République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Hadj LAKHDAR –Batna-

Faculté des Sciences **Département d'Informatique**

N°d'ordre :……
Série :……

Mémoire

En vue de l'obtention du diplôme de

Magister en Informatique

Option**: Systèmes informatiques de communication(SIC)**

Présenté par :

KHEBBACHE Mohibeddine

TITRE

Protocole de transport multicast fiable pour les réseaux sans fil

Soutenu le : 28/01/2014

Devant le jury:

Pr. ZIDANI Abdelmajid	Professeur	**Président**	Université de Batna
Pr. BILAMI Azeddine	Professeur	**Rapporteur**	Université de Batna
Dr. ZIDAT Samir	M.C.A	**Examinateur**	Université de Batna
Dr. MAAMRI Remdane	M.C.A	**Examinateur**	Université de Constantine

Dédicace

À mes chers parents.

À mon frère et mes sœurs.

À toute ma famille.

À tous mes amies.

À tous mes collègues.

Remerciement

Je remercie, Tout d'abord, ALLAH pour la volonté, la force, la santé et la patience qu'il m'a donné afin de réaliser ce travail.

Mes sincères remerciements s'adressent au Professeur. Azeddine Bilami *pour son encadrement, ses qualités humaines, sa confiance et sa patience, ses précieux conseils et ses remarques pertinentes durant la réalisation de ce travail. J'ai eu l'honneur de travailler sous sa direction et je lui présente mon respect et ma gratitude.*

Je tiens également à remercier tous les membres de jury. J'ai eu le plaisir d'avoir accepté l'évaluation de ce mémoire.

Je tiens aussi à remercier tous mes enseignants de la première année de Magister et les responsables de département d'informatique de l'université de Batna pour l'effort qu'ils ont déployé durant ma formation.

Enfin, une immense merci à tous mes collègues et amies ; surtout :
Mme. KHELIFA Hanane, Mlle. BOUTEMDJER Ouassila, Nadjib, Samir, Raouf, Wassim, Salah, Younec, Saâdan, Ridha, Mohammed, Djaber, Ali, Ahmed, Okba, Abdelaziz, Thaoui, Walid ... *pour leur soutien inconditionnel et leur encouragement.*

Résumé

La communication multipoint (multicast) s'avère comme une solution naturelle pour soutenir efficacement les applications multipoint. Dans les réseaux ad hoc, le support d'une communication multicast mène à des nouvelles pistes d'investigation, afin d'adresser les problèmes inhérents du routage multicast au niveau réseau et de la fiabilité au niveau supérieur du service de routage multicast best effort. Dans ce mémoire, nous proposons un nouvel protocole, nommé WASRM (Wireless Active Scalable Reliable Multicast), qui soutient les applications multipoint de type many-to-many déployées dans les réseaux ad hoc, dont l'objectif est de résoudre la problématique autour la fourniture d'un service multicast fiable au niveau transport, qui est essentiel et fortement exigé par ces applications. Notre solution est fondée sur l'adoption des temporisateurs aléatoires en combinaison avec le support des routeurs actifs. Cette combinaison vise à garantir la délivrance des données multidestinataires et assurer une utilisation efficace des ressources de réseau, tout en allégeant les problèmes survenus lors du passage à l'échelle d'un grand nombre de récepteurs. La simulation permet de couvrir les aspects de validation des performances de notre protocole.

Mots clés : Réseaux ad hoc, Routage multicast, Multicast fiable, Transport.

Abstract

A multipoint communication (multicast) proves to be a natural solution to effectively support multipoint applications. In ad hoc networks, the support of multicast communication leads to new areas of investigation, in order to address the problems inherent of multicast routing at network layer and the reliability at upper layer of the best effort multicast routing service. In our work, we proposed a new protocol, named WASRM (Wireless Active Scalable Reliable Multicast), which support many-to-many multipoint applications deployed in ad hoc networks, in order to resolve the problematic of providing reliable multicast service at the transport level, which is essential and highly required by these applications. Our solution is based on an adoptation of random timers with the combination of active routers support. The aim of this combination is to guarantee the delivery of multicast data and to ensure the efficient use of network resources, while minimizing the problems encountered when scaling to a large number of receivers. The simulation allows validation aspects of our protocol performances to be covered.

Key words: ad hoc networks, multicast routing, reliable multicast, transport.

ملخص

الاتصال المتعدد (الإرسال المتعدد) يظهر كحل طبيعي لدعم بكل فعالية التطبيقات المتعددة. دعم الاتصال ذو الانتشار المتعدد على مستوى الشبكات اللاسلكية الحرة (ad hoc)، أدى إلى سبل جديدة في البحث من أجل معالجة المشاكل المتأصلة الخاصة بتوجيه الإرسال المتعدد (routage multicast) على مستوى طبقة الشبكة وكذا تأكيد الموثوقية (fiabilité)على مستوى النقل لخدمة توجيه الإرسال المتعدد بأقل جهد. في هذه المذكرة، اقترحنا بروتوكول جديد، اسمه WASRM(Wireless Active Scalable Reliable Multicast)، الذي يدعم التطبيقات المتعددة من نوع العديد-إلى-العديد المنتشرة على مستوى الشبكات اللاسلكية الحرة (ad hoc)، بغرض حل إشكالية توفير خدمة الإرسال المتعدد الموثق في طبقة النقل، الضرورية و المطلوبة بقوة من طرف هذه التطبيقات. الحل الذي اقترحناه يستند على تبني المؤقتات العشوائية بالتنسيق مع دعم أجهزة التوجيه النشط . هذه التركيبة تهدف إلى ضمان تسليم البيانات ذات الاستقبال المتعدد وتحقيق الاستخدام الفعال لموارد الشبكة مع تخفيف المشاكل الطارئة أثناء التعامل مع عدد كبير للمستقبلين. المحاكاة تسمح بتغطية جوانب التصديق على أداء البروتوكول الذي اقترحناه.

الكلمات المفتاحية: الشبكة الحرة (ad hoc)، توجيه الإرسال المتعدد، الانتشار المتعدد الموثق، النقل.

Table des matières

Chapitre 3: Multicast dans les réseaux sans fil

Chapitre 4: Proposition d'un protocole de transport multicast fiable pour les réseaux ad hoc

Chapitre 4: Evaluation des performances

Liste des figures

Liste des tableaux

Introduction générale

Introduction générale

Les réseaux sans fil représentent un cas particulier de réseaux informatiques, qui sont nés pour permettre à des équipements de se relier sans avoir recours à un support filaire (par voie hertzienne), dont l'intérêt d'accéder au réseau **n' importe où** et **n'importe quand.**

Les réseaux sans fil 'ad-hoc' sont formés par un ensemble de terminaux sans fil qui se communiquent, sans l'aide d'une infrastructure ou une administration centrale, de sorte que les utilisateurs puissent installer, à **tout temps** et **partout**, un réseau temporaire.

Dans le contexte des communications de groupe, et grâce à l'installation rapide et moins coûteuse des réseaux sans fil, la flexibilité de l'interface radio et leurs caractéristiques d'auto-organisation et orienté-groupe, de nombreuses applications mobiles requièrent un service de communication multicast ont été déployées dans ces réseaux, telles que : les fournisseurs de service, l'enseignement à distance, le domaine militaire et les opérations de secours.

En outre, certaines de ces applications sont peu sensibles à la contrainte de temps alors qu'elles ne peuvent tolérer la perte des données en exigeant une fiabilité totale de délivrance. Néanmoins, ces dernières peuvent être sacrifiées par son déploiement dans les réseaux sans fil, là où le taux de perte est élevé et les protocoles de multicast implémentés au niveau réseau n'assurent aucune garantie sur la livraison fiable de données (délivrance à moindre effort).

