République Algérienne Démocratique Et Populaire
Ministère de L'enseignement Supérieur et de la Recherchre Scientifique

Université de Djilali Bounaâma-Khemis Miliana

Faculté des Sciences et de la Technologie
Département de Mathématiques et Informatique

Mémoire de Master

en Informatique

Spécialité :Génie Logiciel et Système Distribué

Thème

Amélioration des performances du protocole de routage multicast MAODV pour l'internet des objets

---

Présenté par :

Drani Nourhane

Frid Hadia

Membres du jury :

Encadrante : Mme.H.Hachichi.

Co-Encadrant : Mr.O.Harbouche.

Président : Mr.S.Hadj Sadouk

Examinateur : Mr.N.Azouza

Année universitaire : 2022-2023

Remerciement

Nous remercions tout d'abord **ALLAH** tout-puissant de nous avoir armés de force et la volonté nécessaire pour La réalisation de ce modeste travail.
Nous tenons à exprimer nos profondes gratitudes et nos sincère remerciements à notre encadreur **M.Harbouche Oussama** pour l'honneur qu'il nous fait en acceptant de guider cette mémoire avec ses conseils et son aide précieuse. Sans vous, la réalisation de ce mémoire n'aurait pas eu lieu. Encore une fois, merci beaucoup.
Nous tenons à exprimer notre profonde gratitude à tous ceux qui ont aidé aide et encourageme.
Nous remercions les membres du jury qui nous font le grand honneur d'évaluer notre travail.
Nous exprimons notre profonde gratitude à tous les enseignants du département d'Informatique de l'université Djilali Bounaama pour les connaissances qu'ils nous ont transmises tout au long de notre parcours universitaire en vue d'obtenir notre diplôme de master.
Et enfin, nous exprimons nos plus profonds et sincères remerciements à nos parents et à nos familles qui nous ont toujours soutenus, encouragés et aidés. Ils ont su nous donner toutes les chances de réussir.

Dédicaces

Je consacre ce modeste travail :

Á mes chèrs parents symbole de sacrifice, de tendresse, qui m'ont a éclairée mon chemin et qui m'ont encouragé et soutenue toute au long de mes études,

Á mes frères Rayane ,Yasser et Baraa je vous souhaite beaucoup de joie, de réussites et de bonheur dans la vie,

Á qui m' a aidé et supporté dans les moments difficiles a qui a resté à côté de moi mon chèr mari monaim ,

Á Hadia, chère amie, avant d'être binôme,

Á ma chèr famille,

Á mes chèrs amis ,

Á tous mes enseignants,

Á tous ceux qui ont apporté de l'aide de près ou de loin pour la réalisation de ce travail.

Merci.

Drani Nourhane

Dédicaces

Je tiens à dédier cet événement marquant de ma vie :

Á mes chers parents, qui ont toujours été présents pour moi. Ils ont illuminé mon parcours, m'ont encouragé et soutenu tout au long de mes études ,

Je souhaite particulièrement exprimer ma profonde gratitude envers mamère, qui occupe une place spéciale dans mon cœur. Quelles que soient mes actions ou paroles, les mots semblent insuffisants pour exprimer toute ma reconnaissance envers elle. Ta présence à mes côtés a toujours été une source inébranlable de force face aux obstacles que j'ai rencontrés. Ta bienveillance et ton soutien inconditionnel ont été des piliers indispensables dans ma vie. Je suis profondément reconnaissante d'avoir des parents aussi merveilleux, incarnant le sacrifice et la tendresse ,

Á mes frères Abdelhassib, Abdallah et Abderrahmane, je vous souhaite une abondance de joie, de réussite et de bonheur dans la vie,

Á celui qui m'a aidé et soutenu tout au long de cette année dans les moments difficiles, qui est resté à mes côtés,les mots semblent insuffisants pour exprimer toute ma gratitude envers lui. Que Dieu préserve Kamel pour moi .

Á ma chèr famille,

Á mes chèrs amis,

Á tous mes enseignants,

Á Nourhane, chère amie, avant d'être binôme,

Á tous ceux qui ont apporté leur aide, que ce soit de près ou de loin, pour la réalisation de ce travail.

Merci.

Frid Hadia

Résumé

Les protocoles de routage jouent un rôle crucial dans la mise en place des réseaux IoT. Ils permettent aux données de trouver leur chemin à travers un réseau et déterminent les chemins optimaux pour acheminer les paquets de données entre les différents nœuds du réseau. Dans ce contexte, les protocoles de routage sont responsables de l'établissement des routes de communication entre les objets connectés. Ils déterminent les chemins les plus efficaces pour acheminer les données d'un objet à un autre, en tenant compte de facteurs tels que la disponibilité des nœuds, la qualité des liens, la latence, la consommation d'énergie, etc.

Dans ce travail, nous proposons d'utiliser les nœuds critiques du réseau comme élément clé dans l'établissement des chemins de routage. Un nœud critique est un élément essentiel au maintien de la cohérence du réseau, et sa suppression aurait pour conséquence une dégradation de la connectivité globale. Cette approche offre une solution plus ou moins optimale, puisque les variantes du problème de détection des nœuds critiques (CNDP) visent toujours à minimiser leur nombre ou à éviter leur présence en adaptant les ressources existantes.

Pour atteindre cet objectif, nous avons utilisé le simulateur NS2 pour simuler le protocole MAODV et évaluer notre proposition. Les résultats obtenus ont ensuite été comparés à ceux issus de la simulation de notre proposition.

Mots clés : Internet des Objets, MAODV, nœuds critiques, CNDP, , CNP, 3C-CNP.

Abstract

Routing protocols play a crucial role in setting up IoT networks. They enable data to find its way through a network, and determine the optimal paths for routing data packets between different network nodes. In this context, routing protocols are responsible for establishing communication routes between connected objects. They determine the most efficient paths for routing data from one object to another, taking into account factors such as node availability, link quality, latency, energy consumption and so on consumption, etc.

In this work, we propose to use critical network nodes as a key element in establishing routing paths. A critical node is an essential element in maintaining network coherence, and its removal would result in a degradation of overall connectivity. This approach offers a more or less optimal solution, since variants of the critical node detection problem (CNDP) always aim to minimize their number or avoid their presence in the network. minimizing their number or avoiding their presence by adapting existing resources.

To achieve this objective, we used the NS2 simulator to simulate the MAODV protocol and evaluate our proposal. The results obtained were then compared with those obtained from the simulation of our proposal.

Keywords : Internet Of Things,MAODV,critical nodes,CNDP, CNP, 3C-CNP.

Table des matières

Liste des tableaux

Table des figures

Liste des abréviations

IoT Internet of Things .

IdO Internet des Objets.

DSDV Destination-Sequenced Distance-Vector.

OLSR Optimized Link State Routing Protocol.

DREAM Distance Routing Effect Algorithm for Mobility.

DSR Dynamic Source Routing.

AODV Ad Hoc On demand Distance Vector Routing.

RREQ Route Request.

RREP Route Reply.

RERR Route Error.

ZRP Zone Routing Protocole.

IARP IntrAzone Routing Protocol .

IERP IntErzone Routing Protocol.

OC Objet Connecté.

ODMRP On Demand Multicast Routing Protocol.

JQ Join Query.

CAMP Core-Assisted Mesh ProtocoL.

MAODV Multicast Ad hoc On Demand Vector.

RPL Routing Protocol for Low power and lossy networks-LLNS.

DODAG Destination Oriented Directe Acyclic Graph.

DAG Directed Acyclic Graph.

DIO DODAG Information Object.

DAO Destination Advertisement Object.

DIS DODAG Information Sollicitation.

COAP Constrained Application Protocol.

HTTP Hypertext Transfer Protocol.

OSI Open Systems Interconnection.

UDP User Datagram Protocol.

ETX Expected Transmission Count.

ETT Expected Transmission Time.

WCETT Weighted Cumulative ETT .

iAWARE interference AWARE.

LD Link Duration.

CNDP critical nodes detection problem.

CNP Critical node problem.

3C-CNP Three-level Clustering Network Protocol.

NS2 Network Smilator.

OTCL (Object Tools Command Language.

Introduction générale

Avec l'avancement des technologies sans fil et l'émergence de l'Internet des Objets (IdO), les réseaux ad hoc ont gagné en importance en tant que moyen de communication essentiel. Les réseaux sans fil traditionnels permettent aux utilisateurs de se connecter à un point d'accès central, tel qu'un routeur ou une antenne de téléphonie mobile, pour accéder à Internet ou à d'autres services. Cependant, dans de nombreux scénarios, il n'est pas possible ou pratique d'avoir une infrastructure de communication centralisée. C'est là que les réseaux ad hoc entrent en jeu.

Un réseau ad hoc est un type de réseau sans fil où les nœuds, tels que les appareils mobiles ou les capteurs, peuvent se connecter directement les uns aux autres sans passer par une infrastructure centralisée. L'intégration des réseaux ad hoc dans l'Internet des Objets offre des possibilités infinies pour la collecte et le partage d'informations entre des objets connectés. Cependant, le routage dans ces réseaux ad hoc de l'IdO présente des défis uniques. Le routage dans les réseaux ad hoc de l'IdO vise à trouver des chemins efficaces pour transmettre les données entre les nœuds. De plus, ils doivent garantir la fiabilité des communications et la conservation des ressources, tout en minimisant la consommation d'énergie et en prolongeant la durée de vie des dispositifs.

Ce mémoire se concentre sur l'amélioration du protocole de routage réactif MAODV (Multicast Ad hoc On-Demand Vector) dans le contexte de l'Internet des Objets (IdO). Le MAODV est un protocole de routage largement utilisé dans les réseaux ad hoc, mais il nécessite des ajustements pour répondre aux exigences spécifiques des réseaux de l'IdO. En reliant le protocole MAODV à la détection des nœuds critiques à l'aide de la théorie des graphes, on peut améliorer la performance globale du réseau ad hoc. En identifiant et en renforçant les nœuds critiques, on peut réduire les temps de transmission, améliorer la stabilité du routage et réduire la consommation d'énergie. Cela contribue à une meilleure fiabilité et une meilleure efficacité

du protocole MAODV dans les réseaux ad hoc.Ce mémoire est structuré en trois chapitres afin d'explorer en détail les différents aspects liés aux protocoles de routage. Le premier chapitre présente les généralités concernant les protocoles de routage, ainsi que les concepts liés aux réseaux mobiles Ad-Hoc et à l'internet des objets. Le deuxième chapitre se concentre spécifiquement sur le protocole MAODV. Il aborde sa définition, son fonctionnement général, ainsi que ses mécanismes de routage et les différentes métriques utilisées. Enfin, le dernier chapitre est dédié à l'évaluation et à l'amélioration du protocole MAODV. Il présente les résultats des simulations réalisées sur NS2 et propose des améliorations basées sur ces résultats.

Chapitre 1

LES PROTOCOLES DE ROUTAGE DANS L'IDO

1.1 Introduction

Les réseaux sans fil connaissent une expansion croissante et ont suscité un intérêt considérable ces dernières années. Les réseaux mobiles ad hoc, ou MANET (Mobile Ad hoc Network), sont des réseaux locaux sans fil, dépourvus d'infrastructure et fonctionnant avec un contrôle distribué. Ils peuvent être définis comme un ensemble de nœuds interconnectés et communicants, pouvant être mobiles, sans nécessiter de support fixe ni d'administration centralisée. Le déploiement d'un réseau ad hoc est simple et ne requiert aucun prérequis ; il suffit de disposer de terminaux dans un espace donné pour créer un réseau ad hoc. Chaque nœud du réseau se comporte comme un routeur et transmet les paquets vers d'autres nœuds. Le chemin suivi par les paquets, depuis un nœud source jusqu'à un nœud destination, est déterminé par un protocole de routage.

Dans ce chapitre, nous abordons les concepts de base liés aux réseaux ad hoc. Nous détaillons les notions fondamentales sur les réseaux sans fil, puis nous présentons les principales caractéristiques des réseaux ad hoc. Ensuite, nous définissons le routage, plus particulièrement les protocoles de routage dans les MANETs, en mettant en évidence leurs caractéristiques et en les classifiant pour présenter différents exemples de protocoles de routage. Enfin, nous proposons une vue d'ensemble de l'Internet des objets.

1.2 Les réseaux sans fil :

1.2.1 Définition d'un réseau sans fil :

Les réseaux ad hoc sont des réseaux radio qui se déploient facilement et automatiquement entre des individus souhaitant communiquer entre eux, sans qu'il soit nécessaire de mettre en place une infrastructure complète. Ils fonctionnent selon le principe du pair-à-pair (Peer to Peer), ce qui signifie que deux stations peuvent communiquer entre elles si elles sont suffisamment proches l'une de l'autre. De nombreuses techniques de création de ce type de réseau sont actuellement étudiées dans divers laboratoires de recherche.[1]

1.2.2 Les architectures d'un réseau sans fil :

1. **Mode avec infrastructure :**

   Ce mode de fonctionnement est très semblable au protocole Ethernet des réseaux filaires. Les machines se connectent à un point d'accès appelé aussi station de base, qui partage la bande passante disponible. Les stations de base sont munies d'une interface de communication sans fil avec les sites mobiles qui se trouvent dans sa zone géographique ou sa couverture radio.[2]

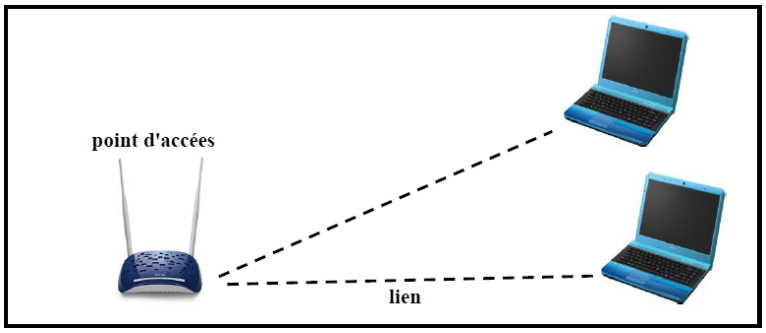


FIGURE 1.1 – Mode sans infrastructure.

