 19, no. 5, p. 1240, 2019.

[288] Y. B. Aissa, H. Grichi, M. Khalgui, A. Koubâa, and A. Bachir, "QCOF : New RPL Extension for QoS and Congestion-Aware in Low Power and Lossy Network," in *Proceedings of the 14th International Conference on Software Technologies*, pp. 560–569, 2019.

[289] B. Safaei, A. M. H. Monazzah, T. Shahroodi, and A. Ejlali, "Objective function : A key contributor in Internet of Things primitive properties," in *Proceedings of IEEE International Conference on Real-Time and Embedded Systems and Technologies (RTEST)*, pp. 39–46, 2018.

[290] Q. Xu, X. Xiong, G.-L. Feng, M.-J. Guo, and L. Wan, "Design of Intelligent Campus Multimedia Interactive System Based on Internet of Things Technology," in *Proceedings of IEEE International Conference on Virtual Reality and Intelligent Systems (ICVRIS)*, pp. 223–226, 2019.

[291] A. Malik, J. Qadir, B. Ahmad, K.-L. A. Yau, and U. Ullah, "QoS in IEEE 802.11-based wireless networks : a contemporary review," *Journal of Network and Computer Applications*, vol. 55, pp. 24–46, 2015.

[292] J.-H. Lee, G.-S. Hong, Y.-W. Lee, C.-K. Kim, N. Park, and B.-G. Kim, "Design of efficient key video frame protection scheme for multimedia internet of things (IoT) in converged 5G network," *Mobile Networks and Applications*, vol. 24, no. 1, pp. 208–220, 2019.

[293] J. Kua, S. H. Nguyen, G. Armitage, and P. Branch, "Using active queue management to assist IoT application flows in home broadband networks," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1399–1407, 2017.

[294] P. Asghari, A. M. Rahmani, and H. H. S. Javadi, "Internet of Things applications : A systematic review," *Computer Networks*, vol. 148, pp. 241–261, 2019.

[295] C. Semeria, "Supporting differentiated service classes : queue scheduling disciplines," *Juniper networks*, pp. 11–14, 2001.

[296] M. Shreedhar and G. Varghese, "Efficient fair queueing using deficit round robin," in *Proceeings of ACM International Conference on SIGCOMM Computer Communication Review*, vol. 25, pp. 231–242, 1995.

[297] S. Park, J. Kim, G. M. Tihfon, H.-Y. Ryu, and J. Kim, "Dynamic multimedia transmission control virtual machine using weighted Round-Robin," *Cluster Computing*, vol. 19, no. 1, pp. 293–300, 2016.

[298] A. Colakovic and M. Hadzialic, "Internet of Things (IoT) : A review of enabling technologies, challenges, and open research issues," *Computer Networks*, vol. 144, pp. 17–39, 2018.

[299] H. Bouzebiba and M. Lehsaini, "Equilibrated DWRR Scheduling Algorithm for Multimedia Transmission in Internet of Multimedia Things," *Computers and Electrical Engineering*, p. Submitted paper.

[300] A. Dunkels, "Rime-a lightweight layered communication stack for sensor networks," in *Proceedings of the European Conference on Wireless Sensor Networks (EWSN), Poster/Demo session, Delft, The Netherlands*, 2007.

[301] J.-Y. Kwak, J.-S. Nam, and D.-H. Kim, "A modified dynamic weighted round robin cell scheduling algorithm," *ETRI journal*, vol. 24, no. 5, pp. 360–372, 2002.

[302] C.-C. Wu, H.-M. Wu, and W. Lin, "Efficient and fair multi-level packet scheduling for differentiated services," in *Proceedings of the 7th IEEE International Symposium on Multimedia (ISM'05)*, pp. 7–pp, 2005.

[303] C. Zhang and M. MacGregor, "Scheduling latency-critical traffic : a measurement study of DRR+ and DRR++," in *Proceedings of IEEE International Workshop on High Performance Switching and Routing, Merging Optical and IP Technologie*, pp. 262–267, 2002.

[304] W. Pattara-Atikom, P. Krishnamurthy, and S. Banerjee, "Distributed mechanisms for quality of service in wireless LANs," *IEEE Wireless Communications*, vol. 10, no. 3, pp. 26–34, 2003.

[305] S. S. Kanhere, H. Sethu, and A. B. Parekh, "Fair and efficient packet scheduling using elastic round robin," *IEEE Transactions on parallel and distributed systems*, vol. 13, no. 3, pp. 324–336, 2002.

[306] R. Riggio, D. Miorandi, and I. Chlamtac, "Airtime deficit round robin (ADRR) packet scheduling algorithm," in *Proceedings of the 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, pp. 647–652, 2008.