Par conséquent, le développement des mécanismes de niveau supérieur (transport ou application), pour adresser le problème de la fiabilité multicast, devient un objectif crucial dans ces réseaux. Ces derniers doivent s'adapter aux diverses contraintes rencontrées, et en plus, doivent garder ses performances avec un groupe de taille importante, tout en garantissant la propriété de **la scalabilité**.

Par ailleurs, l'adaptation du protocole universel de transport unicast fiable **TCP** (Transmission Control Protocol) dans ce contexte reste aujourd'hui un défi de recherche. Bien que les travaux courants de recherche proposent des solutions afin d'offrir des degrés variés de la fiabilité multicast, sur plusieurs niveaux de la pile des protocoles. Or ils restent incapables d'assurer une fiabilité totale, avec un groupe de taille important, dans ces environnements hostiles. En conséquence, la fiabilité multicast demeure toutefois un problème complexe dans les réseaux sans fil en générale, et les réseaux sans fi ad hoc en particulier.

La problématique que nous procurons se réfère à quel est le degré le plus élevé de la fiabilité des communications multicast que l'on peut assurer, et sur quel niveau de l'architecture, pour satisfaire les besoins de plusieurs applications multipoint déployées dans les réseaux sans fil ad hoc, tout en garantissant la scalabilité et l'utilisation efficace des ressources.

Notre objectif est de proposer un protocole de multicast fiable au niveau transport, adaptable pour les environnements sans fil ad hoc, qui doit supporter des applications multipoint spécifiques tout en garantissant le passage à l'échelle d'un grand nombre de récepteurs, et assurant une utilisation efficace des ressources de réseau. Ce protocole améliore la fiabilité du protocole de routage multicast sous-jacent, afin de garantir la délivrance réussite de presque 100% des paquets de données, c'est-à-dire, assurer la fiabilité totale de délivrance de bout-en bout de tous les paquets à tous les récepteurs.

Pour arriver à cette fin, nous avons proposé une nouvelle solution baptisée « **WASRM** » pour **W**ireless **A**ctive **S**calable **R**eliable **M**ulticast. Notre solution se repose sur l'adoptation de l'approche basée sur les temporisateurs aléatoires, pour la suppression des **NACK** (Negative ACKnowledge) et des retransmissions dupliqués, avec la contribution des routeurs actifs (le support du routeur) dans le processus de recouvrement.

Le choix d'adopter l'approche basée sur les temporisateurs, qui repose sur le mécanisme de recouvrement des pertes, **ARQ** (Automatic Repeat Request), de la classe « receiver-initiated », a été motivé par le fait qu'elle soit particulièrement robuste quant au changement de la topologie, permette de pallier le problème d'implosion des acquittements en feedback et garantisse une fiabilité totale tout en assurant la mise à l'échelle des récepteurs en croissance.

En plus, la contribution des routeurs actifs vient du fait qu'ils puissent mettre en cache, de façon probabiliste, une copie des paquets de données bien reçus, dont le but est d'aider à retransmettre les paquets de données pour les recouvrir localement, et également à restreindre la protée de retransmission pour alléger le problème majeur de localité de perte de l'approche précédente et surtout assurer un recouvrement scalable.

En outre, notre solution tire profit du concept innovant, **cross-layer**, dans la conception des protocoles adaptés pour les réseaux sans fil, afin d'améliorer ses performances par le partage des informations d'état du réseau entre les différentes couches. Ainsi, l'exploitation de la nature de diffusion inhérente au support sans fil, pour minimiser le taux d'erreur et le surcoût de retransmission.

Notre solution proposée, dans le contexte des réseaux ad hoc, vient pour supporter efficacement les applications de type **many-to-many** nécessitant des communications multicast de type **multipoint à multipoint fiable,** comme les domaines militaires et les opérations du secours après une catastrophe, où plusieurs sources peuvent exister dans le même groupe multicast**.** Pour valider ses performances, nous utilisons un outil de simulation de réseaux, tel que le simulateur réseau NS2.

Nous avons organisé la structuration de ce mémoire en cinq principaux chapitres :

Le premier chapitre présente brièvement l'évolution des différents types des réseaux sans fil et décrit en détaille la famille des réseaux sans fil ad hoc, tout en mettant l'accent sur les problématique rencontrées de la recherche. Le deuxième chapitre englobe un état de l'art sur le sujet de la fiabilité des communications multicast, et notamment les approches et les stratégies implantées récemment dans le réseau Internet. Le troisième chapitre se concentre sur le support des communications multicast dans les réseaux sans fil associé avec une étude synthétique des travaux de recherche qui ont été développés pour résoudre le problème de la fiabilité multicast dans la famille des réseaux sans fil ad hoc. Notre solution proposée est détaillée, avec une description de stratégies, des structures de données et d'algorithmes, dans le quatrième chapitre.

Dans le dernier chapitre, nous évaluons par simulation les performances de notre protocole proposé. Finalement, nous clôturons le travail faisant l'objet de ce mémoire par une conclusion générale, qui fournit aussi quelques perspectives d'amélioration au futur.

Réseaux sans fil

1. Introduction

Les réseaux sont constitués d'une série d'équipements matériels connectés entre eux par support de transmission et de processus logiciels (protocoles et règles) afin de transporter les données d'une machine terminale à une autre.

Similairement aux réseaux filaires, les réseaux sans fil permettent de relier très facilement des équipements distants d'une dizaine de mètres à quelques kilomètres mais sans recourir à une liaison filaire. En plus, la flexibilité des interfaces radio ainsi que la prolifération et la miniaturisation des équipements mobiles puissants (les téléphones intelligents, ordinateurs portables, assistants numériques personnels(PDA)…) ouvrent la voie pour un large déploiement des technologies sans fil et le passage à l'ère de l'informatique omniprésent où un utilisateur peut accéder au réseau et bénéficier de tous ses services n'importe quand et n'importe où.

Généralement, les réseaux sans fil peuvent être fixes ou mobiles. Du plus, ils constituent d'une infrastructure fixe de communication ou seulement des nœuds terminaux communicants sans infrastructure (ad hoc).

Le sujet des réseaux sans fil sera entamé dans le présent chapitre, allant de la représentation des différents types de ces réseaux, jusqu'à nous arriverons à décrire la classe des réseaux sans fil ad hoc en termes de champs d'application, limites et problématiques de recherche.

2. Réseaux informatiques

Les réseaux informatiques sont, des réseaux de communication, nés du besoin d'interconnecter un ensemble des équipements terminaux situés à distance les uns des autres. Pratiquement, ils misent à la disposition de ces équipements des ressources afin de transporter les données d'une source à un ou plusieurs destinataires selon des règles bien définies.

Dans un premier temps, ces communications étaient destinées au transport des données informatiques. Aujourd'hui, avec la numérisation, les réseaux informatiques seront aptes à transporter de nombreux types de données (données numériques sous forme d'une série des valeurs binaires), où, l'intégration de la parole téléphonique (voix) et de la vidéo est généralisée dans les réseaux informatiques tout en formant ainsi un environnement vital aux applications multimédias **[1]**.

Dans un réseau, les équipements sont interconnectés physiquement par le biais des supports de transmission, où à chaque nature de support correspond une forme particulière du signal qui s'y propage. Par ailleurs, dû à l'hétérogénéité des supports physiques de transmission, les réseaux informatiques peuvent être des réseaux filaires (câblés), des réseaux sans fil et des réseaux satellites. L'union de ces réseaux peut constituer le réseau public « **Internet** » ou « le réseau de réseaux » **[2]**. La figure **(1.1)** illustre les différents équipements terminaux et supports de transmission qui peuvent constituer un réseau informatique **[1]**.