2. ***Mode sans infrastructure ou réseau Ad hoc :***

   Ce mode ne nécessite pas de point d'accès car les stations elles-mêmes initient la communication sans dépendre d'un équipement externe. Chaque nœud d'un tel réseau se comporte comme un routeur et contribue à trouver et maintenir des chemins de communication entre les différents appareils. Ce type de réseau s'organise de manière auto-organisée et dynamique, où les nœuds coopèrent pour acheminer les données et assurer la connectivité du réseau. [2]

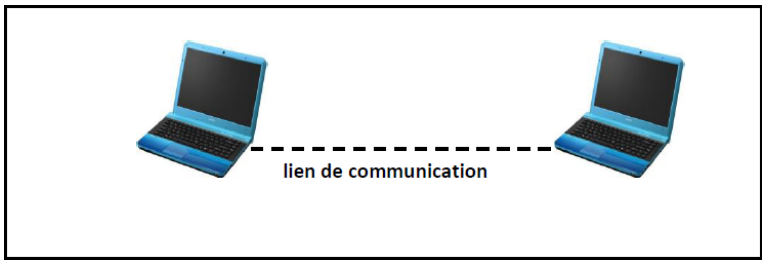


FIGURE 1.2 – Mode sans infrastructure.

1.3 Les réseaux mobiles Ad hoc :

1.3.1 Définition :

Un réseau ad hoc, généralement appelé MANET (Mobile Ad hoc Network), est composé d'un ensemble relativement dense de nœuds mobiles qui se déplacent librement dans une certaine zone géographique, sans aucune infrastructure fixe préexistante. Chaque nœud dans le réseau ad hoc peut communiquer directement avec un autre nœud à portée de transmission via son interface sans fil, ou indirectement en passant par d'autres nœuds du réseau. Chaque nœud dans le réseau ad hoc joue à la fois le rôle d'un terminal et d'un routeur, participant ainsi à la découverte et à la maintenance des routes entre les nœuds du réseau. Il n'y a pas de limitation de taille pour un réseau ad hoc, qui peut contenir des dizaines ou des milliers de nœuds.[3]

FIGURE 1.3 – Réseau en mode ad-hoc.

1.3.2 Les caractéristiques des réseaux Ad hoc :

Les réseaux mobiles Ad hoc sont caractérisés par ce qui suit :

— **Une topologie dynamique :** Il s'agit d'une des caractéristiques les plus importantes des réseaux ad hoc, où la topologie du réseau change en raison de facteurs incontrôlables tels que la mobilité des nœuds, les interférences et le bruit.[4]

— **L'absence d'infrastructure :** Les réseaux ad hoc se distinguent des autres réseaux mobiles par le fait qu'ils n'ont pas d'infrastructure préexistante ni de système d'administration centralisée. Les hôtes mobiles sont responsables d'établir et de maintenir la connectivité du réseau de manière autonome. [5]

— **Contrainte d'énergie :** Les nœuds dans un réseau ad hoc sont généralement alimentés par des batteries dont la capacité en puissance est souvent limitée. Cela nécessite une

gestion efficace de l'énergie pour prolonger la durée de vie des nœuds et assurer le bon fonctionnement du réseau. [4]

— **Sécurité physique limitée :** Les réseaux ad hoc sont plus vulnérables par rapport aux réseaux filaires et cellulaires en raison de la nature sans fil du support de transmission et de la topologie dynamique du réseau. Des mesures de sécurité appropriées doivent être prises pour protéger les communications contre les attaques et les intrusions. [4]

1.3.3 Utilité et application :

De nos jours, de nombreux systèmes utilisent déjà les technologies sans fil, telles que la téléphonie mobile, et connaissent une expansion considérable. Cependant, ces systèmes nécessitent une infrastructure logistique et matérielle fixe importante pour leur fonctionnement. Les réseaux ad hoc sont idéaux pour des applications caractérisées par l'absence ou la non-fiabilité d'une infrastructure préexistante. Voici quelques exemples d'applications qui bénéficient des réseaux ad hoc :

• Les applications militaires.
• Opérations de secours et missions d'exploration.
• Les bases de données parallèles.
• Enseignement à distance et systèmes de fichiers répartis .
• Simulation distribuée interactive et calcul distribué . [1]

1.4 Théorie du Routage :

1.4.1 Définition du routage dans les réseaux ad hoc :

Le routage dans les réseaux ad hoc englobe un ensemble de mécanismes ou de protocoles qui permettent la découverte des éléments de la topologie du réseau, l'acheminement des paquets depuis la source jusqu'à la destination, et la maintenance des liens de communication en cas de rupture. Étant donné l'absence d'infrastructure et de gestion centralisée dans les réseaux ad hoc, les nœuds mobiles doivent être capables de prendre en charge le routage.

En raison des limitations des réseaux ad hoc, il est essentiel que la construction des chemins de routage se fasse avec un minimum de messages de contrôle et de consommation de bande passante. Par conséquent, de nouveaux protocoles de routage sont spécifiquement conçus pour répondre aux caractéristiques des réseaux ad hoc.[5]

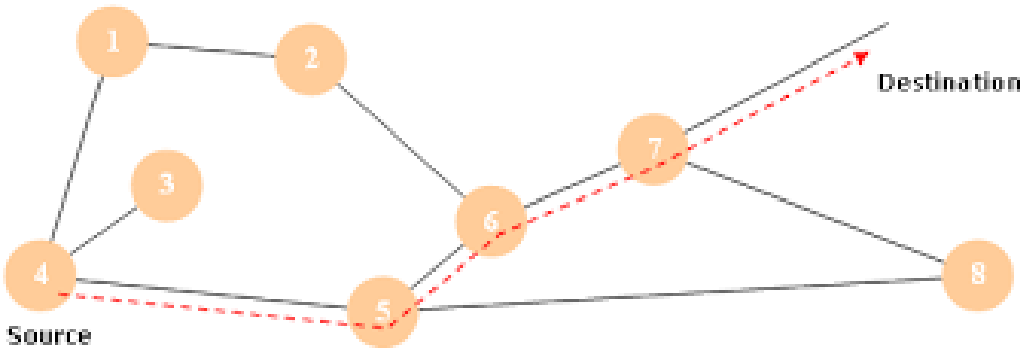


FIGURE 1.4 – Le routage dans les réseaux ad hoc.

1.4.2 Les phases de routage dans les réseaux ad hoc :

Pour assurer un fonctionnement efficace dans un environnement mobile, un protocole de routage dans les réseaux ad hoc se divise généralement en trois phases :

1. **Découverte de l'information de routage :** Cette étape permet d'obtenir les informations nécessaires sur la topologie du réseau afin de choisir un chemin vers le nœud destination. Les nœuds échangent des informations pour obtenir une vue précise de la topologie du réseau. Les protocoles de routage optimisent l'envoi de ces informations pour minimiser la consommation de ressources. [6]
2. **Choix de chemin :** Une fois que les informations de routage sont collectées, le protocole de routage sélectionne un chemin vers la destination. Généralement, le choix du chemin se fait en minimisant le nombre de sauts nécessaires pour atteindre la destination, en sélectionnant le chemin le plus court. Il est également important d'éviter la formation de boucles dans les routes choisies, car cela rendrait le chemin inutilisable, gaspillant ainsi de la bande passante et de l'énergie. [6]
3. **Maintenance des routes :** La topologie d'un réseau ad hoc est en constante évolution en raison de la mobilité des nœuds. Par conséquent, les routes doivent être mises à jour en temps réel pour s'adapter à ces changements. Une route ne doit pas rester invalide pendant une longue période, car cela empêcherait les paquets d'atteindre leur destination.[6]

1.4.3 L'objectif de protocole de routage dans les réseaux ad hoc :

On peut se résumer en cinq points :

— Découvrir dynamiquement les routes vers les sous réseaux d'un réseau et les inscrire dans une table de routage.

— Sélectionner le chemin le plus court vers un sous-réseau .

— Détecter et supprimer les routes invalides.

— Ajouter rapidement de nouvelles routes ou mettre à jour les meilleures routes .

— Prévenir les boucles de routage.[6]

1.4.4 La classification des protocoles de routage :

Les protocoles de routage peuvent être classés dans différents groupes selon leurs caractéristiques. Plus précisément, les protocoles de routage peuvent être classés en fonction de :

A. L'établissement de la route :

1. **Les protocoles de routage proactifs :**

   Les protocoles de routage proactifs essaient de maintenir les meilleurs chemins existants vers toutes les destinations possibles (qui peuvent représenter l'ensemble de tous les nœuds du réseau) au niveau de chaque nœud du réseau. Les routes sont sauvegardées mêmes si elles ne sont pas utilisées. La sauvegarde permanente des chemins de routage, est assurée par un échange continu des messages de mise à jour des chemins, ce qui induit un contrôle excessif surtout dans le cas des réseaux de grande taille. [7] Parmi les protocoles qui appartiennent à cette classe :

   — **Le protocole DSDV (Destination-Sequenced Distance-Vector) :** DSDV (Destination-Sequenced Distance-Vector) est un protocole proactif à vecteur de distance utilisant le routage par saut. Chaque entrée de la table de routage est composée d'une destination, du prochain saut pour atteindre la destination, d'une métrique correspondant au nombre de sauts pour atteindre la destination ainsi que d'un numéro de séquence associé. Le numéro de séquence, assigné par la destination, permet de garantir un routage sans boucle et de s'assurer de la fraîcheur des routes. Lorsqu'un nœud reçoit de nouvelles informations de routage, il les compare à celles de sa table de routage. La nouvelle route vers une destination est préférée si elle a un numéro de séquence plus élevé ou si elle possède le même numéro de séquence et une métrique inférieure. La maintenance des informations de routage est assurée par la transmission de mises à jour de manière périodique (suivant le principe des paquets Hello dans OSPF) ainsi que lors de changements de topologie. [8]

— **Le protocole OLSR (Optimized Link State Routing Protocol) :** OLSR est un protocole proactif, cela signifie que le protocole a une vue globale sur le réseau. Ce protocole a été conçu pour minimiser l'inondation classique du trafic de contrôle par une inondation sélective en utilisant seulement des nœuds spécifiques appelés MPR. Les nœuds MPR sont les seuls nœuds autorisés à diffuser les messages de contrôle. Chaque nœud dans le réseau choisit son MPR parmi ses voisins symétriques pour atteindre les voisins symétriques à deux sauts. [5]

— **Le protocole DREAM (Distance Routing Effect Algorithm for Mobility) :** Le protocole appelé "Algorithme d'Effet de Routage basé sur la Distance, pour la Mobilité" procède par inondation partielle afin de découvrir une route inexistante. Si la source dispose d'informations récentes elle choisit de diffuser sa requête sur un ensemble précis de nœuds voisins. Sinon elle inonde tout le réseau. Nous économisons ainsi le nombre de paquets en circulation. Quand le nœud destination reçoit les données, il envoie des acquittements à la source d'une manière similaire. Dans le cas où la source envoie les données, un timer associé à la réception des acquittements est activé. Si aucun acquittement n'est reçu avant l'expiration du timeout, les données seront retransmises en utilisant une diffusion ordinaire. [9]

2. **Les protocoles de routage réactifs :**

Les protocoles de routage appartenant à cette catégorie, créent et maintiennent les routes selon les besoins. Lorsque le réseau a besoin d'une route, une procédure de découverte globale de routes est lancée, et cela dans le but d'obtenir une information spécifique, inconnue au préalable. [1] Les principaux protocoles réactifs sont :

— **DSR (Dynamic Source Routing) :** Le protocole "Routage à Source Dynamique" (DSR), est basé sur l'utilisation de la technique "routage source". Dans cette technique : la source des données détermine la séquence complète des nœuds à travers lesquelles, les paquets de données seront envoyés. [10]

— **AODV (Ad Hoc On demand Distance Vector Routing) :** Le protocole AODV est un protocole basé sur la construction des tables de routage. En effet, chaque nœud possède sa propre table de routage contenant pour chaque destination le prochain nœud à contacter. La découverte d'une route se fait par inondation par l'émetteur d'un paquet RREQ (Route Request). A la réception d'un de ces paquets, si le nœud connait le chemin pour accéder à la source, il envoie une réponse RREP (Route Reply) a l'émetteur qui arrête d'inonder le réseau.si le nœud ne connait pas le chemin, il

transmet le paquet a ses voisins tout en mémorisant le nœud précédent ayant fait la requête. En cas de cassure du lien, un message RERR (Route Error) est envoyé à l'émetteur qui décide ou non de recommencer l'envoie du paquet suivant le taux d'utilisation de la route. [11]

3. **Les protocoles de routage hybrides :**

   Les protocoles hybrides combinent les deux idées : celle des protocoles proactifs et celle des protocoles réactifs. Ce type de protocoles s'adapte bien aux grands réseaux. Ils utilisent un protocole proactif pour avoir des informations sur les voisins les plus proches (au maximum les voisins à deux sauts). Au-delà de cette zone prédéfinie, le protocole hybride fait appel aux techniques des Protocoles réactifs pour chercher des routes.[12] Parmi les protocoles qui appartiennent à cette classe :

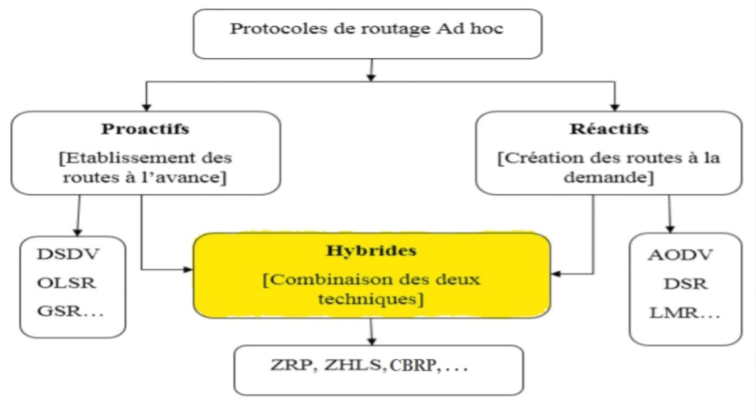


FIGURE 1.5 – Le protocole hybride.