[307] A. G. P. Rahbar and O. Yang, "LGRR : A new packet scheduling algorithm for differentiated services packet-switched networks," *Computer Communications*, vol. 32, no. 2, pp. 357–367, 2009.

[308] D. Lin and M. Hamdi, "Two-stage fair queuing using budget round-robin," in *Proceedings of IEEE International Conference on Communications*, pp. 1–5, 2010.

[309] P.-B. Bok, K. Kohls, Y. Tuchelmann, and K. Kollorz, "I-DWRR-An insolvency enabled scheduling scheme extending Deficit Weighted Round Robin," in *Proceedings of IEEE GLOBECOM Workshops (GC Wkshps)*, pp. 695–700, 2011.

[310] C.-C. Li and K. Wang, "An SLA-aware load balancing scheme for cloud datacenters," in *Proceedings of IEEE International Conference on Information Networking (ICOIN2014)*, pp. 58–63, 2014.

[311] M. S. Sroya and V. Singh, "LDDWRR : Least Delay Dynamic Weighted Round-Robin Load Balancing in Software Defined Networking," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 145–148, 2017.

[312] Y. Han, B. Wang, C. Wang, and W. Wang, "The Dynamic Long-Term Equity DWRR Algorithm In Mine IoT," in *Proceedings of the 4th IEEE International Conference on Computer and Communications (ICCC)*, pp. 840–844, 2018.

[313] I. Saidu, N. A. Shinkafi, A. Roko, and A. Moyi, "A Prioritized Load Aware Weighted Round Robin (PLAWRR) algorithm in Broadband Wireless Networks," *European Journal of Electrical Engineering and Computer Science*, vol. 3, no. 4, pp. 1–4, 2019.

[314] C.-W. Huang, S.-C. Tseng, P. Lin, and Y. Kawamoto, "Radio Resource Scheduling for Narrowband Internet of Things Systems : A Performance Study," *IEEE Network*, vol. 33, no. 3, pp. 108–115, 2019.

[315] F. Al-Turjman, L. Mostarda, E. Ever, A. Darwish, and N. S. Khalil, "Network experience scheduling and routing approach for big data transmission in the Internet of Things," *IEEE Access*, vol. 7, pp. 14501–14512, 2019.

[316] M. M. Nasralla and M. G. Martini, "A downlink scheduling approach for balancing QoS in LTE wireless networks," in *Proceedings of the 24th IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1571–1575, 2013.

[317] M. M. Nasralla, N. Khan, and M. G. Martini, "Content-aware downlink scheduling for LTE wireless systems : A survey and performance comparison of key approaches," *Computer Communications*, vol. 130, pp. 78–100, 2018.

[318] M. K. Alam, S. Latif, M. Akter, M. Arafat, and S. Hakak, "Performance analysis of MAC layer scheduling schemes for IMM applications over high speed wireless campus network in IEEE802. 11e," *Indian Journal of Science and Technology*, vol. 8, no. S3, pp. 53–61, 2015.

[319] D.-H. Nguyen, H. Nguyen, and E. Renault, "E-mqs-a new downlink scheduler for real-time flows in lte network," in *Proceedings of the 84th IEEE Vehicular Technology Conference (VTC-Fall)*, pp. 1–5, 2016.

[320] D.-H. Nguyen, H. Nguyen, and E. Renault, "Performance evaluation of E-MQS scheduler with Mobility in LTE heterogeneous network," in *Proceedings of IEEE International Conference on Communications (ICC)*, pp. 1–6, 2017.

[321] M. M. Nasralla and I. U. Rehman, "QCI and QoS aware downlink packet scheduling algorithms for multi-traffic classes over 4G and beyond wireless networks," in *Proceedings of IEEE International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, pp. 1–7, 2018.

[322] F. K. Khalil, S. Khan, F. Faisal, M. Nawaz, F. Javed, F. A. Khan, R. M. Noor, M. Shoaib, F. U. Masood, *et al.*, "Quality of Service Impact on Deficit Round Robin and Stochastic Fair Queuing Mechanism in Wired-cum-Wireless Network," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 2, pp. 287–293, 2018.

[323] S. Kumar, A. Sarkar, S. Sriram, and A. Sur, "A three level LTE downlink scheduling framework for RT VBR traffic," *Computer Networks*, vol. 91, pp. 654–674, 2015.