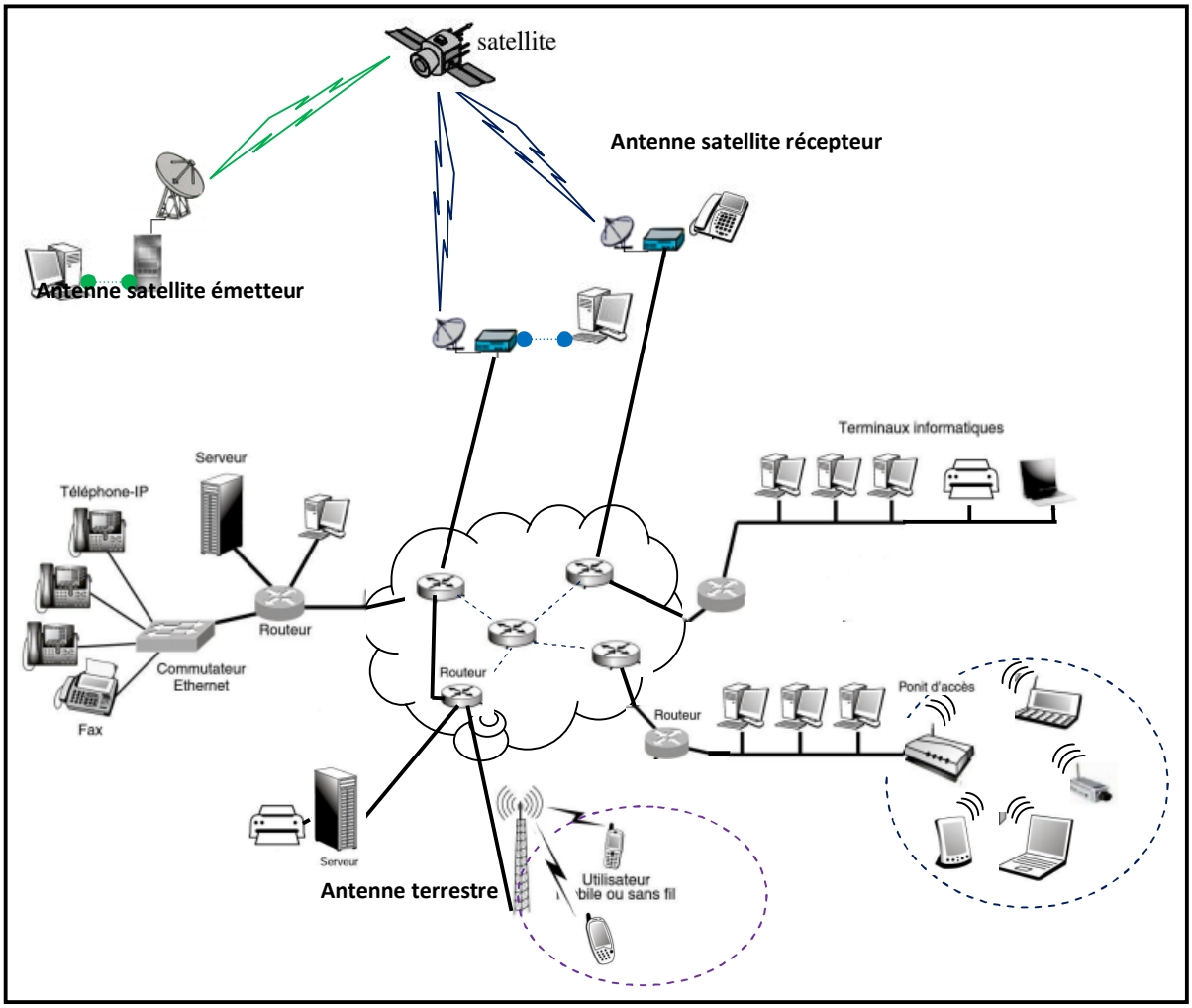

Figure 1.1: Eléments de base d'un réseau informatique.

2.1 Représentation graphique d'un réseau

Au niveau le plus bas, un réseau peut être représenté par un nuage constitué d'un ensemble des nœuds interconnectés par des liens, définissant le cœur du réseau. Leur organisation les uns par rapport aux autres désigne la topologie (physique) du réseau.

Les nœuds s'agissent comme des nœuds de commutation (commutateurs, routeurs, antennes terrestre ou satellites, points d'accès…), dont leur fonction principale est d'assurer l'acheminement des données en transit.

Tandis que les liens représentent les supports de transmission sur lesquels les données étant véhiculées **[3].** La figure ci-dessous **(1.2)** schématise la forme nuage d'un réseau.

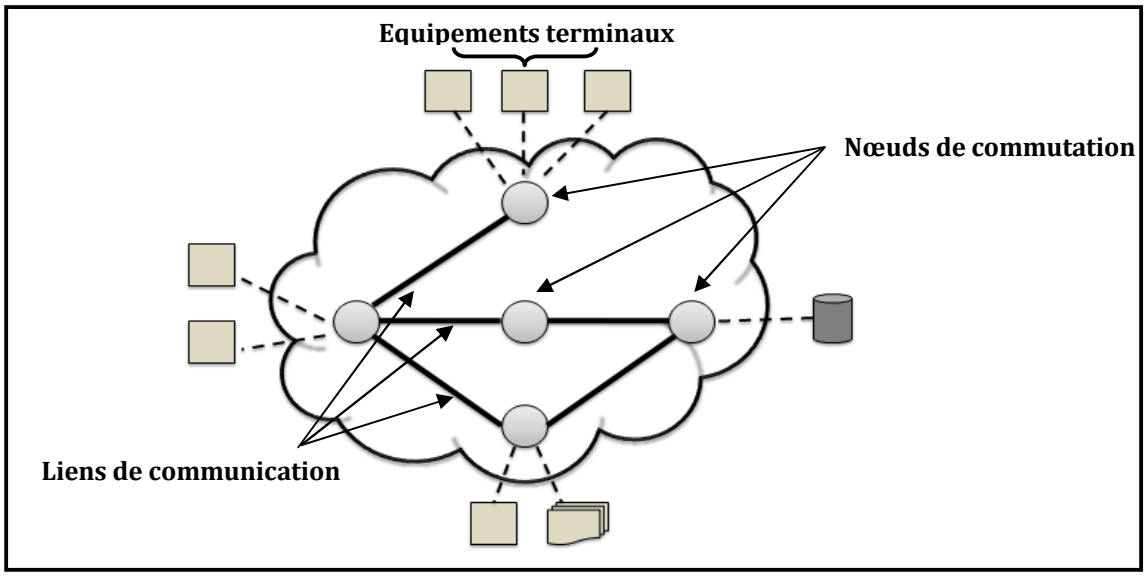

Figure 1.2: Représentation de réseau sous forme d'un nuage [3].

« L'informatique ubiquitaire » désigne que les réseaux informatiques deviennent omniprésents dans la vie quotidienne de nombreuses personnes **[2]**. Pour cela, ils doivent donc fournir une connectivité générale à un grand nombre d'équipements.

Par conséquent, et en plus de support physique de transmission (matériels sous jacent) assurant cette connectivité, il faut en outre une architecture logicielle chargée de définir les règles de transferts et du contrôle des données dans le réseau pour qu'elles soient livrées correctement au(x) destinataire(s) **[3]**.

2.2 Architecture de réseau

L'architecture de réseau est une représentation abstraite (indépendante de toute référence à des logiciels ou matériels particuliers) de la circulation des informations et des concepts utilisés au sein d'un réseau quelconque, qui est organisée sous forme des couches de **protocoles** et **services** empilées, dont le nombre, le nom, le contenu et la fonction de chacune diffère selon le réseau en question.