— **ZRP (Zone Routing Protocole) :** ZRP est un protocole hybride. Dans le voisinage proche d'un nœud, ZRP utilise une technique de routage proactif classique. Pour router des chemins en dehors de cette zone de voisinage, ZRP s'appuie sur une technique réactive. ZRP définit pour chaque nœud une zone de routage, qui inclut tous les nœuds dont la distance minimale à ce nœud est x. Les nœuds qui sont exactement à la distance x sont appelés nœuds périphériques. Pour trouver une route vers des nœuds situés à une distance supérieure à x, ZRP utilise un système réactif, qui envoie une requête à tous les nœuds périphériques. ZRP met pour cela en œuvre deux types de fonctionnement : IARP (IntrAzone Routing Protocol) et IERP (IntErzone Routing Protocol). [13]

B. Les fonctions des protocoles :

1. **Routage Unicast :**

   Dans les réseaux informatiques, le terme unicast est une méthode de transmission dans laquelle une station envoie des informations à une autre station. C'est une communication un-à-un. La transmission unicast est utilisée, où une station transmet des informations privées ou uniques à une autre station. Par exemple la navigation sur le Web, ici, il y a un seul demandeur de service et un seul fournisseur de services.[14]

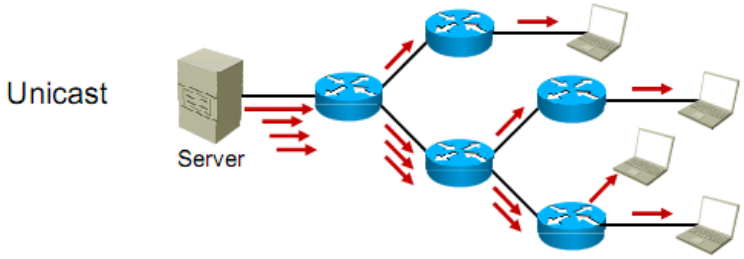


FIGURE 1.6 – Routage Unicast.

2. **Routage Multicast :**

   Multicast, est une méthode de transmission d'information où une station transmet le paquet d'information aux stations intéressées seulement. C'est une méthode de communication un-à-plusieurs. C'est un mélange entre Unicast et Broadcast, où l'Unicast envoie le paquet à une seule station, et le Broadcast envoie le paquet à toutes les stations, le Multicast n'envoie le paquet qu'à certaines stations sélectionnées dans le réseau. Des exemples de Multicast sont la transmission de courriels, la livraison multimédia, etc. [14]

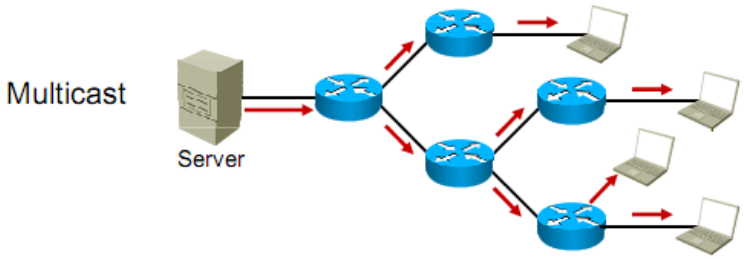


FIGURE 1.7 – Routage Multicast.

1.5 Internet des objets :

1.5.1 Objet Connecté :

Avant de définir les concepts d'IdO, il est important de définir l'objet connecté qui est un dispositif dont la finalité première n'est pas d'être un système informatique ni une interface d'accès au web, exemple, un objet tel qu'une machine à café ou une serrure était conçue sans intégration de systèmes informatiques ni connexion à Internet. L'intégration d'une connexion Internet a un OC permet de l'enrichir en terme de fonctionnalité, d'interaction avec son environnement, il devient un OC Enrichi(OCE), par exemple, l'intégration d'une connexion internet à la machine à café la rendant accessible à distance. Un OC peut interagir avec le monde physique de manière indépendante sans intervention humaine. Il possède plusieurs contraintes telles que la mémoire, la bande passante ou la consommation d'énergie. Un objet connecté a une valeur lorsqu'il est connecté à d'autres objets et briques logicielles, par exemple : une montre connectée n'a d'intérêt qu'au sein d'un écosystème orienté santé/bien-être, qui va bien au-delà de connaître l'heure.[15]

Un OC à trois éléments clés :

– Les données produites ou reçues, stockées ou transmises.

– Les algorithmes pour traiter ces données.

– L'écosystème dans lequel il va réagir et s'intégrer.

Les propriétés d'usage d'un OC :

– Ergonomie (utilisabilité, maniabilité, ...).

– Esthétisme (formes/couleurs/sons/sensations, ...).

– Usage (histoire culturelle, profil, matrice sociale, ...).

– Méta-Morphisme (adaptabilité, personnalisation, modulation, ...).[16]

1.5.2 Définition d'IDO :

Kevin Ahston, le cofondateur de l'Auto-ID Center du MIT a employé le terme « Internet Of Things (Internet des Objets) » en 1999. IDO a été prononcé dans le cadre d'une présentation pour l'entreprise Procter Gamble (PG). Ce terme convoque, le monde d'objets, d'appareils et de capteurs qui sont interconnectés par internet.

Le CERP-IdO « Cluster des projets européens de recherche sur l'Internet des objets » définit l'internet des objets comme : « une infrastructure dynamique d'un réseau global. Ce réseau

global a des capacités d'auto-configuration basée sur des standards et des protocoles de communication interopérables. Dans ce réseau, les objets physiques et virtuels ont des identités, des attributs physiques, des personnalités virtuelles et des interfaces intelligentes, et ils sont intégrés au réseau d'une façon transparente».

Cette définition montre les deux aspects de l'IdO : temporel et spatial qui permettent aux personnes de se connecter de n'importe où à n'importe quel moment à travers des objets connectés (smartphone, tablettes, capteurs, caméras de vidéosurveillance...).
L'Internet des objets doit être pensé pour un usage facile et une manipulation sécurisée pour éviter des menaces et risques potentiels, tout en masquant la complexité technologique sous-jacente. [15]

FIGURE 1.8 – Internet des objets.

1.5.3 Caractéristiques de l'Internet des objets :

Il existe les caractéristiques suivantes de l'IoT comme suit : [16]

Connectivité :

La connectivité est une exigence importante de l'infrastructure IoT. Les objets de l'IoT doivent être connectés à l'infrastructure IoT. N'importe qui, n'importe où, n'importe quand peut se connecter, cela devrait être garanti à tout moment. Par exemple, la connexion entre les personnes via des appareils Internet tels que les téléphones mobiles et d'autres gadgets, ainsi que la connexion entre les appareils Internet tels que les routeurs, les passerelles, les capteurs, etc.

Intelligence et identité :

L'extraction de connaissances à partir des données générées est très importante. Par exemple, un capteur génère des données, mais ces données ne seront utiles que si elles sont correctement interprétées. Chaque appareil IoT a une identité unique. Cette identification est utile pour suivre l'équipement et parfois pour interroger son état.

Évolutivité :

Le nombre d'éléments connectés à la zone IoT augmente de jour en jour. Par conséquent, une configuration IoT devrait être capable de gérer l'expansion massive. Les données générées en tant que résultat sont énormes et doivent être traitées de manière appropriée.

Dynamique et auto-adaptatif (complexité) :

Les appareils IoT doivent s'adapter de manière dynamique aux contextes et scénarios changeants. Supposons une caméra destinée à la surveillance. Il doit être adaptable pour travailler dans différentes conditions et différentes situations d'éclairage (matin, après-midi, nuit).

Architecture :

L'architecture IoT ne peut pas être de nature homogène. Il devrait être hybride, prenant en charge les produits de différents fabricants pour fonctionner dans le réseau IoT. IoT n'appartient à aucune branche d'ingénierie. L'IoT est une réalité lorsque plusieurs domaines se rejoignent.

Sécurité :

Il existe un risque que les données personnelles sensibles des utilisateurs soient compromises lorsque tous leurs appareils sont connectés à Internet. Cela peut entraîner une perte pour l'utilisateur. La sécurité des données est donc le défi majeur. De plus, l'équipement impliqué est énorme. Les réseaux IoT peuvent également être à risque. Par conséquent, la sécurité des équipements est également essentielle.

1.5.4 Les domaines d'application de l'IdO :

Les potentialités oertes par l'IdO et son aspect ubiquitaire permettent de développer de nombreuses applications. Cependant, seules quelques applications sont actuellement déployées.

L'utilisation de l'IdO permettra le développement de plusieurs applications intelligentes à l'avenir qui toucheront essentiellement : la domotique, les villes, le transport, la santé et l'industrie.

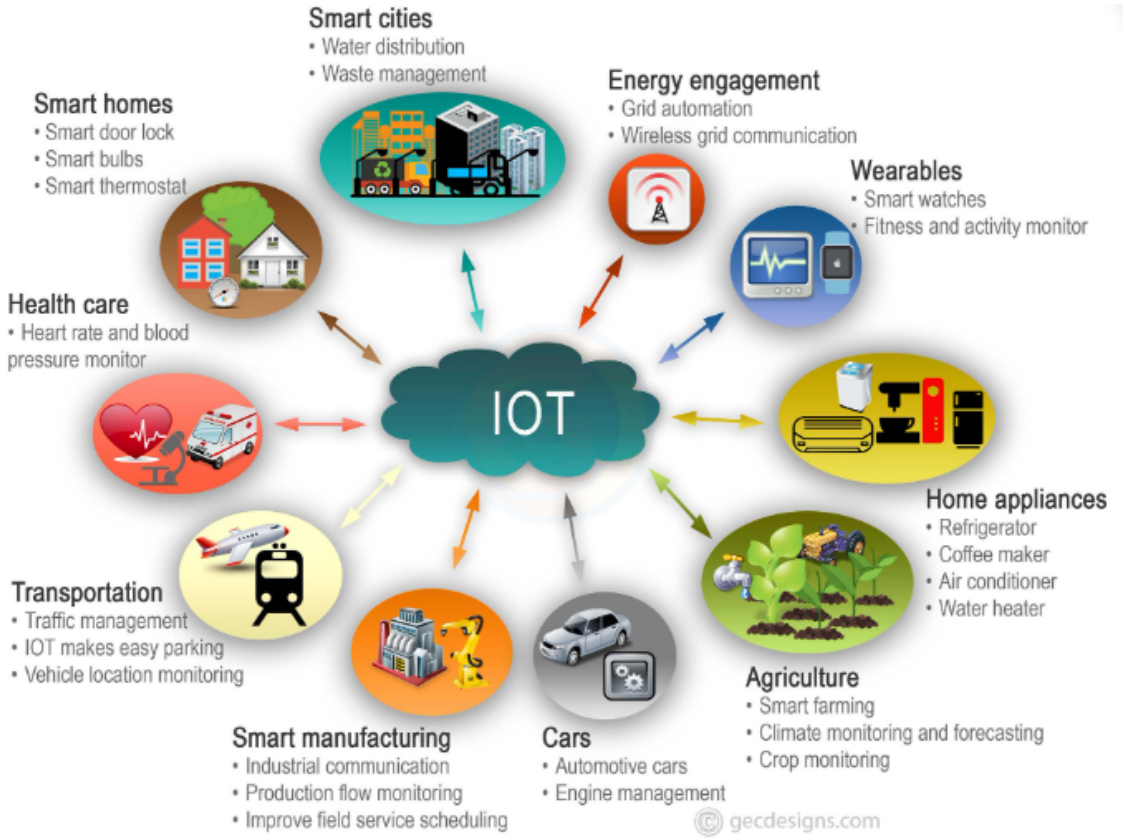


FIGURE 1.9 – Les domaines de IdO.

1.5.5 Les protocoles de l'internet des objets :

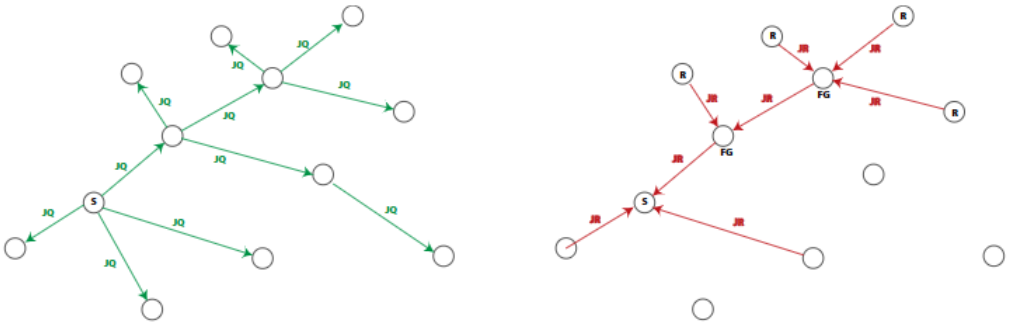
1. Protocole ODMRP

ODMRP est un protocole de routage multidiffusion réactif, destiné à être utilisé dans les réseaux mobiles ponctuels (MANET). L'ODMRP est un système multicast basé sur un maillage plutôt que sur un arbre, qui offre plus de fiabilité et est plus facile à maintenir des topologies in dynamiques. Il applique des procédures à la demande pour construire dynamiquement des itinéraires multicartes et maintenir l'appartenance à des groupes multicast, en utilisant une approche à l'état souple. La construction de base utilisée par l'ODMRP est le groupe de transmission [CGZ98], un maillage de nœuds responsables de la transmission des paquets de données multidiffusion envoyés par la source correspondante. ODMRP inonde périodiquement les messages Join Query (JQ) pour renforcer ce groupe de redirection, en demandant aux membres multicast de répondre avec les messages Join Reply(JR), qui sont ensuite transmis par

les routeurs intermédiaires vers la source ; les routeurs intermédiaires sont ajoutés au groupe de redirection. Le processus de génération de maillage est lancé chaque fois qu'un routeur (la source) a des paquets de données à envoyer au groupe multicast, pour lequel aucun état n'est déjà établi. Il est divisé en deux phases principales :

•une phase « publicitaire » durant laquelle la source génère et inonde un paquet Join Query dans tout le réseau, annonce son adresse et la destination des paquets multidiffusion.