Résumé

Ce travail entre dans le domaine d'internet des objets (IoT), et plus spécifiquement dans l'internet des objets multimédias (IoMT). En comparaison avec l'IoT, les réseaux IoMT exigent un certain niveau de qualité de service (QoS) plus élevé en termes de bande passante, de gigue, de fiabilité, de délai, etc. En effet, nous proposons d'aborder les problèmes d'incapacité des protocoles de communication d'IoT pour satisfaire les contraintes de QoS des applications l'IoMT. A cet effet, en commençant dans une première partie par une optimisation du protocole de routage RPL, qui est l'un des principaux éléments constitutifs des LLNs dans l'IoT, pour l'adapter aux communications multimédias. Dans ce contexte, nous avons proposé dans cette thèse une amélioration de ce protocole appelée *FreeBandWidth RPL* permettant un meilleur transfert de données multimédias dans les réseaux IoMT. Ce protocole est basé sur le calcul de la bande passante tout au long du chemin de routage et sur une fonction d'objectif adaptative pour avoir un meilleur équilibrage de charge entre les différents chemins de routage, particulièrement, lors d'une surcharge de données multimédias. Dans la deuxième partie, nous avons proposé une nouvelle extension équilibrée de l'algorithme d'ordonnancement DWRR, nommée *Equilibrated Deficit Weighted Round Robin (EDWRR)*. EDWRR garantit un taux de perte de paquets réduit dans chaque file d'attente et cela est due essentiellement à la procédure d'interruption de la mise en file d'attente de manière à avoir un taux de perte de paquets équilibré. L'implémentation des deux solutions proposées dans un émulateur a prouvé qu'elles sont plus performantes en comparaison avec les protocoles et les algorithmes d'ordonnancement concurrents.

Mots clés : IoT, IoMT, RPL, LLNs, QoS, Routage, Ordonnancement, DWRR.

Abstract

This work is part of the Internet of Things (IoT), and more specifically in the Internet of Multimedia Objects (IoMT). Compared to IoT, IoMT networks require a higher level of Quality of Service (QoS) in terms of bandwidth, jitter, reliability, data loss, delay, etc. Indeed, we propose to address the incapacity problems of IoT communication protocols to satisfy the QoS constraints of IoMT applications. To this end, starting in the first part with an optimization of the RPL routing protocol, which is one of the main components of LLNs in IoT, to adapt it to multimedia communications. Consequently, we have proposed in this thesis an improvement of this protocol called *FreeBandWidth RPL* allowing a better transfer of multimedia data in IoMT networks. It is based on the calculation of the bandwidth along the routing path and on an adaptive objective function to have a better load balancing between the different routing paths, in particular, during a multimedia data overload. In the second part, we proposed a new balanced extension of the DWRR scheduling algorithm, called *Equilibrated Deficit Weighted Round Robin (EDWRR)*. EDWRR guarantees a reduced packet loss rate in each queue and this is mainly due to the process of interrupting the queuing so as to have a balanced packet loss rate. The implementation of the two solutions proposed in an emulator has proven that they are more efficient in comparison with competing scheduling protocols and algorithms.

Keywords: IoT, IoMT, RPL, LLNs, QoS, routing, scheduling, DWRR.

ملخص

يعد هذا العمل جزءًا من إنترنت الأشياء، وبشكل أكثر تحديدًا في إنترنت الأشياء ذات الوسائط المتعددة. بالمقارنة مع إنترنت الأشياء ، تتطلب شبكات مستوى أعلى من جودة الخدمة من حيث النطاق الترددي والتذبذب والموثوقية وفقدان البيانات والتأخير وما إلى ذلك. في الواقع ، نقترح معالجة مشاكل عدم القدرة على بروتوكولات الاتصال بإنترنت الأشياء لتلبية متطلبات جودة الخدمة للتطبيقات. تحقيقا لهذه الغاية ، بدءا من الجزء الأول مع تحسين بروتوكول توجيه، الذي يعد أحد المكونات الرئيسية لـ LLNs في إنترنت الأشياء ، لتكييفه مع اتصالات الوسائط المتعددة. وبالتالي ، اقترحنا في هذه الأطروحة تحسين هذا البروتوكول المسمى مما يسمح بنقل أفضل لبيانات الوسائط المتعددة في الشبكات. وهو يعتمد على حساب عرض النطاق الترددي على طول مسار التوجيه وعلى وظيفة الهدف التكيفي للحصول على موازنة تحميل أفضل بين مسارات التوجيه المختلفة ، على وجه الخصوص ، أثناء التحميل الزائد لبيانات الوسائط المتعددة. في الجزء الثاني ، اقترحنا امتدادًا جديدًا متوازنًا لخوارزمية جدولة، تسمى عجز الموازنة المرجحة. يضمن انخفاض معدل فقدان الحزمة في كل قائمة انتظار وهذا يرجع بشكل رئيسي إلى عملية مقاطعة قائمة الانتظار للحصول على معدل فقدان حزم متوازن. أثبت تطبيق الحلين المقترحين في المحاكي أنهما أكثر كفاءة مقارنة ببروتوكولات وخوارزميات الجدولة المتنافسة.

الكلمات المفتاحية :IoT، IoMT، QoS، LLN، RPL، DWRR، التوجيه ، الجدولة.