Le rôle des protocoles, dans une architecture, est crucial à la fourniture des services et à la standardisation des informations échangées grâce à la définition des règles déterminant le format et la signification des paquets ou des messages véhiculés. L'ensemble des protocoles utilisés par un réseau donné s'appelle « **une pile de protocoles** » **[2].**

L'architecture générique (modèle de référence) **OSI** (Open Systems Interconnection), provenant de la normalisation de l'**ISO,** constituée par, en plus de médium physique, sept couches, comme montre la figure **(1.3)**. Les principales d'entre-elles sont **[1, 2, 4]**:

- **La couche Liaison** : elle fournit les moyens d'établir, de maintenir et de gérer les connexions de liaison de données entre les entités réseau. Elle détecte et corrige les erreurs de la couche physique. Ses responsabilités incluent : l'adressage physique, le contrôle de flux, d'erreurs et d'accès au médium. **La trame** est l'unité de données manipulée.
- **La couche Réseau** : fournit aux entités de transport les moyens d'établir, de maintenir et de gérer les connexions de réseau. Ses responsabilités sont l'adressage logique et le routage de sorte qu'elle achemine **les paquets** à travers le réseau jusqu'à l'utilisateur final.
- **La couche Transport** : elle fournit des services fiables de transfert **des messages** de bout-en-bout pour les couches supérieures, et optimise l'utilisation des services réseau disponibles. Ses responsabilités: la segmentation / désegmentation, le contrôle de flux et d'erreur.
- **La couche Application** : Elle contient les entités d'application, c'est-à-dire les processus des applications d'utilisateurs qui génèrent les informations à échanger.

Les systèmes d'extrémité implémentent toutes les couches, tandis que les équipements du réseau, dans les systèmes intermédiaires, n'implémentes que les couches basses.

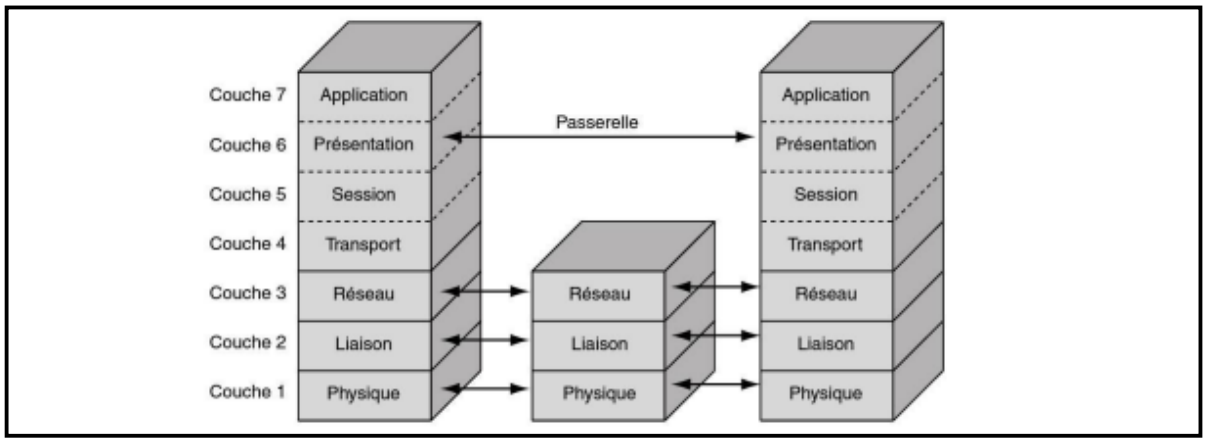

Figure 1.3: Architecture (le modèle de référence) OSI [1].

L'interopérabilité entre équipements hétérogènes issus de différents constructeurs implique des normes d'interconnexion définissant le comportement de chaque équipement vis-à-vis des autres. L'**ISO** (International Standardization Organization) et l'**ITU** (International Telecommunications Union) représentent les principaux organismes internationaux de normalisation, tandis que l'**ECMA** (European Computer Manufacturer), l'**EIA** (Electronic Industries Association), L'**IEEE** (Institute for Electricity and Electronics Engineers) et l'**IAB** (Internet Architecture Board) soient des regroupements de divers constructeurs **[4]**.

3. Réseaux sans fil

Un réseau sans fil (en anglais **Wireless network**) est, comme son nom l'indique, un cas particulier des réseaux informatiques dans lequel au moins deux équipements (ordinateur, PDA, imprimante, routeur…) peuvent communiquer sans liaison filaire (indépendamment des prises murales). Néanmoins, il recourt à des ondes hertziennes (radio et infrarouges) comme un support de transmission. Il est plutôt considéré comme une extension de réseau filaire existant, et non pour le remplacer, offrant l'avantage d'une connectivité sans fil **[5]**.

Les équipements terminaux qui se trouvent à l'intérieur de la zone couverte par le réseau peuvent communiquer directement ou par l'intermédiaire d'une borne d'accès (points d'accès ou stations de base) jouant le rôle de routeur. Les communications entre les bornes d'accès peuvent être hertziennes ou par câble **[1].**

3.1 Intérêts et avantages des réseaux sans fil

- L'intérêt principal des réseaux sans fil vise à offrir à un utilisateur la possibilité de se connecter (accéder) au réseau n'importe où et n'importe quand, tout en se déplaçant dans un périmètre géographique plus ou moins étendu, notion de « **mobilité** » ou « **itinérance** ».
- De plus, l'installation de tels réseaux ne demande pas de lourds aménagements des infrastructures existantes, comme le cas des réseaux filaires. Elle est simple, plus économique (moins coûteuse), rapide et permet la dynamicité et la flexibilité de la topologie du réseau.
- Les transmissions radioélectriques sont toutefois soumises à une réglementation stricte. En effet, elles servent à un grand nombre d'applications (militaires, scientifiques, amateurs) **[5].**
- L'extensibilité du réseau permet d'avoir toujours une couverture hertzienne correspondante aux besoins réels. Ceci garantit son évolutivité par rapport au réseau filaire.

La spécificité cruciale donc des réseaux sans fil est d'assurer aux usagers (utilisateurs) nomades et mobiles (plutôt qu'aux usagers stationnaires) une connectivité aux services réseau fixes et mobiles.

3.2 Catégories des réseaux sans fil

L'essor des réseaux sans fil est au fait qu'un utilisateur puisse se connecter au réseau indépendamment de leur localisation physique ou de leur comportement de mouvement. Compte tenu du niveau de mobilité (la position relative des composants réseau), les réseaux sans fil peuvent être divisé en: réseaux sans fil fixes et réseaux sans fil mobiles.

Dans les réseaux sans fil fixes, les composants du réseau occupent une position fixe, alors que les équipements terminaux soient faiblement mobiles dans une zone géographiquement limitée. C'est là où les usagers nomades peuvent accéder à partir des points fixes en ayant recourus éventuellement à des liaisons sans fil. Néanmoins, dans les réseaux sans fil mobiles, on peut avoir la mobilité des terminaux de réseau, tout en préservant la connexion durant leur mouvement (l'ubiquité des usagers), ou du réseau en totalité **[2]**.

En outre, les technologies sans fil utilisent plusieurs gammes de produits qui ont été normalisés par les groupes de travail proviennent de l'IEEE et de l'ETSI **[1]**. La figure **(1.4)** décrit les différentes catégories de réseaux suivant le périmètre géographique offrant la connectivité, le débit, la portée des transmissions et la norme qu'ils se reposent.