•une phase de « réponse », au cours de laquelle les routeurs souhaitant recevoir les packs multicast répondent avec un paquet Join Reply, qui est ensuite agrégé et réacheminé vers la source. Les routeurs intermédiaires -c.-à-d. les routeurs qui ne sont pas nécessairement abonnés à l'adresse de destination, mais qui se trouvent sur les chemins entre les récepteurs multicast et la source- sont signalés comme faisant partie du maillage multicast de cette source (ou groupe d'acheminement) et transmettra les paquets de données multicast provenant de cette source. [17]



(a) Advertising phase (b) Reply phase

FIGURE 1.10 – ODMRP opérations.

2. Le protocole CAMP

CAMP C'est un protocole de routage multicast qui construit une structure de maillage partagée pour chaque groupe multicast. Dans CAMP, un ou plusieurs nœuds jouent le rôle de noyau (ou Core), prenant ainsi en charge les opérations d'adhésion au groupe. Ils sont utilisés pour limiter le trafic de contrôle nécessaire à la jointure d'un nœud au groupe multicast. Les opérations d'inondation du réseau sont de ce fait inutiles. Lorsqu'un nœud désire joindre la session multicast, il vérifie dans un premier temps s'il y a des membres du groupe parmi ses voisins. Si c'est le cas, il les informe de sa nouvelle appartenance au groupe par l'intermédiaire

d'un message de mise à jour CAMP UPDATE. Sinon, deux possibilités s'offrent à lui il peut soit : 1) Essayer de joindre un membre du groupe par l'intermédiaire d'un mécanisme de recherche par anneaux croissants.
2) Contacter un des noyaux du groupe multicast. S'il opte pour la première solution, n'importe quel nœud membre peut répondre par un message JOIN-ACK qui est propagé jusqu'à l'initiateur de la requête.
Si la deuxième solution est choisie, le chemin pour joindre le noyau va alors être incorporé entièrement au maillage. Un nœud receveur détermine périodiquement s'il reçoit des paquets de données de la part des voisins qui sont sur le chemin inverse le plus court vers la source. Si ce n'est pas le cas, le nœud envoie un message HEART BEAT le long du chemin inverse le plus court. Ce processus permet de s'assurer que tous les chemins inverses entre les sources et les receveurs sont bien inclus dans le maillage. CAMP a l'avantage d'une part de ne pas utiliser l'inondation et d'autre part que les requêtes soient propagées uniquement en direction des membres du maillage. Cependant, il repose sur un protocole unicast sous-jacent pour garantir des distances correctes vers chaque destination en un temps fini. [18]

3. Le protocole RPL (Routing Protocol for Low power and lossy networks-LLNS) :

RPL est un protocole de routage proactif à vecteur de distance qui construit un DODAG (Destination Oriented Directe Acyclic Graph) pour l'acheminement des données vers la station de base. Le DODAG construit permet à chaque nœud du DODAG de transmettre les données qu'il a récolté jusqu'au DODAG root (racine). Chaque nœud dans le DODAG sélectionne un parent selon une métrique de routage donnée et une fonction objective. Les données récoltées sont acheminées de fils à parent jusqu'à la racine.[19] Par ailleurs, pour le bon fonctionnement du protocole RPL, chaque nœud contient la base des informations suivantes :[19]

- Un ID du nœud
- Un rang (R).
- Liste des prédécesseurs.
- Père par défaut.
- Liste des destinataires.

Le protocole RPL comporte quatre types de messages de contrôle utilisés dans la phase de découverte de routes. Ces messages sont : [19]

1. DIO
2. DAO

3. DIS

4. DAO-ACK

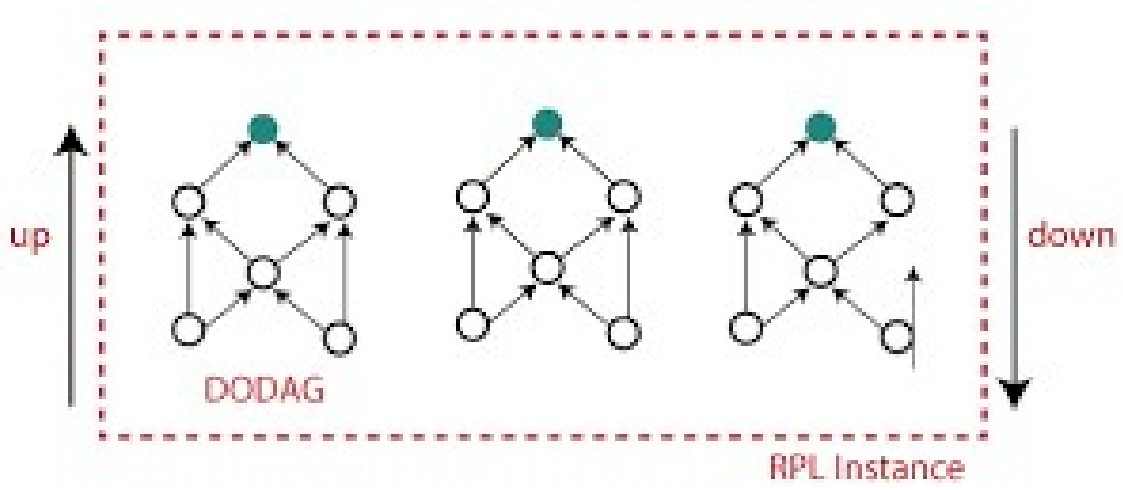


FIGURE 1.11 – Topologie RPL.

4. Le protocole COAP (Constrained Application Protocol) :

Coap est un protocole de transfert Web optimisé pour les périphériques et réseaux contraints utilisés dans les réseaux de capteurs sans fil pour former l'Internet des objets. Basé sur le style architectural REST, il permet de manipuler au travers d'un modèle d'interaction client-serveur les ressources des objets communicants et capteurs identifiées par des URI en s'appuyant sur l'échange de requêtes-réponses et méthodes similaires au protocole HTTP. L'utilisation des services web est courante sur les applications Internet. CoAP étend ce paradigme à l'Internet des objets et aux applications M2M qui peuvent ainsi êtres développées avec des services web RESTful partagés et réutilisables. Tout en prenant en compte les contraintes et besoins de l'Internet des objets tel que le support de l'asynchrone ou du multicast. CoAP est prévu pour devenir un protocole d'application omniprésent dans le futur Internet des objets . Le protocole CoAP se situe au niveau applicatif de la couche OSI et s'appuie sur UDP pour la communication. Il met en œuvre une méthode d'observation des ressources et fournit des fonctions de découverte des périphériques pour minimiser l'intervention humaine. Implémenté avec différents langages, ce protocole peut être utilisé dans des domaines tels que la santé ou la gestion énergétique.[20]

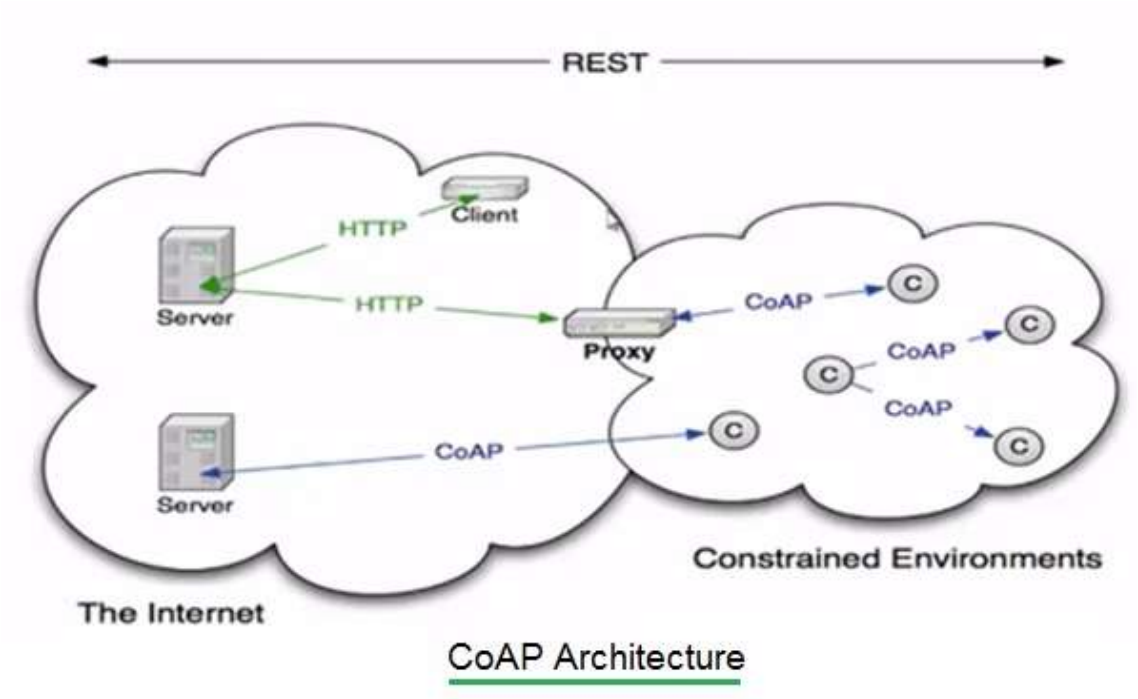


FIGURE 1.12 – Architcture de COAP.

5. Le protocole MAODV

MAODV est le protocole de multidiffusion associé au protocole de routage Ad hoc On-Demand Distance Vector (AODV), et en tant que tel, il partage de nombreuses similitudes et formats de paquets avec AODV. Les types de paquets Route Request et Route Reply sont basés sur ceux utilisés par AODV, tout comme la table de routage unicast. De même, de nombreux paramètres de configuration utilisés par MAODV sont définis par AODV. Le lecteur est renvoyé au projet Internet AODV pour les valeurs suggérées de ces paramètres, ainsi que pour les détails sur le fonctionnement en monodiffusion d'AODV. MAODV est le protocole de multidiffusion associé au protocole de routage Ad hoc On-Demand Distance Vector (AODV), et en tant que tel, il partage de nombreuses similitudes et formats de paquets avec AODV. Les types de paquets Route Request et Route Reply sont basés sur ceux utilisés par AODV, tout comme la table de routage unicast. De même, de nombreux paramètres de configuration utilisés par MAODV sont définis par AODV. Le lecteur est renvoyé au projet Internet AODV pour les valeurs suggérées de ces paramètres, ainsi que pour les détails sur le fonctionnement unicast d'AODV.[21]

1.6 Conclusion

Dans ce chapitre, nous nous consacrons à une étude sur le routage dans les réseaux MANETs (Mobile Ad Hoc Network), plus spécifiquement dans les réseaux IdOs. Nous abordons tout d'abord le routage de manière générale, en mentionnant différentes classifications de protocoles, à savoir les protocoles proactifs, réactifs et hybrides. Ensuite, nous présentons un aperçu du routage dans l'IdO, en introduisant le concept du routage Unicast et Multicast, ainsi que les protocoles adaptés à ces types de routage.

Dans cette étude, nous accordons une attention particulière au routage Multicast dans les réseaux mobiles ad hoc et son intégration dans l'internet des objets, qui constitue l'objet de notre recherche. Dans le chapitre suivant, nous décrirons en détail le protocole de routage MAODV (Multicast Ad hoc On-Demand Distance Vector), ses fonctionnalités et son utilisation dans les réseaux ad hoc mobiles,Le chapitre se termine en mettant en évidence le problème de détection des nœuds critiques (CNDP) dans le protocole MAODV.

Chapitre 2

LE PROTOCOLE DE ROUTAGE LAODV

2.1 Introduction

De nombreuses applications des réseaux mobiles ad hoc, telles que les conférences, la gestion des urgences et les opérations militaires, nécessitent un routage multicast. De plus, ces applications ont également des exigences en matière de services multimédias, tels que les appels audio et vidéo ainsi que les conférences audio et vidéo. Dans les environnements mobiles ad hoc, le protocole de routage réactif à la demande AODV est devenu le protocole par défaut, bien établi.
Le protocole MAODV est un protocole de routage largement utilisé dans les réseaux ad hoc. Il offre une solution efficace pour les communications sans fil dans des environnements où les infrastructures de réseau traditionnelles sont absentes ou limitées. Cependant, afin d'optimiser les performances de ce protocole, il est nécessaire d'utiliser des outils et des techniques adaptés. C'est là que la théorie des graphes entre en jeu.La théorie des graphes fournit les bases conceptuelles et les outils mathématiques nécessaires pour modéliser, représenter, calculer et optimiser les routes dans le protocole MAODV. Elle est essentielle pour le fonctionnement efficace du protocole et pour l'amélioration des performances globales du réseau ad hoc.

Ce chapitre est divisé en deux parties. Dans la première partie, nous allons explorer le fonctionnement de ce protocole ainsi que ses implications pour les réseaux mobiles ad hoc, dans le cadre de notre travail de recherche. Dans la deuxième partie, nous aborderons le problème de détection des nœuds critiques (CNDP) dans le protocole MAODV.