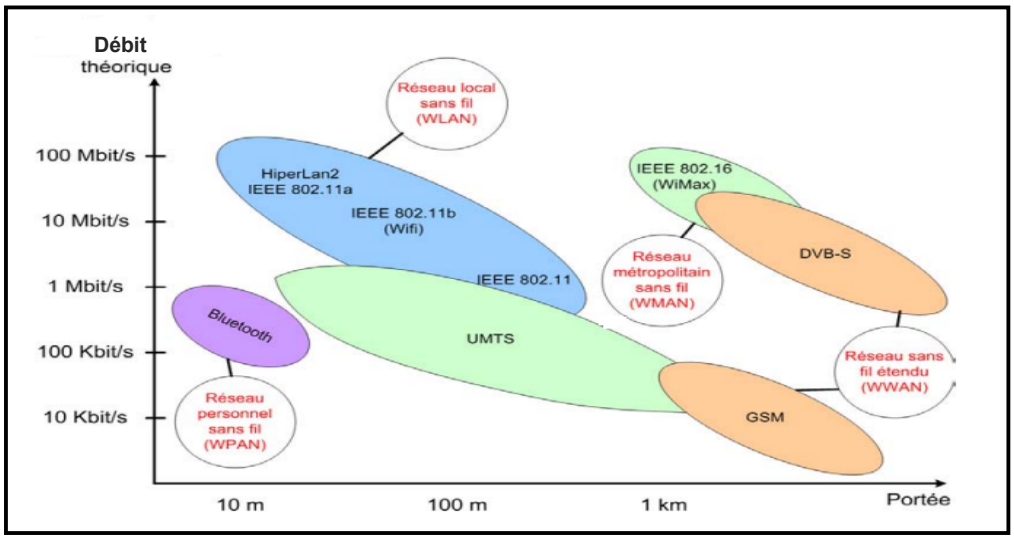

Figure 1.4: Catégories de réseaux sans fil.

- **Réseau étendu sans fil (WWAN, *Wireless Wide Area Network*):** nommé également réseau cellulaire étendu, qui est constitué par un ensemble de « cellules » couvrant un pays. Chacune dispose une station de base qui sert comme un point d'accès de toutes les communications **[6]**. Bien que dans ce contexte, là où les stations de base soient édifiées une fois pour toutes, le réseau lui-même demeurant fixe ; cependant les terminaux sont uniquement soumis au mouvement. la famille des réseaux cellulaires qui supportent la mobilité sont appelés « réseaux de mobiles » ou « réseaux mobiles » **[7]**. Ceci grâce à la gestion du changement intercellulaire (**handover** ou **handoff**), et le changement du réseau d'opérateur « **itinérance** (en anglais **roaming**) » **[7]**. En outre, l'évolution des systèmes cellulaires mènent à plusieurs générations. **GSM** (Global System for Mobile Communications) et **UMTS** (Universal Mobile Telecommunications System) représentent, respectivement, la deuxième et la troisième génération des réseaux de mobiles.

- **Réseau métropolitain sans fil (WMAN, *Wireless Metropolitan Area Network*) :** Les réseaux hertziens IEEE 802.16, destinés principalement aux opérateurs de télécommunication, visent à fournir un accès Internet aux habitants des zones géographiques difficiles à couvrir. Ces réseaux forment « la boucle locale radio(BLR) » qui offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 km. Le consortium **WiMAX** (Worldwide Interoperability for Microwave Access) est mis en place pour développer les applications de cette norme**.** Deux versions ont été commercialisées : WiMAX fixe (IEEE 802.16-2004) et WiMAX mobile (IEEE 802.16e) **[1].**
- **Réseau local sans fil (WLAN, *Wireless Local Area Network*):** il permet de relier des équipements terminaux équipés d'interface radio de faible portée (ordinateurs portables, ordinateurs de bureau, PDA ou équipements d'électronique grand public) sur un rayon de plusieurs centaines de mètres tout en créant un réseau local privé à haut débit par voie hertzienne, là où l'installation de câble poserait trop de problèmes (les immeubles de bureaux anciens, les gares, les aéroports…). Les équipements restent faiblement mobiles à l'intérieur de la périphérie de la zone de couverture. La norme des réseaux locaux sans fil est IEEE 802.11. Il existe plusieurs technologies concurrentes : le **Wi-Fi** (Wireless Fidelity) ou IEEE 802.11b et le **HiperLAN1/2** (High Performance Radio LAN 1/2), qui opère dans des bandes non soumises à licence, comme les bandes **ISM** (industriel, scientifique et médicale) **[5]**.
- **Réseau personnel sans fil (WPAN, *Wireless Personal Area Network*) :** réseau individuel sans fil ou réseau domestique sans fil. Il concerne les réseaux sans fil d'une faible portée, quelques dizaines de mètres, où des équipements très peu distants communiquent sans liaison filaire. Il relie des périphériques à l'échelle individuelle (humaine) (une oreillette à un téléphone mobile) ou deux équipements peu distants (téléphones portables, appareils domestiques, assistants personnels (PDA), micro-ordinateurs). La norme de ce type de réseau est IEEE 802.15. Il existe plusieurs technologies utilisées pour les WPAN : **Bluetooth**, **HomeRF** (Home Radio Frequency), **ZigBee** et **infrarouge [5]**. D'autres technologies de communication en champ proche ou **NFC** (Near Field Communication), comme **RFID** (Radio-Frequency Identification), permettent aussi de construire des PAN **[2]**.

Dans les réseaux sans fil, les réseaux cellulaires s'appuient sur la commutation de circuit. Pour entrer pleinement dans l'ère des paquets, il a fallu attendre la troisième génération, celle de l'UMTS et du cdma2000. Cependant, les vrais réseaux IP dans le monde hertzien ont été introduits par les travaux de l' IEEE et de l'ETSI. En particulier, les réseaux de la gamme Wi-Fi ou WiMAX qui transportent des paquets IP encapsulés dans des trames Ethernet **[1]**.

3.4 Architectures des réseaux sans fil

Deux grandes familles de réseaux sans fil, à savoir: les réseaux avec infrastructure et les réseaux sans infrastructure (Infrastructureless) **[4]**.

- **Les réseaux à infrastructure** : Dans les réseaux avec infrastructure, le réseau est géré par une ou plusieurs bornes d'accès stationnaires (stations de base ou points d'accès). Lorsqu'un réseau comprend plusieurs bornes, celles-ci sont raccordées par un réseau filaire (comme Ethernet, ATM, Internet) formant ainsi une infrastructure qui demeure fixe. La communication entre les équipements terminaux est pilotée à un moment ou un autre par le biais d'une borne où un nœud (équipement) mobile utilise une communication radio sans fil direct d'un seul saut (single hop) pour accéder à cette borne qui le relie à l'infrastructure filaire. Les réseaux cellulaires et les réseaux WLAN en mode avec infrastructure fonctionnent selon ce modèle.

- **Les réseaux sans infrastructure (ad hoc)** : Les réseaux ad hoc sont des réseaux sans fil capables de s'organiser sans infrastructure définie préalablement. Dans les réseaux ad hoc, les communications s'effectuent directement en point à point entre les stations où la gestion et la configuration de tels réseaux ne nécessitait aucun administrateur. Pour communiquer entre eux, les terminaux ont seulement besoin de disposer de logiciels adéquats et de bonde de fréquences autorisée. C'est le modèle de fonctionnement des WPAN et des réseaux WLAN en mode ad hoc (sans infrastructure).

3.5 Limites des réseaux sans fil

- **Allocation des fréquences d'émission**: le problème majeur des réseaux sans fil est de trouver une bande de fréquence adéquate et disponible. La première solution consiste à utiliser de coûteuses portions du spectre sous licence définies par une réglementation propre à chaque pays, tandis que la deuxième approche adoptée utilise des bandes non soumises à licence (bande ISM) qui peuvent se trouver en conflit avec d'autres équipements (des commandes d'ouverture de porte de garage, des fours à micro-ondes). **[2]**

- **La fiabilité**: Les liaisons sans fil sont relativement peu fiables et sont encore très lentes comparativement aux liaisons câblées.

- **L'interférence et l'évanouissement**: à cause des obstacles rencontrés et aux réflexions successives, un signal source peut être amené à atteindre le(s) récepteur(s) en empruntant des chemins multiples (multipath). Ce phénomène appelé **atténuation** ou **évanouissement (fading),** due aux trajets multiples, résultant un affaiblissement de la puissance d'émission.

De plus, plusieurs émissions simultanées sur des bandes de fréquences proches étant susceptibles d'être interférées au niveau de(s) destinataire(s). En effet, la qualité de la transmission sera dégradée tout en influant la fiabilité de la liaison (taux d'erreur élevé) **[7]**.

- **La sécurité**: comme les transmissions sans fil sont des diffusions, un pirate peut facilement écouter ou espionner les informations circulées en clair dans le réseau. Il est donc impératif de mettre en place les dispositions nécessaires (authentification, algorithmes de cryptage) afin de protéger le contenu des flux et d'assurer la confidentialité des données dans le réseau **[7]**.
- **l'économie d'énergie:** les terminaux sans fil peuvent être fixes ou mobiles. Le problème principal des terminaux mobiles concerne leur batterie, qui n'a généralement que peu d'autonomie. Cette limitation doit être prend à mesure que le temps d'activité d'un terminal mobile soit maximal.
- **Risques sanitaires:** l'impact des radiofréquences sur la santé de l'homme représente le sujet des débats scientifiques. Aujourd'hui, plusieurs études sont en train de démontrer que les symptômes des « électro-hypersensibles » soient effectivement dus aux ondes radio **[5]**.

4. Réseaux sans fil Ad hoc

Les réseaux ad hoc datent de plusieurs dizaines d'années. Ils visent à réaliser un environnement de communication qui se déploie sans autre infrastructure que les mobiles eux-mêmes. Les désires d'avoir un réseau sans infrastructure ont été découverts dans les années 1970 avec l'utilisation de la technologie '**packet radio'** dans les projets 'ALOHA' et 'packet radio network (PRNET)' **[9]**. Le terme 'ad hoc' signifie 'peut prendre différentes formes' et 'peut être mobile, autonome ou en réseau' **[9]**. Autrement, il implique qu'on puisse créer un réseau spontané pour fournir un service dédié à un type particulier d'applications **[10]**.

Un réseau sans fil ad hoc (sans infrastructure) est constitué d'une collection de deux ou plusieurs nœuds sans fil (muni d'une interface radio transceiver) situés à proximité les uns des autres et qui se communiquent, en partageant le même lien de communication et indépendamment (sans l'aide) à une infrastructure existante ou à une administration centrale (station de base ou point d'accès), pour former un réseau dynamique et temporaire, donc ces réseaux sont auto-organisés (***self-organizing***) et adaptatifs **[9]**. Un tel réseau peut fonctionner dans un mode autonome ou peut être connecté à un réseau filaire fixe comme l'Internet **[11]**. La figure suivante **(1.5)** montre des exemples des réseaux ad hoc.

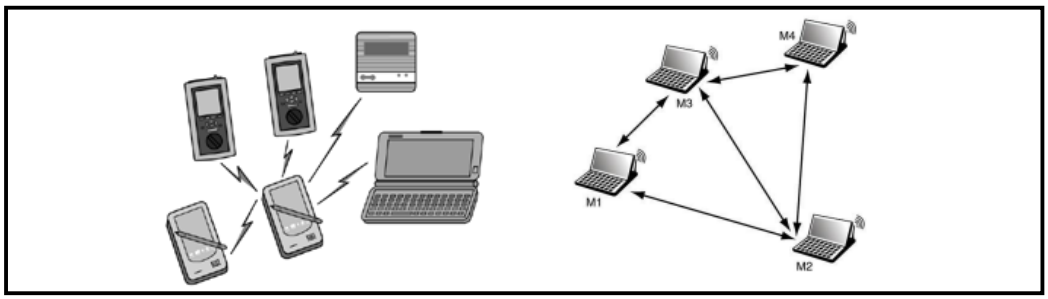

Figure 1.5: Exemples de réseaux sans fil ad hoc [9].

Sachant que les nœuds se communiquent en mode d'égale à égale (p2p) selon le principe store-and-forward (sans aucune borne d'accès n'est utilisée), les données puissent être livrées directement via un chemin uni-saut (single hop path) aux destinations qui ont à la portée radio de la source. Comme montre la figure **(1.6),** le nœud A peut communiquer avec le nœud B qui est à sa portée radio. Bien qu'en raison de la limitation de la couverture radio de l'interface sans fil, les données sont ainsi acheminées indirectement à travers des nœuds intermédiaires, constituant un chemin multi-saut (multi-hop path), qui relayent les données jusqu'à la destination éloignée de la source en utilisant un mécanisme de routage (cas des nœuds A et C de la figure **(1.6)**). En effet, chaque nœud du réseau peut fonctionner comme un hôte et/ou un routeur **[10]**.

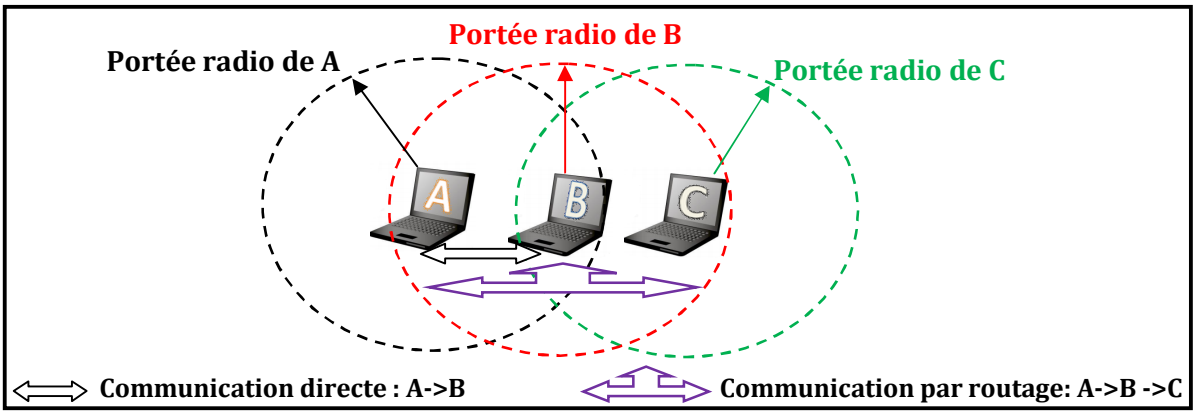

Figure 1.6: Communication dans les réseaux ad hoc.

Dans leur configuration mobile, les réseaux ad-hoc sont connus sous le nom des réseaux ad hoc mobiles ou **MANET** (**M**obile **A**d hoc **NET**works), quant à eux, un cas particulier des réseaux 'mobiles' sans infrastructure fixe, dont les nœuds à peine initialisés sont capables, en quelques instants, d'échanger de l'information en fonction de leur localisation **[7]**. Ainsi, les nœuds mobiles se déplacent librement s'organisent arbitrairement tout en traduisant le changement rapide et imprévisible de la topologie du réseau **[11]**. En outre, MANET fait aussi référence au nom d'un groupe de travail de l'IETF, qui se préoccupe de la standardisation des protocoles de routage basés sur la technologie IP pour les réseaux ad hoc **[1]**.

4.1 Différences entre les réseaux ad hoc et les réseaux cellulaires

Les réseaux ad hoc et les réseaux cellulaires peuvent coexister afin de former un réseau sans fil étendu dans des zones multiples. Cependant, ils sont complémentaires dans des différents points. Parmi lesquels le tableau **(1.2)** présente les plus essentiels **[11]**:

réseau sans fil cellulaire	réseau sans fil ad hoc
avec infrastructure	sans infrastructure (Infrastructureless)
Stations de base fixes et pré-localisées	Pas de bornes d'accès ou de concentration (stations de base ou points d'accès)
topologie statique de réseau backbone (réseau cœur)	topologies très dynamique et multi-saut (multihop) de réseau
Environnement relativement occupé et une connectivité stable	Environnement hostile (bruit, pertes) et une connectivité irrégulière
planification détaillée avant que la station de base puisse être installée	réseau se forme automatiquement et s'adapte aux changements
Installation coûteuse et lente	Installation rapide et de coût faible

Tableau 1.1: Différences entre les réseaux sans fil cellulaires et ad hoc.