2.2 Présentation du protocole MAODV :

2.2.1 Définition du protocole MAODV :

AOMDV (Ad hoc on Demand Multipath Distance Vector) est un protocole de routage réactif multi chemin. Il s'agit d'une extension d'AODV et fournit également deux services principaux, à savoir la découverte et la maintenance des routes.
MAODV est un protocole de routage à la demande qui découvre une route lorsqu'une source doit communiquer avec une destination.
Le protocole de routage multi-chemin construit plusieurs chemins disjoints sans boucle de routage allant de la source vers la destination mais il n'utilise que le meilleur chemin en terme de nombre de saut comme chemin primaire pour transfère les données. Ces chemins multiples peuvent être utilisés pour la répartition de la charge ou comme routes de secours lorsque la

route principale échoue .[6]

2.2.2 Fonctionnement du protocole MAODV :

MAODV et fonctionne de manière réactive, à la demande. Il utilise le même principe qu'AODV, et les mêmes formats de requêtes de recherche de routes. Dans AODV, les tables de routage de chaque nœud sont mises à jour lorsque ceux-ci désirent connaitre le chemin vers une destination non répertoriée (ou pour laquelle l'information correspondante est périmée) ou lorsqu'ils participent à une recherche de route lancée par un autre nœud. Le protocole MAODV construit un arbre partagé centré sur un noyau (le leader du groupe) pour chaque groupe multicast du réseau. Le nœud leader est le premier participant au groupe, il est chargé de le gérer et de le maintenir en place. L'arbre peut contenir des nœuds qui ne font pas partie du groupe. Un numéro de séquence est associé à chaque groupe.

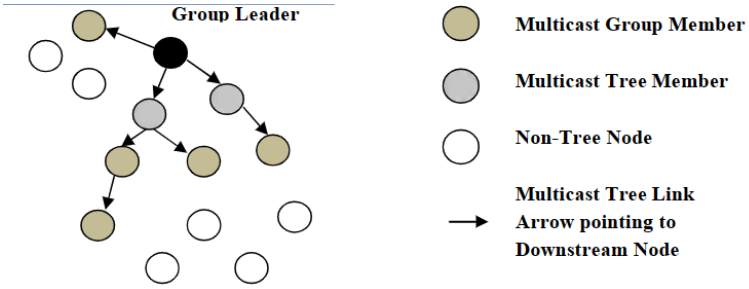


FIGURE 2.1 – Arbre partagé.

Un nœud MAODV maintient une table de routage comme dans AODV pour le routage unicast (l'algorithme AODV maintient une table sur chaque nœud, indexée par destination et notamment le voisin auquel envoyer le paquet pour atteindre cette destination. Si la destination recherchée n'est pas dans la table, on doit donc découvrir une route jusqu'au destinataire. L'algorithme agit à la demande : recherche d'une route uniquement lorsque c'est nécessaire), mais aussi une table de routage pour la structure en arbre du groupe . [22]

1. Table de routage :

La découverte de route trouve une route vers une destination en inondant les paquets de requête sur tout le réseau. La maintenance des routes permet de détecter et de signaler les interruptions de route pouvant être causées par le mouvement des nœuds. AODV n'utilise pas de mises à jour périodiques, les routes sont découvertes et maintenues au besoin.

Chaque nœud intermédiaire de la route entre le nœud source et le nœud de destination doit maintenir une table de routage contenant :

- L'adresse IP de la destination.
- Next Hop : Adresse IP du prochain nœud en direction de la destination (Le nœud suivant).
- Hop count : Le nombre de saut nécessaire pour atteindre la destination.
- La distance en nombre de nœud (le nombre de nœud nécessaire pour atteindre la destination).
- Le numéro de séquence destination : Il permet de distinguer les nouvelles routes des anciennes.
- Le temps d'expiration de l'entrée de la table : C'est le temps au bout du quel l'entrée est valide.

Une entrée de la table est mise à jour lorsque le nœud reçoit un message contenant :

- un numéro de séquence plus élevé pour la destination.
- le même numéro de séquence mais un Hop Count plus petit.
- le même numéro de séquence mais que la route avait été marquée comme invalide ou en cours de réparation. [23]

La mise à jour de ces tables s'effectue par l'échange de trois types de messages entre les nœuds : RREQ, RREP, RRER.

2. Types des messages MAODV :

Il se compose de 3 types de messages de routage comme suit :

— RREQ " Route Request Message" :
les nœuds voisins par une une nœud source désirant envoyer des paquets de données vers un nœud destinataire. [4]

Source Address	Source Sequence Number	Broadcast_ id	Destination Address	Destination Sequences Number	Hop_ Count

TABLE 2.1 – format général d'une route réquest.[1]

— RREP “ Route Reply Message” :

lorsque la destination reçoit le RREQ, elle répondra par un RREP comme accusé de réception. Ce paquet permet de confirmer le chemin par le quel le paquet RREQ a été reçu. [5]

Source Address	Destination Address	Destination Sequences Number	Hop_ Count	Life_Time

TABLE 2.2 – format général d’une route reply.[24]

— RERR “Route Error Message” :

paquet envoyé par un nœud lorsque la liaison avec son voisin est rompue (chemin invalide).[5]

3. La Découverte de route :

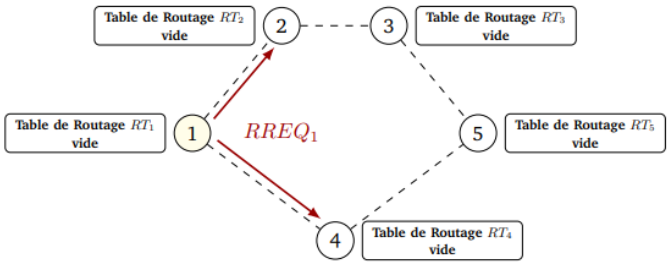
L’idée principale dans MAODV consiste à calculer différentes routes, allant de la source de trafic jusqu’à la destination, tout en évitant la formation de boucles de routage. Au début de la procédure, la source envoie le message de demande de route RREQ à ses nœuds voisins. Les nœuds voisins reçoivent le RREQ et envoient à leur tour un RREQ à leurs nœuds voisins. Cette opération est répétée jusqu’à ce que le nœud destination reçoive la demande de route. Ce dernier génère une réponse de route RREP pour chaque RREQ reçu. Le nœud source reçoit plusieurs RREPs correspondants aux chemins découverts, Si un seul RREP est reçu donc une seule route est reconnue entre la source et la destination, alors elle envoie les paquets de données sur cette route, Sinon, si plusieurs RREP ont été reçu, la source choisit la meilleure route c’est-à-dire celle ayant le plus petit nombre de saut «hop_count».

Les autres routes restent en attente de l’arrivé d’un paquet RERR indiquant la rupture de la route principale, dans ce cas la meilleure route parmi les routes alternatives est sélectionnée pour retransmettre les données. Si aucun RREP n’est reçu, une nouvelle phase de découverte de route est déclenchée .[6]

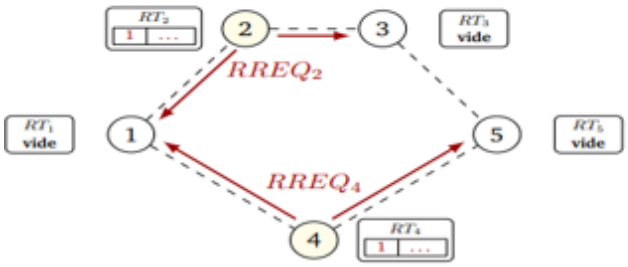
4. Maintenance des routes :

Afin de maintenir les routes, une transmission de messages HELLO est effectuée. Ces messages sont en fait des réponses de route (RREP) diffusés aux voisins avec un nombre de sauts

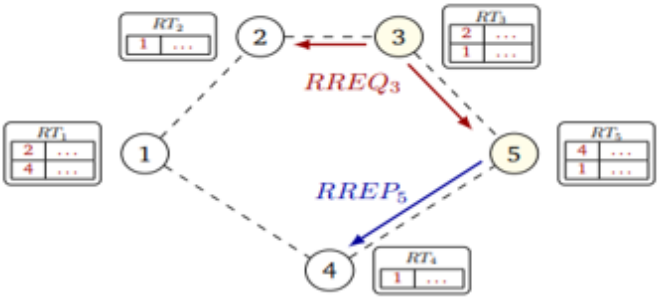
égal à un. Si au bout d'un certain temps, aucun message n'est reçu d'un nœud voisin, le lien en question est considéré défaillant. Alors, un message d'erreur RERR (Route ERRor) se propage vers la source et tous les nœuds intermédiaires vont marquer la route comme invalide et au bout d'un certain temps, l'entrée correspondante est effacée de leur table de routage. Le message d'erreur RERR peut être diffusé ou envoyé en unicast en fonction du nombre de nœuds à avertir de la rupture de liaison détectée. Ainsi, s'il y en a un seul, le message est envoyé en unicast sinon, il est diffusé.[25]



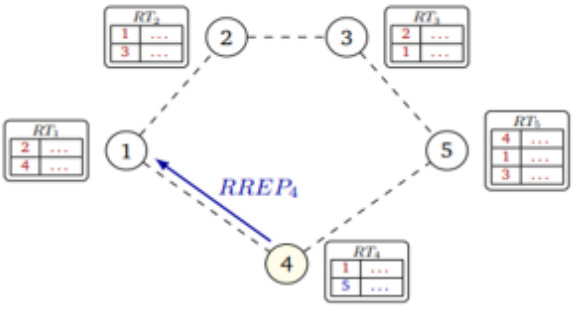
a Le nœud 1 initialise une demande de route pour obtenir un chemin vers 5.



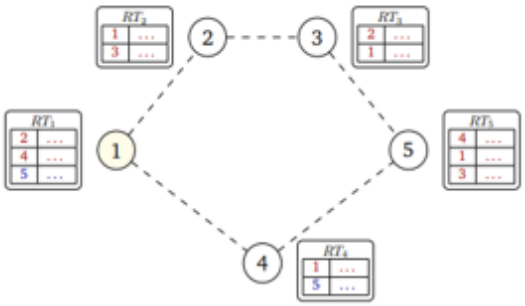
b. 2 et 4 retransmettent la demande de route



c. 5 initialise une réponse de route



d. 4 retransmit la réponse de route



e. Arrivée de la réponse de route à la source 1

FIGURE 2.2 – Exemple d'établissement de route entre 1 et 5.

2.2.3 Les avantages et les inconvénients du MAODV :

1. **Les avantages :**

   — MAODV est sans boucle car les boucles sont surmontées en utilisant le numéro de séquence.

   — Réduisez le temps de découverte de route et limitez les messages de contrôle dans la découverte de route.

2. **Les inconvénients :**

   — MAODV a plus de frais généraux de message lors de la découverte de route en raison d'une inondation accrue et comme il s'agit d'un protocole de routage multi-chemins, la destination répond aux multiples RREQ, ces résultats sont plus longs.

   — Un encombrement peut survenir en raison d'un plus grand nombre de messages RREQ et RREP.[26]

2.2.4 Les Metriques de routage :

De nombreux protocoles de routage utilisent des métriques pour déterminer le plus "court"chemin à partir d'une source vers une destination. Une métrique est une valeur numérique associéeà chaque lien. Le plus "court"chemin représente le minimal coût de ce chemin vis-à-vis de cettemétrique. Elle doit garantir l'isotonicité . La métrique reflète généralement le coût d'utilisation d'une route particulière par rapport à un objectif d'optimisation . Le tableau 2.3 présente quelques objectifs d'optimisation d'un algorithme de calcul de route ainsi que celui de la métrique de routage. [26]

Maximiser la probabilité de transmission des données : minimiser le taux depertes des données dans les réseau.
Minimiser le délai : sélectionner le chemin assurant un délai minimum
Maximiser le débit d'un chemin : sélectionner un chemin de bout-en-bout composéde liens de grande capacité.
Répartir équitablement la charge de trafic :équilibrer la charge de trafic de sortequ'aucun nœud (ou lien) ne soit disproportionnellement utilisé.

TABLE 2.3 – Objectifs d'optimisation d'une métrique de routage.

2.2.5 Métrique basée sur la topologie du réseau :

Dans cette technique, les métriques considèrent les informations liées à la topologie du réseau, en particulier le nombre de voisins pour chaque nœud et le nombre de sauts pour atteindre une destination particulière. Ces métriques utilisent juste les informations de connectivité entre les nœuds sans prendre en compte d'informations sur la qualité de la liaison reflétant les performances du réseau, tel que le débit, le taux de pertes ou le délai. L'exemple le plus connu de ces métriques est la métrique Hop Count. [26]

1. La métrique Hop Count :

   la métrique Hop Count (nombre de saut) est la plus couramment utilisée dans les protocoles de routage existants. Hop Count indique seulement l'existence d'un lien entre deux nœuds. Elle est égale à 1 si le lien existe, et + si le lien n'existe pas. Elle est simple à calculer et elle évite toute charge de calcul supplémentaire pour le protocole de routage.[26]

   La figure 2.3 illustre un exemple simple d'une topologie de réseau ad hoc. La métrique Hop Count choisit le chemin avec le nombre minimum de sauts de la source A pour atteindre la destination E. Le tableau 2.4 montre le chemin approprié et le nombre de sauts nécessaires pour la communication de la source A avec le reste des nœuds du réseau, en appliquant la métrique Hop Count. La route sélectionnée par Hop Count de la source A vers la destination E est la route directe A $\rightarrow$ E car E est un voisin direct de A. [26]

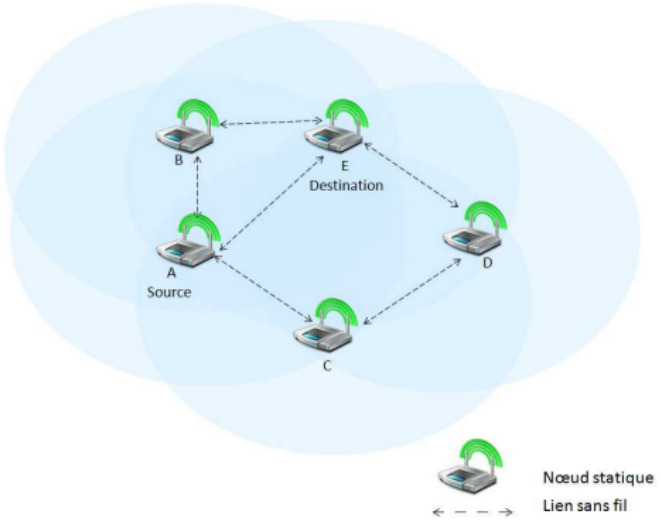


FIGURE 2.3 – Exemple de topologie de réseaux ad hoc.

Noeud	Route	Nombre de saut
B	A → B	1
C	A → C	1
D	A → C → D ou A → E → D	2
E	A → E	1

TABLE 2.4 – Table de routage du nœud A avec la métrique Hop Count [3]

2.2.6 Métriques de la qualité de lien :

Pour améliorer le routage, d'autres paramétres de qualité de lien ont été considérés pour trouver une meilleure route, tels que le taux de pertes , la bande passante ou le délai d'un chemin.[26]

1. La métrique ETX :

   La metrique Expected Transmission Count (ETX) est défini comme le nombre prévu de transmissions de couche MAC qui est nécessaire pour réussir la livraison d'un paquet via une liaison sans fil. Le poids d'un chemin est défini comme la somme des ETX de tous les liens le long du chemin. Étant donné que les chemins longs et les chemins avec perte ont de gros poids sous ETX, la métrique ETX capture les effets des rapports de perte de paquets et de la longueur de chemin.

   De plus, ETX est également une métrique de routage isotonique, qui garantit un calcul facile des chemins de poids minimum et du routage sans boucle dans tous les protocoles de routage. Toutefois, les inconvénients d'ETX sont qu'elle ne tient pas compte du brouillage

ou du fait que différentes liaisons peuvent avoir des débits de transmission différents.[27]

2. La métrique ETT :

   La métrique Expected Transmission Time (ETT) a été proposée pour prendre en consideration les liens avec différentes capacités dans un réseau. Le calcul d'ETT est basé sur la metrique ETX mais ETT prend en compte à la fois la taille des paquets de données.[26]

2.2.7 Métriques de charge du trafic :

Ces métriques choisissent les meilleures routes en fonction de l'estimation de la charge du trafic des nœuds formant le chemin, tandis que les métriques de qualité de lien choisissent leurs routes en fonction de la qualité des liens des routes. [26]

1. La métrique EAB :

   La métrique Expected Available Bandwidth (EAB) a été proposée pour résoudre le problème des zones de concentration de trafic du réseau, en assurant un débit élevé et un faible délai moyen de bout-en-bout. EAB prend en compte la bande passante disponible et le taux de transmission réussie. La bande passante disponible est calculée comme estimation de la bande passante totale moins la largeur de la bande passante occupée par chaque lien sur un nœud Si un lien a beaucoup de bande passante disponible, un nœud peut transmettre plus de quantité de données via ce lien. Cette métrique choisit un chemin qui a un faible délai de bout-en-bout et un taux de livraison élevé.[26]

2. La métrique MF-Transmission Failure :

   Cette métrique est définie dans le but de prendre en compte les échecs de transmission en considérant le mécanisme de backoff utilisé dans les réseaux en attribuant des coefficients à chaque chemin. Ces coefficients agissent comme métrique pour sélectionner une route entre différents chemins et pour assurer aussi l'équilibrage de charge. Par conséquent, cette métrique aide les protocoles de routage à équilibrer le trafic et à éviter le trafic à travers les chemins congestionnés.[26]

2.2.8 Les métriques muti-canaux :

Les nœuds multicanaux sont prometteurs pour une capacite accrue ce type de réseau. Il est important de préciser que le terme multicanal fait référence à l'utilisation de plusieurs canaux ou frequences. Avec le réseau multicanal, un nœud peut envoyer et recevoir des données en même temps et les nœuds peuvent transmettre sur les deux canaux simultanément. Parmi les

métriques multicanaux :

- La métrique WCETT.
- La métrique MIC.
- La métrique MCR.
- La métrique iAWARE .
- Les métriques mETX ENT.
- La métrique DBETX.
- Les métriques BATD iBATD .

Nous en décrivons deux.[26]

1. La métrique WCETT (Weighted Cumulative ETT) :

   WCETT est une extension de la métrique ETT, Le but de WCETT est de réduire l'interférence en minimisant le nombre de nœuds qui utilisent le même canal sur le chemin total. Ainsi la diversité des canaux utilisés entrainera une réduction au niveau de interférence.[28]

2. La métrique iAWARE :

   La métrique interference AWARE (iAWARE) estime le temps moyen pendant lequel le médium physique est occupé par la transmission de chaque voisin interférant. Cette métrique prend en compte les interférences inter-flow et intra-flow, mais aussi elle est caractérisée par un modèle physique d'interférence et elle considére aussi la variation de la qualité du lien. Afin de reproduire les variations des interférences entre les voisins, le calcul de iAWARE se base sur le rapport signal à bruit (Signal to Noise Ratio : SNR) et le rapport signal à bruit et interférence (Signal to Interference and Noise Ratio : SINR). [26]

2.2.9 Métriques sensibles à la mobilité :

Les métriques basées sur la technique de sondage telles que ETX et ses dérivées sont plus efficaces pour les réseaux statiques que la métrique Hop Count. Les métriques de mobilité visent à adapter les routes en temps réel malgré changements fréquents des nœuds. Une large catégorie des métriques utilisent des mesures de la puissance du signal et leurs taux de variation afin de déduire la stabilité des liens et des routes.[26] Parmis les métriques sensibles a la mobolité sont :

• Les métriques Link Associativity Ticks Path Average degree of association stability.

• Les métriques Link Affinity Path Stability.

• Les métriques Link Availibity Path Availability.

• La métrique LD.

• La métrique Link Change Rate, Link State Changes λ lc.

• La métrique Link Stability Ls.

Nous allons detailler deux métriques :

1. Les métriques Link Associativity Ticks Path Average degree of association stability :
   Les nœuds mobiles transmettent des balises (beacon) de la couche liaison à des intervalles de temps fixe (une seconde comme valeur par défaut). Chaque nœud mesure le nombre reçu des sondes (probe) (associativity ticks) de leurs voisins. Les valeurs mesurées donnent une indication sur la stabilité réelle de la liaison. Si les nœuds mobiles sont dans un état de forte mobilité, alors les valeurs d'associativity tick sont faibles. Par contre, si le nœud mobile est plus stable, alors les valeurs d'associativity tick sont élevées, Cette métrique prend comme hypothèse le fait que les nœuds alternent entre des périodes de transition/migration et veille (idleness).[29]
2. la métrique Link Duration (LD) :
   La métrique Link Duration c'est la durée moyenne du lien existant entre deux nœuds i et j a l'instant t. C'est une mesure de la stabilité du lien entre ces nœuds.[?ref30] Cette métrique est calculée en mesurant la durée de vie d'une liaison entre deux nœuds m et n à l'instant t1. Pour chaque lien existant, elle donne le temps à partir de la détection de la liaison. Tant que les deux nœuds m et n sont à portée radio l'un de l'autre, alors LD augmente.[26]

2.2.10 Vecteur de Distance :

Dans les protocoles à vecteur de distances, la table de routage d'un nœud est calculée en fonction des tables reçues par ses voisins, comme son nom l'indique, ce protocole fonctionne selon une notion de distance. Chaque nœud enregistre dans sa table de routage les next hops et les distances nécessaires pour atteindre toutes les destinations du réseau. Selon le protocole, cette distance peut être le nombre de hop, la bande passante, etc. À chaque modification de sa table de routage, le nœud broadcaste celle-ci. Cette table peut être modifiée lorsqu'une autre table a été reçue d'un voisin, ou lorsque le nœud a détecté un changement de topologie dans son voisinage. Lorsqu'un nœud reçoit une table de routage d'un de ses voisins, il recalcule les routes les plus courtes pour chaque destination. Ces calculs sont effectués via l'équation de Bellman

Ford. Les vecteurs de distances sont des messages utilisés pour distribuer les informations à propos du réseau. À la création du réseau, chaque nœud crée une table de routage contenant son propre identifiant comme destination et next hop et un coût associé nul. À intervalles réguliers, chaque nœud envoie sa table de routage à ses voisins via des vecteurs de distances. Le nom de ces messages est issu du fait qu'ils peuvent être vus comme des vecteurs où la direction est le voisin à contacter et la distance est le nombre de hops à effectuer pour atteindre la destination. Lorsqu'un nœud réceptionne un tel message, il utilise l'équation de Bellman-Ford pour déterminer si la table de routage actuelle doit être mise à jour avec celle reçue de son voisin. Si la table est mise à jour, le nœud envoie sa nouvelle table à ses voisins. Ce processus continue 14 tant que des mises à jour sont à réaliser par les nœuds. Une fois que tous les nœuds ont obtenu les informations sur les meilleures routes, le réseau est stabilisé. Si un nœud détecte un changement de topologie, c'est-à-dire que l'un de ses voisins n'est plus accessible, le nœud indique son voisin comme inaccessible dans sa table de routage, partage celle-ci à son voisinage et l'information est transmise sur l'ensemble du réseau.[31]

2.3 Notions de la theorie des graphes pour l'amelioration du maodv

Plusieurs mécanismes et fonctions dans les réseaux, tel que la propagation et la synchronisation sont influencées par un sous ensemble de nœuds qui sont généralement qualifiés de nœuds Importants, tout dépend de leurs rôles dans le réseau. Identifier les nœuds importants d'un réseau permet de bien comprendre leurs propriétés structurelles et fonctionnelles. D'un point de vu connexité, les nœuds importants sont ceux qui maintiennent la connectivité du réseau, et ainsi leur suppression déconnecte le réseau. Ces nœuds sont connus dans la littérature par les « nœuds critiques », et le problème qui les étudie est le « Problème de détection de nœuds critiques dans les réseaux ».

2.3.1 Problème de détection de nœuds critiques (CNDP) :

Le problème de détection de nœuds critiques est un problème d'identification des nœuds importants dans un graphe dont l'élimination diminue la performance du réseau dans une large mesure. Cette importance dépend du rôle principal d'un nœud et pas seulement de sa position dans le réseau. Selon les mesures de connectivité à vérifier, il existe plusieurs variantes de CNP, et l'optimisation de la suppression des nœuds pour chacune d'entre elles peut donner

des solutions optimales différentes pour le même graphe. [32] Dans cette section, nous allons présenter les différentes variantes du CNDP, en mettant en avant celles qui ont été classées parmi les meilleures approches fondamentales pour résoudre ce problème.

2.3.2 Le nœud critique ?

Dans un réseau, un nœud critique est celui qui maintient la cohérence du réseau et dont la suppression dégradera sa connectivité .[23]

2.3.3 Différentes variantes de CNDP :

Dans le cas général, CNDP cherche un ensemble de nœuds dans un graphe dont la suppression minimise ou maximise une métrique prédéfinie. Donc, on a en entrée un graphe G = (V ; E) et une métrique de connectivité nommée δ, et on sortie un ensemble de nœuds $S \subseteq V$ tel que $G[V \setminus S]$ optimise la métrique δ. Généralement, on a deux cas :

- Optimiser la métrique δ de telle sorte que le nombre des nœuds à supprimer ne dépasse pas nœuds K ($|S| \leq K$).
- Minimiser le nombre de nœuds à supprimer, de telle sorte que la métrique δ soit bornée par une borne donnée β.

La classe des variantes du premier cas est applicable quand nous avons des informations sur le nombre de nœuds à identifier mais nous ne savons pas le moyen d'atteindre notre objectif de façon optimale. Ceci est le cas de, par exemple, la destruction d'une organisation terroriste, nous essayons de neutraliser la communication entre ses membres en éliminant certains d'entre eux, et en raison des ressources limitées, nous ne pouvons neutraliser K que membre tout en maximisant la fragmentation du réseau de communication en utilisant les ressources possibles afin d'atteindre notre objectif. Cependant, si nous cherchons à neutraliser totalement le réseau terroriste, et nous savons qu'au moins t personnes doivent communiquer pour prendre une décision, donc pour atteindre notre objectif, nous essayons d'éliminer un sous ensemble de nœuds tels que le réseau devient composé de sous ensembles d'au maximum t-1 membres. Dans un tel cas, nous ne savons pas le nombre de nœuds à cibler, mais nous avons des informations sur la structure du réseau que nous devions obtenir, ainsi c'est dans une telle situation que les variantes du deuxième cas sont applicable. On note que la métrique δ sert à décrire comment la structure du réseau doit être déconnectée après la suppression de nœuds critiques. [33] Dans la suite de cette section, nous allons examiner en détail chacune des variantes qui ont été présentées dans la littérature :

1. CNP : Critical Node Problem

Dans cette variante, la métrique considérée est la minimisation de la connectivité par paires dans le réseau. Donc, on cherche à trouver un ensemble $S \subseteq V$ d'au maximum k nœud, dont la suppression minimise la connectivité par paires dans le graphe induit $G[V \setminus S]$. L'utilisation de cette métrique permet de, simultanément, maximiser le nombre de composantes connexes et de minimiser la variance de cardinalité entre les différentes composantes dans $G[V \setminus S]$. Ceci peut être formulé en utilisant la fonction suivante :

$$\mathrm{F(S)} = \sum_{C_i \in G[V \setminus S]} \left(\frac{\delta_i(\delta_i - 1)}{2} \right)$$

est l'ensemble de toutes les composantes connexes dans $G[V \setminus S]$ après la suppression des k nœuds, et δ_i représente la taille de la composante C_i. Ainsi, la version décisionnelle de CNP est [33] :

Entrée : un graphe non orienté G (V ;E) et un entier K .