4.2 Applications des réseaux ad hoc

Les réseaux ad hoc sont utiles dans de nombreux cas de figure **[10, 11, 12]**:

- Initialement, les réseaux ad hoc sont introduits pour les applications militaires afin d'accomplir des missions temporaires et la gestion du champ de bataille. Dans ce cas, un réseau ad hoc peut être formé entre les soldats sur le terrain ou des avions de chasse dans l'air.
- Ils peuvent également être utilisés pour fournir des applications de gestion des services de crises ou pour coordonner les secours en cas de catastrophe là où les moyens (infrastructure) de communication sont inexistants ou détruits par des forces naturelles (tremblement de terre, cyclone…) et le recours à une communication rapide est cruciale.
- Ils permettent aussi de mettre en place, dans un laps de temps restreint, dans des espaces publiques peu équipés en infrastructures de communication lourdes (aéroports, hôtels, gars, salle de conférence, classe…) ou pour couvrir des événements sociaux comme les conférences scientifiques (un meeting avec un très grand nombre de participants) ou des réseaux de communication de groupe qui supportent des applications collaboratives (un jeu multi-joueurs, commerce mobile « m-commerce»…).

- Le réseau ad hoc est utilisé « d'une façon opportuniste » pour étendre un réseau domestique ou un réseau de campus à des zones difficilement accessibles ou inaccessibles par les réseaux cellulaires traditionnels de sorte qu'un terminal situé en dehors d'une cellule peut se connecter à une machine d'un autre utilisateur couverte par la cellule.
- Récemment, l'introduction des nouvelles technologies, comme le Bluetooth, IEEE 802.11 ou WiFi et Hiperlan, aide au déploiement commercial des réseaux ad hoc en dehors du domaine militaire. Pratiquement, Bluetooth est conçu pour supporter un réseau personnel (PAN) sans fil entre divers équipements. Tandis que la norme IEEE 802.11 la formulation d'un réseau ad hoc en l'absence d'un point d'accès sans fil (le mode de fonctionnement « ad hoc »).

À l'instar, des autre types des réseaux ad hoc qui sont émergés comme des applications très utiles tels que :

- Les réseaux de capteurs sans fil **(sensor network)** qui sont constituent de nœuds qui recueillent et transmettent des informations autour l'état de l'environnement physique ;
- Réseaux sans fil mailles **(mesh network)** ;
- Réseau de véhicules VANET (**vehicular area network**) qui pourrait être formé indépendamment de l'emplacement des véhicules. L'objectif fondamental est de trouver des informations locales pertinentes à proximité, comme les stations de gaz et des restaurants.

L'émergence des multiples applications des réseaux ad hoc évolue l'accès à l'information de « **n'importe quand**, **n'importe où** » à « **tout temps**, **partout** », dans le but de rendre possible la mise en place très rapide, partout et en tout temps, d'un réseau de communication.

4.3 Insuffisances des réseaux ad hoc

Les réseaux ad hoc ont de nombreux avantages indéniables (auto-configuration, adaptabilité, extensibilité…), mais aussi un certain nombre d'écueils en raison de la mobilité des nœuds couplée avec la capacité de diffusion locale.

Additionnement à l'absence d'infrastructure fixe et leur caractère multi-saut, ces réseaux héritent les problèmes traditionnels des réseaux sans fil qui sont liés étroitement à la qualité du signal propagé (support de transmission). Les principaux problèmes sont **[7, 10, 11, 12]**:

- **Débit plus faible que celui du monde filaire:** la bande passante est une ressource rare, cette limitation est un résultat du nombre restreint de fréquences et de canaux disponibles, et l'affaiblissement du signal dû aux conditions du milieu de propagation. Ainsi, les algorithmes et les protocoles doivent utilisés efficacement la bande passante disponible.

- **Limitation de la puissance et de la portée de transmission:** la puissance du signal diminue avec la distance, les évanouissements (ou fadings) et les atténuations tout en affectant d'autant l'asymétrie d'un lien (lien asymétrique).
- **Interférences et collisions:** les liens radios ne sont pas isolés, deux transmissions simultanées sur une même fréquence ou en utilisant des fréquences proches peuvent interférer au niveau de la réception (cas des fréquences utilisées dans la bande ISM). En outre, la complexité de gérer la concurrence d'accès à l'interface radio qui est partagée mène à la collision au niveau de récepteur et pose le problème de redondance. Ces deux phénomènes s'ajoutent au bruit et accroissent le nombre d'erreur sur la transmission et amoindrissent d'autant les performances d'un lien radio.
- **Taux élevé d'erreur:** la perte des paquets parvenu due aux erreurs de transmission radio (plus fréquentes que dans les réseaux filaires), à la mobilité et au problème d'énergie.
- **Vulnérabilité à la congestion du réseau:** due à la capacité naturelle de diffusion (broadcast) du l'interface radio sans fil.
- **Mobilité et topologie dynamique:** au contraire des réseaux fixes, où les changements de route surviennent à la suite d'une congestion dans le réseau ou d'une panne chronique, la tracé des route est modifiée assez fréquemment à cause de la mobilité imprévisible et arbitraire des nœuds, et notamment les nœuds intermédiaires, qui mène à la disparition ou l'apparition d'un lien entre deux nœuds, ou même lorsque la batterie est épuisée ou une panne survient tout en rendant la topologie de réseau dynamique.
- **Consommation d'énergie:** les réseaux ad hoc peuvent posséder uniquement des terminaux mobiles. Son problème principal concerne leur batterie, qui n'a généralement que peu d'autonomie. Sachant qu'un terminal consomme l'énergie pendant la transmission et pour maximiser sa durée de vie, il faut économiser autant que possible les transmissions inutiles.
- **Sécurité:** les réseaux ad hoc sont généralement plus vulnérables aux attaques et aux menaces de sécurité physiques que les réseaux avec infrastructure ou les réseaux filaires. La capacité des intrus de l'écoute et le spoofing de canal et les récepteurs passifs d'espionner les communications radio doit être soigneusement considérée.
- les problèmes du terminal caché ou exposé et l'hétérogénéité des équipements mobiles

Ces contraintes mettront des difficultés et autant des défis en face du développeur, et certaines problématiques de recherche à résoudre que nous allons explorer dans la section suivante.

4.4 Défis et problématiques de recherche

Les réseaux ad hoc posent de nombreuses problématiques du fait de ses caractéristiques. La principale d'entre elles est le routage nécessaire pour transférer les paquets d'un point à un autre point du réseau. L'un des objectifs du groupe MANET est de proposer une solution à ce problème. Parmi les autres problèmes, nous allons mentionner les suivantes :

a- L'accès au media

Contrairement aux réseaux cellulaires, il ya l'absence d'administration centralisée et la synchronisation globale dans les réseaux sans fil ad hoc. Par conséquent, les systèmes TDMA et FDMA ne sont pas adaptés. En plus, puisque les mêmes médias sont partagés par plusieurs nœuds mobiles, l'accès au canal commun doit être fait de manière distribuée, grâce à un protocole de contrôle d'accès au média MAC (Media Access Control). Ce protocole doit assurer l'accès au média tout en évitant d'éventuelles collisions avec des nœuds voisins. La présence de la mobilité, les problèmes des terminaux cachés et exposés doivent être pris en compte quand il s'agit de concevoir des protocoles MAC pour les réseaux sans fil ad hoc.

b- Le support de multicast

Le multicast ou multidiffusion est une forme particulière de diffusion (diffusion multipoint ou de groupe) d'une seule copie de messages à partir d'une source à des multiples destinataires, identifiées par la même adresse du groupe, au même temps. Ceci réduit considérablement le nombre des messages transmis, en fournissant un service de communication qui supporte les communications de groupe en termes de l'utilisation efficace des ressources de réseau **[12]**.