Sortie : F(S)= $\arg\min_{S \subseteq V} \sum_{c_i \in G(V \setminus S)} \frac{\delta_i(\delta_i - 1)}{2} ou |S| \leq K$

Exemple :

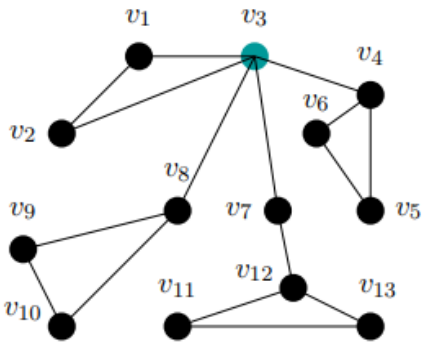


FIGURE 2.4 – Exemple de graphe.[32]

disons que v3 est le nœud choisi pour être supprimé, dans ce cas nous nous retrouverons avec :

Nombre de composants : 4

- Le composant 1 contient les nœuds : v1 , v2 .
- Le composant 2 contient les nœuds : v4, v5, v6 .
- Le composant 3 contient les nœuds : v8, v9, v10 .

• Le composant 4 contient les nœuds : v7, v11, v12, v13.

La fonction est calculée comme suit : $F(S) = \sum \frac{\delta_i(\delta_i-1)}{2} = \frac{2(2-1)}{2} + \frac{3(3-1)}{2} + \frac{3(3-1)}{2} + \frac{4(4-1)}{2} = 13.$

le résultat :

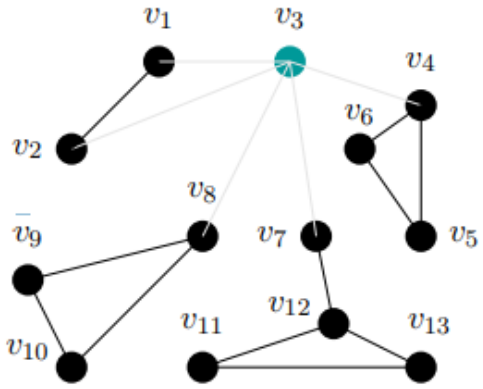


FIGURE 2.5 – Exemple de graphe.

La solution optimale pour le CNP est que lorsque la fonction objectif mentionnée précédemment est minimisée à la valeur 0, cela donne un graphe résiduel avec n - k seuls nœuds isolés après suppression des k nœuds critiques.

Cela équivaut à trouver un ensemble de couverture de sommets avec au plus k nœuds, ou un ensemble indépendant avec au moins n - k nœuds. Alors, résoudre CNP, dans ce cas, équivaut à trouver la couverture de sommets minimale dans le graphe.[32]

2. 3C-CNP : Component Cardinality Constraint CNP

3C-CNP cherche à minimiser l'ensemble de nœuds à supprimer tout en limitant la taille de chaque composante connexe dans le graphe induit à une borne donnée β. Sa formulation peut être énoncée comme suit :[33]

Entrée : un graphe G (V ; E) non orienté avec un entier β.

Sortie : Un ensemble minimal de nœuds $S \subseteq V$ ou $\delta_n \leq \beta$ pour toute composante $h \in G(V \setminus S)$.

2.4 Conclusion

Dans ce chapitre, nous avons abordé le protocole de routage MAODV de manière générale dans les MANETs. Nous avons discuté de son principe de fonctionnement, sa topologie, son mécanisme ainsi que le fonctionnement de son mecanisme de maintenance. Ensuite, nous avons défini la notion de métrique de routage dans les réseaux ad hoc. Nous avons identifié six catégories de métriques : basées sur la topologie du réseau, basées sur la mesure de la puissance du signal pour refléter la qualité de la liaison, d'équilibrage de la charge de trafic, multi-canaux et sensibles à la mobilité. Par la suite, nous avons présenté la méthode du vecteur de distance. Enfin, nous avons abordé le problème de détection des nœuds critiques ainsi que ses variantes, CNP (Cluster-based Network Protocol) et 3CNP (Three-level Clustering Network Protocol). Dans le chapitre suivant, nous allons detailer notre proposition et présenterons les outils de simulation couramment utilisés pour évaluer les performances des protocoles de routage dans les réseaux ad hoc. Nous examinerons également les résultats de la simulation et effectuerons une comparaison entre le protocole de routage amélioré utilisant la théorie des graphes et le protocole originale.

Chapitre 3

SIMULATION DU PROTOCOLE MAODV ET L'APPROCHE PROPOSÉ DANS LES IOT

3.1 Introduction

Le problème de détection de nœud critique (Critical Node Detection Problem) dans le protocole MAODV fait référence à l'identification des nœuds essentiels ou critiques dans le réseau ad hoc. Les nœuds critiques sont des nœuds dont la défaillance ou la compromission peut avoir un impact significatif sur le bon fonctionnement du réseau. Dans le contexte du protocole MAODV, la détection de nœuds critiques est importante pour plusieurs raisons. Tout d'abord, elle permet d'identifier les nœuds dont la perte peut entraîner une dégradation du routage ou une fragmentation du réseau. De plus, cela peut aider à la conception de mécanismes de protection ou de récupération pour ces nœuds critiques, améliorant ainsi la résilience du réseau ad hoc.

Il est important de souligner que la détection de nœuds critiques est un domaine de recherche en évolution constante, avec plusieurs approches et techniques proposées dans la littérature. Dans ce contexte, deux approches couramment utilisées sont le CNP (Critical Node Problem) et le 3C-CNP (3C Critical Node Problem).Ces approches peuvent être appliquées pour détecter les nœuds critiques dans le protocole MAODV et permettre une meilleure gestion et protection du réseau ad hoc.

3.2 Outils de simulation et d'étude :

Simuler, c'est modéliser un système complexe, afin de prévoir son comportement dans le-monde réel. Il s'agit d'une approche permettant de représenter le fonctionnement d'un système-réel constitué de plusieurs entités, de modéliser les différentes interactions entre elles, et enfin évaluer le comportement global du système et son évolution dans le temps. Le recours à la simulation permet de contourner les limites de la complexité des modèles analytiques. Toutefois, il est nécessaire de bien identifier les caractéristiques du système afin de le représenter, le plus finement possible, par des modèles abstraits.[2]

3.2.1 Présentation du NS2 (Network simulator 2) :

NS est un outil logiciel de simulation de réseaux informatiques. Il est essentiellement élaboré avec les idées de la conception par objets, de la réutilisation du code et de modularité. Il est aujourd'hui un standard de référence en ce domaine, plusieurs laboratoires de recherche recommandent son utilisation pour tester les nouveaux protocoles.[2] Le simulateur NS2 actuel est particulièrement bien adapté aux réseaux à commutation de paquets et à la réalisation de simulations de grande taille .NS2 est écrit en C++ et utilise le langage OTCL (Object Tools Command Language) dérivé de TCL. A travers OTCL, l'utilisateur décrit les conditions de la simulation : la topologie du réseau, les caractéristiques des liens physiques, les protocoles utilisés, les communications qui ont lieu. La simulation doit d'abord être saisie sous forme de fichier que NS va utiliser pour produire un fichier contenant les résultats. Mais l'utilisation de l'OTCL permet aussi à l'utilisateur de créer ses propres procédures (par exemple s'il souhaite enregistrer dans un fichier l'évolution d'une variable caractéristique du réseau au cours du temps). Il contient les fonctionnalités nécessaires à l'étude des algorithmes de routage unicast ou multicast, des protocoles de transport, de session, de réservation, des services intégrés, des protocoles d'application comme FTP. A titre d'exemple la liste des principaux composants actuellement disponibles dans NS par catégorie est :

•application : Web, ftp, Telnet, générateur de trafic (CBR...).

•transport : TCP, UDP, RTP, SRM.

•routage unicast : Statique, dynamique (vecteur distance).

•routage multicast : DVMRP, PIM.

•gestion de file d'attente : RED, DropTail, Token bucket.[2]

3.2.2 Les Outils utilisés par NS2 :

NS-2 met à disposition divers outils cruciaux pour satisfaire les exigences de simulation, tels que :

NAM (Network Animator) :

NAM est un outil de visualisation qui présente deux intérêts principaux : représenter la topologie d'un réseau décrit avec NS-2, et afficher temporellement les résultats d'une trace d'exécution NS-2. Par exemple, il est capable de représenter des paquets TCP ou UDP, la rupture d'un lien entre nœuds, ou encore de représenter les paquets rejetés d'une file d'attente pleine. Ce logiciel est souvent appelé directement depuis les scripts TCL pour NS-2, pour visualiser directement le résultat de la simulation.[2]

Xwin server :

facilite la représentation graphique des résultats d'une simulation en affichant des courbes.

3.3 Proposition :

Ce mémoire se propose d'apporter des améliorations aux performances du protocole de routage MAODV, en se concentrant spécifiquement sur les nœuds critiques. Dans cette étude, nous avons exploré l'utilisation des algorithmes CNP et 3C-CNP pour améliorer le fonctionnement de MAODV.
La topologie du réseau est représentée sous forme de graphe, qui est ensuite utilisé en tant qu'entrée pour l'algorithme CNP (Conservative Network Partitioning). L'algorithme CNP identifie les nœuds critiques dans le graphe, qui sont des points clés du réseau.
Les nœuds critiques identifiés par CNP sont ensuite utilisés comme entrée pour le protocole MAODV amélioré. MAODV, basé sur les nœuds critiques, génère de nouveaux chemins de routage améliorés pour les communications dans le réseau. La sortie du protocole MAODV amélioré est donc constituée de ces nouveaux chemins de routage, qui sont améliorés en fonction des nœuds critiques. Ces chemins de routage améliorés permettent d'acheminer efficacement les données dans le réseau, en tenant compte des caractéristiques spécifiques des nœuds critiques.

Ainsi, le processus complet commence par la topologie représentée sous forme de graphe, qui est utilisée comme entrée pour CNP pour identifier les nœuds critiques. Les nœuds critiques

identifiés sont ensuite utilisés comme entrée pour MAODV amélioré, qui génère des chemins de routage améliorés. Ces nouveaux chemins de routage améliorés constituent la sortie du protocole MAODV amélioré, permettant une meilleure performance du réseau en prenant en compte les nœuds critiques.

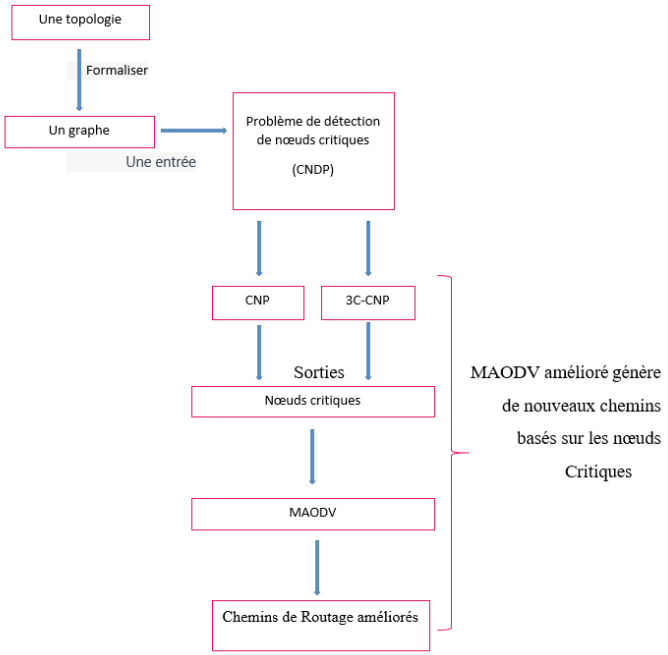


FIGURE 3.1 – Schéma de proposition.

Par la suite, nous avons réalisé une comparaison détaillée entre MAODV original, MAODV améliorée avec CNP, et MAODV améliorée avec 3C-CNP, afin d'évaluer les gains potentiels de ces améliorations. Les résultats obtenus offrent des perspectives prometteuses pour améliorer les performances du protocole de routage MAODV dans des environnements critiques.

3.3.1 Critères d'évaluation :

- **Overhead** : est le paquet total envoyé (paquet de contrôle + données paquet) divisé par les paquets de données reçus.[35]
- **pdr :** défini par le nombre moyen de données paquets livrés au groupe de multidiffusion sur le nombre de paquets de données censés être livrés à destination par session .[36]
- **Delay :**C'est le rapport de la différence de temps entre le nombre de paquets envoyés et reçus sur le temps total nécessaire pour atteindre la destination. Si le retard diminue, les performances du réseau donnent une meilleure sortie.[37]
- **Drope :**C'est le nombre de paquets non reçus dans la destination qui est le taux d'aban-

don de paquets.[37]

3.3.2 Les résultats de simulation :

— **Overhead :**

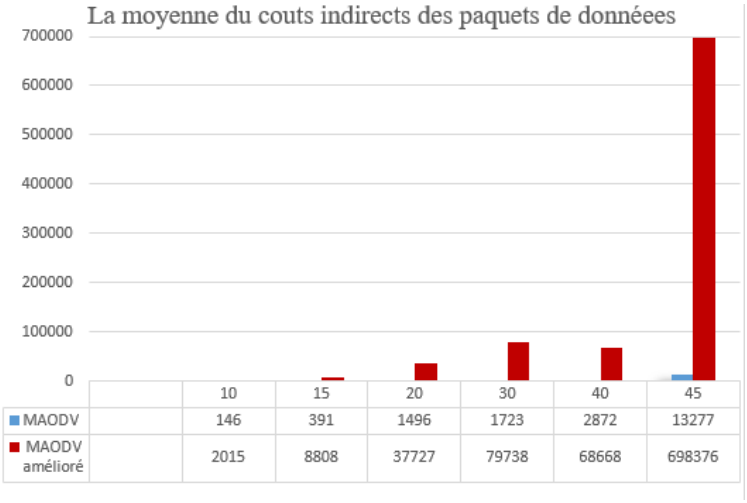


FIGURE 3.2 – Le routage dans les réseaux ad hoc.

— **Pdr :**

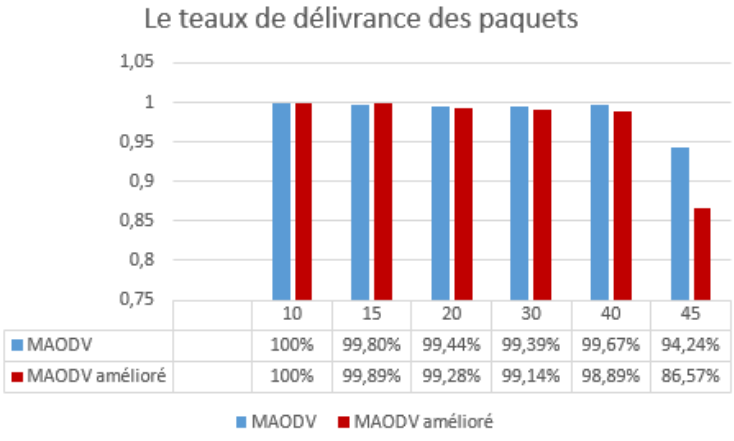


FIGURE 3.3 – Le routage dans les réseaux ad hoc.

— **Delay :**

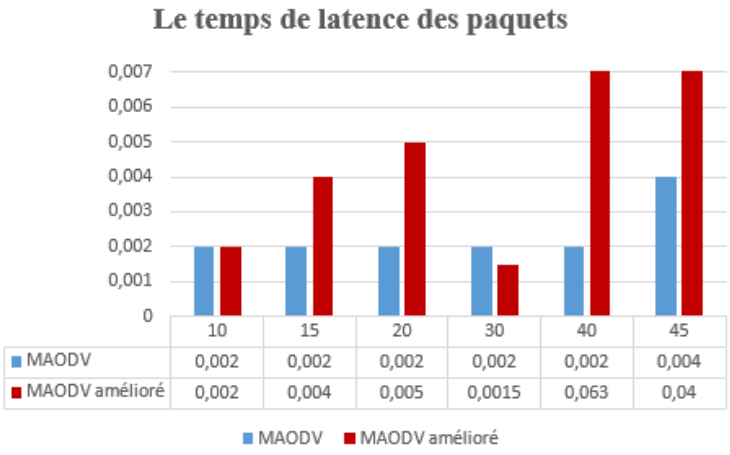


FIGURE 3.4 – Le temps de latence des paquets.

— **Drope :**

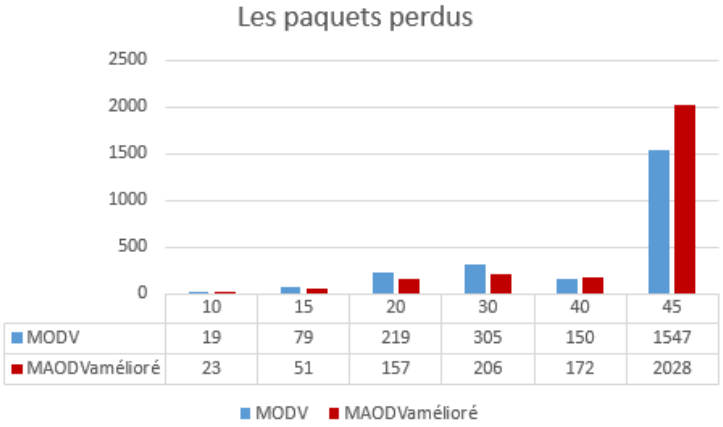


FIGURE 3.5 – Les paquets perdus.

3.4 Conclusion :

Le principal objectif de ce chapitre était de présenter notre proposition concernant les nœuds critiques dans le protocole de routage MAODV, dans le but d'améliorer la fiabilité et renforcer le réseau.

Conclusion génerale

Dans le cadre de ce mémoire, nous n'avons pas rencontré de problèmes majeurs avec le protocole de routage dans les réseaux IdOs. Cependant, il est essentiel de prendre en compte les exigences spécifiques de ces réseaux, ce qui représente un défi pour la communauté scientifique. Parmi ces défis, on trouve la mobilité constante des nœuds et les contraintes de mémoire de stockage limitée des objets. Notre étude s'est focalisée principalement sur le protocole MAODV dans le but de proposer une amélioration visant à optimiser ses performances. Notre proposition s'est déroulée en deux parties distinctes : tout d'abord, nous avons abordé la détection des nœuds critiques au sein du réseau, puis nous avons procédé à des simulations standard ainsi qu'à des simulations où nous avons évité ces nœuds critiques. Concernant la première partie, nous avons présenté les variantes CNP et 3C-CNP que nous avons mises en œuvre pour la détection des nœuds critiques. Pour la deuxième partie, nous avons apporté des modifications à notre protocole afin d'éviter ces nœuds critiques. Pour ce faire, nous avons utilisé le simulateur NS2 comme environnement de développement pour mettre en œuvre notre approche et observer les causes et les effets selon différents scénarios de simulation. Ensuite, nous avons présenté et analysé les résultats obtenus.

Malgré certains inconvénients, tels que le manque de documentation pratique et la difficulté de prise en main de NS2, ce rapport présente le protocole MAODV comme une étude de cas dans le contexte d'un réseau IoT. Nous avons étudié en détail le fonctionnement de MAODV ainsi que réalisé des simulations. Nous avons également cherché à acquérir une expérience plus approfondie de l'outil NS2 et à approfondir notre compréhension.

Les résultats obtenus nous ont permis de conclure que le protocole amélioré offre de meilleures performances que le protocole standard, notamment en termes de réduction du nombre de paquets perdus, d'augmentation du taux de livraison et de diminution des coûts indirects moyens des paquets de données. En ce qui concerne les perspectives futures, pour compléter notre étude, nous encourageons les étudiants souhaitant poursuivre dans cette voie à explorer les différentes méthodes de réduction des nœuds critiques afin de comparer l'efficacité de tous les

algorithmes de détection de ces nœuds critiques. Il serait également intéressant d'évaluer leur impact potentiel sur les résultats de notre proposition.

Bibliographie

[1] *ABDELHAMID ZEBDI,DZ-MAODV : NOUVEAU PROTOCOLE DE ROUTAGE MUL TICAST POUR LES RÉSEAUX ADHOC MOBILES BASÉ SUR LES ZONES DENSES,L'UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES .*

[2] *Boukhebiza Meroua,La sécurité du protocole de routage OLSR dans un réseau AD HOC mobile,Université SAAD DAHLEB Blida, Thèse de master, année 2019-2020.*

[3] *Boukhechem. N, «Routage dans les réseaux mobiles Ad hoc par une approche à base d'agent» , mémoire Présenté en vue de l'obtention du diplôme de Magister en informatique, Université de Constantine, Promotion 2007-2008.*

[4] *Smaala Aziz, « Analyse analytique des protocoles multicast géographique dans les réseaux de capteurs », Thèse de master en informatique, université Larbi Ben M'hidi – Oum El Bouaghi, année 2017-2018.*

[5] *Amir Abdelkader AOUIZ,«Qualité de service dans les protocoles multi-chemins»,Thése de doctorat,Université Djillali Liabés de Sidi Bel Abbés En cotutelle internationale avec l'université de Haute Alsace-France ,2020.*

[6] *Melle ZIADA Khawla et Melle BENMAMACE Yasmina, « Étude et simulation du protocole de Routage AOMDV dans les réseaux mobiles ad hoc », Thèse de master, Université A. MIRA Bejaïa, année 2020-2021.*

[7] *MERATATE Soumia, « Les protocoles de routage dans le réseau ad-hoc », Thèse de master, UNIVERSITE DE MOHAMED BOUDIAF - M'SILA, année 2015.*

[8] *Farid JADDI, « une extension hiérarchique adaptative du protocole de routage ad hoc DSR », Ecole Doctorale d'Informatique et Télécommunications, pour obtenir LE TITRE DE DOCTEUR DE L'INSTITUT NATIONAL POLYTECHNIQUE DE TOULOUSE, année 2006.*

[9] *Henoune Mohammed Mokhtar, « La sécurité des réseaux sans fil », mémoire pour obtenir le diplôme de magister Spécialité Informatique Option : Ingénierie des logiciels et des réseaux, université d'Oran, 2010/2011.*

[10] *Badache, N and Lemlouma, Tayeb,Le routage dans les réseaux mobiles ad hoc,Master Degree Dissertation,University of USTHB, Algiers, Algeria,2000*

[11] *HAGGAR BACHAR SALIM « les protocoles de routage dans les réseaux ad hoc »21/06/2007, master de recherche STIC, Université de Reims VFR science.*

[12] *KETTOUCHE FERIEL, « Protocole de routage multi-chemins EAOMDV avec consommation d'énergie dans les réseaux sans fil Ad Hoc », UNIVERSITE ABDELHAMID IBN BADIS MOSTAGANEM, Thèse de master, année 2012-2013.*

[13] *Routage dans les réseaux ad hoc, Auteur(s) : Paul MÜHLETHALER, date de publication : 10 nov. 2004.*

[14] *https ://waytolearnx.com/2018/07/difference-entre-unicast-et-multicast.html*

[15] *SALEH, Imad. Internet des Objets (IdO) : Concepts, enjeux, défis et perspectives. Revue Internet des objets, 2018, vol. 2, no 10.21494.*

[16] *StackLima. Caractéristiques de l'internet des objets. Date de publication 05 juillet 2022.*

[17] *Axel Colin de Verdiere, « Multicast and flooding in Ad Hoc Networks », University of CaliforniaLos Angeles, Master of Science in Computer, Science, année 2014.*

[18] *Cédric FERRARIS, « Multicast explicite dans les réseaux ad hoc mobiles : implémentation, analyse et simulations d'un nouveau protocole multicast pour MANETs », Université de Montréal, Mémoire présenté à la Faculté des études supérieures en vue de l'obtention du grade de Maître ès Sciences (M.Sc.) en informatique, année 2007.*

[19] *Elizabeth M. Royer, « Multicast Ad hoc On-Demand Distance Vector (MAODV) Routing », University of California, Santa Barbara, 15 July 2000.*

[20] *KEBIR Bahia et RAHMOUNI Samia, « Amélioration des performances du protocole de routage RPL », Université Abou Bakr Belkaid– Tlemcen, 04 juillet 2017.*

[21] *Ouadah Abdenour, « Modélisation et vérification formelle d'un protocole CoAP pour l'internet des objets », Université Mohamed Boudiaf De M'sila, 2018 / 2019.*

[22] *Fellah Soumaya,«Optimisation du routage multicast dans les reseaux sans fil mailles»,Université d'Oran ,mémoire Présenté en vue de l'obtention du diplôme de Magister en informatique.*

[23] *Benceni, N. (2017). Maintenance proactive des routes dans les réseaux mobiles ad hoc pour le protocole AODV (Doctoral dissertation, FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE-UNIVERSITE MOHAMED BOUDIAF-M'SILA).*

[24] *] Kanthimathi, S., and P. JhansiRani. "Optimal routing based load balanced congestion control using MAODV in WANET environment." International Journal of Advanced Computer Science and Applications 12.3 (2021).*

[25] *AYACHI, Mohamed Ali. Contributions à la détection des comportements malhonnêtes dans les réseaux ad hoc AODV par analyse de la confiance implicite. 2011. Thèse de doctorat. Université Rennes 1 ; Université Européenne de Bretagne ; Université 7 Novembre à Carthage.*

[26] *Sabrine NAIMI. Gestion de la mobilité dans les réseaux Ad Hoc par anticipation des métriques de routage. 2015. Thèse de doctorat. Université Paris Sud-Paris XI ; École nationale d'ingénieurs de Tunis (Tunisie).*

[27] *Yang Yaling, Jun Wang, and Robin Kravets. "Designing routing metrics for mesh networks." IEEE workshop on wireless mesh networks (WiMesh). 2005.*

[28] *CHEHATA, AHMED. "ALGORITHMES DE ROUTAGE DANS LES RÉSEAUX SANS-FIL DE RADIOS COGNITIVES À MULTI-SAUTS." UNIVERSITÉ DU QUÉBEC À MONTRÉAL (2011).*

[29] *G. Parissidis, M. Karaliopoulos, R. Baumann, T. Spyropoulos, and B. Plattner. Routing metrics for wireless mesh networks. jan 2009.*

[30] *Bai, Fan, Narayanan Sadagopan, and Ahmed Helmy. "IMPORTANT : A framework to systematically analyze the Impact of Mobility on Performance of RouTing protocols for Adhoc NeTworks." IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428). Vol. 2. IEEE, 2003.*

[31] *K,Billel, Z.Fatma Zohra. "Simulation des protocoles des routages AODV et OLSR dans les réseaux ad-hoc via Opnet."*

[32] *Foudad Nesrine , Ziani Imane." Social Network Analysis" .Université Hassiba Benbouali de Chlef.*

[33] *Lalou Mohammed, Mohammed Amin Tahraoui, and Hamamache Kheddouci. "The critical node detection problem in networks : A survey." Computer Science Review 28 (2018) : 92-117.*

[34] *KINZI Dihia et MEDJBEUR Atika, Etude et simulation du protocole de routage DSDV dans le cadre des réseaux Ad-hoc ,année 2017/2018.*

[35] *Tran, Thong-Nhat and Nguyen, Toan-Van and Shim, Kyusung and Da Costa, Daniel Benevides and An, Beongku,A new deep Q-network design for QoS multicast routing in cognitive radio MANETsIEEE Access,pages=152841–152856,2021*

[36] *Khan, Faheem and Abbas, Sohail and Khan, Samiullah,An efficient and reliable core-assisted multicast routing protocol in mobile Ad-Hoc network,International journal of advanced computer science and applications,2016*

[37] *Mandhare, VV and Thool, RC,Improving QoS of mobile ad-hoc network using cache update scheme in dynamic source routing protocol,journal :Procedia Computer Science , pages=692–699,2016*