Dans le contexte des réseaux ad hoc, les utilisateurs se communiquent généralement de façon collaborative pour accomplir une mission critique, comme les pompiers dans une mission de recherche et secours. Ces applications nécessitent des communications de groupe afin d'utiliser efficacement les ressources limitées disponibles (bande passante et énergie). Cette nécessité peut être satisfaite naturellement par les communications multicast en motivant notamment le support de multicast dans les réseaux ad hoc **[10]**.

Le routage multicast est un sous problème de routage qui se relève lors du support de multicast. Dans ce contexte, la mobilité accrue des nœuds de réseaux ad hoc, en particulier les nœuds jouant le rôle des routeurs, ne permet pas d'adopter les protocoles de routage multicast pour les réseaux filaires, qui suggèrent l'immobilité des nœuds du réseau, ou même pour les réseaux sans fil avec infrastructure-fixe, qui ont basés sur des nœuds routeurs fixes.

Ainsi, les protocoles sus-indiqués construisent un arbre multicast comme une structure de distribution multicast, qui est moins adaptée pour la topologie dynamique des réseaux ad hoc du fait qu'elle soit fragile et demande beaucoup de reconfiguration à chaque changement de connectivité. Ceci augmente l'échange des messages de contrôle en consommant indésirablement les ressources dans un environnement de bande passante limitée et d'énergie restreinte.

Dans cette optique, il faudra proposer des nouveaux protocoles de routage multicast qui doivent considérer la durée limitée des batteries des équipements mobiles ainsi que les ressources limitées du réseau **[11]**. En effet, le routage multicast dans les réseaux ad hoc devenu un sujet de recherche actif où plusieurs recherches ont porté sur la conception des protocoles de routage multicast **[41 ,42]**.

Par nature, les communications sans fil entraînent un certain nombre de problèmes n'ayant pas d'équivalence dans le monde filaire. Parmi eux, les taux élevés d'erreurs rencontrés davantage dans les réseaux ans fil ad hoc résultant la perte des données. Cependant, additivement au routage multicast efficace, certaines applications multipoint déployées au sein de ces réseaux nécessitent la livraison fiable (la garantie de la délivrance sans erreurs et sans pertes) des données acheminées à tous les membres du groupe. Par conséquent, la fiabilité des communications multicast (en anglais « **Reliable multicast** ») est une exigence primordiale.

Malheureusement, les protocoles développés de multicast fiable, pour les réseaux fixes ou même les réseaux sans fil avec infrastructure, ne sont pas appropriés dû aux contraintes limitatives caractérisant les réseaux ad hoc. Par conséquent, il est nécessaire de développer des protocoles robustes et efficaces, quant à l'utilisation des ressources rares disponibles (éviter les retransmissions intitules), garantissant le passage à l'échelle d'un grand nombre de récepteurs.

Malgré les propositions qui ont étudié les problèmes du **routage** et de **la fiabilité**, le multicast demeure toujours une problématique complexe dans les réseaux ad hoc **[11]**.

c- La mobilité et la mise à l'échelle (scalabilité)

Dans certaines applications (par exemple, les réseaux de capteurs, les applications militaires dans un champ de bataille, les grilles de véhicules urbains…), le réseau ad hoc peut atteindre plusieurs milliers de nœuds. Pour les réseaux sans fil avec infrastructure (réseaux cellulaires), la scalabilité est simplement manipulée par une construction hiérarchique. Dans tels réseaux, la mobilité limitée aux terminaux peut également être facilement manipulé en utilisant des techniques de transfert intercellulaire (handover) ou IP Mobile **[8]**.

En revanche, en raison de l'extension de la mobilité au réseau lui-même et du manque d'une infrastructure fixe, les réseaux ad hoc ne tolèrent pas IP mobile ou une structure hiérarchique fixe. Ainsi, la mobilité, conjointement avec le passage à grande échelle est l'un des défis les plus importants dans la conception des réseaux ad hoc **[10]**.

d- La sécurité

La sécurité est devenue une nécessité clé pour assurer une communication protégée entre les nœuds mobiles dans un environnement hostile. Cette nécessité est cruciale dans les réseaux sans fil, et notamment dans les réseaux ad hoc, qui sont généralement plus vulnérables aux menaces de sécurité que les réseaux filaires. Avec la capacité de diffusion des canaux sans fil, les intrus ont la possibilité d'écouter les messages circulés et même d'attaquer (de façon active ou passive) le réseau et injecter des virus tout en perturbant son fonctionnement (par exemple, réintroduit les paquets de contrôle faux, endommagé les tables de routage, refuse de service…). Cependant, l'absence d'infrastructure rend les solutions classiques de la sécurité basant sur les autorités de certification et les serveurs en ligne inapplicables. Ainsi, la défense contre ces attaques nécessite des nouvelles techniques puissantes de cryptage qui doivent prendre en considération l'utilisation efficace et la variété des ressources disponibles (bande passante, énergie, CPU, mémoire…) **[11]**.

5. Conclusion

Le présent chapitre a présenté succinctement le problème d'interconnecter des équipements terminaux pour transporter des données numériques tout en recourant à des technologies sans fil. La prolifération des équipements mobiles puissants et l'avènement de la technologie sans fil conduisent à la naissance d'une nouvelle classe de réseaux sans fil sans infrastructure, les réseaux ad hoc.

Les réseaux ad hoc peuvent s'organiser arbitrairement pour former un réseau temporaire sans aucune infrastructure préexistante. En raison de leurs limitations (énergie, mobilité, bande passante), le support des communications multicast reste une problématique de recherche en termes d'acheminer et d'assurer une livraison fiable de données aux multiples récepteurs.

Le chapitre suivant présentera un état de l'art autour des approches développées pour répondre à la problématique de la fiabilité des communications multicast, particulièrement, dans le réseau IP filaire « Internet », qui sert comme une référence pour l'adoptation des approches existantes dans d'autres cas de réseaux (réseaux sans fil, réseaux satellites…).

Fiabilité multicast: état de l'art

CHAPITRE 2

1. Introduction

La progression et le large déploiement des technologies des réseaux de communications fournissent un environnement vital pour l'émergence d'un nouveau type d'applications impliquant un groupe de participants dans la communication (communication multipoint).

En fait, le service de communication multicast fournit une solution naturelle aux facteurs limitatifs de solution point-à-point, en termes d'utilisation de ressources et la mise à l'échelle, bien qu'il supporte efficacement les communications multipoint.

Afin de supporter les communications multicast, un modèle de service réseau **multicast IP** a été proposé, avec le travail de Deering (1980) **[13].** Dans ce modèle, la mission d'une couche réseau et d'offrir un service de livraison multicast de trafic généré sans aucune garantie de sa fiabilité. Cette fiabilité est une condition primordiale exigée par les applications multipoint. Par conséquent, la conception des protocoles de niveau supérieur (transport), qui offre un service de communication multicast fiable, devient un objectif crucial.

Dans le présent chapitre, nous allons aborder le problème de la fiabilité des communications multicast au niveau dés réseaux à base IP, notamment le réseau Internet. D'abord nous présenterons le support de multicast, puis un état de l'art autour des approches de la fiabilisation du multicast, dans les réseaux de communication en générale, et réseau Internet en particulier.

2. Communication de groupe (communication multipoint)

À l'opposition des applications point-point, des nouvelles applications, où un groupe de participants s'intéressent par les données échangées, sont désormais émergées avec le large déploiement des technologies des réseaux de communications. Ces dernières nécessitent des communications de groupe (multipoint) où une ou plusieurs sources peuvent envoyer des données aux multiples récepteurs (communication **one-to-many** ou **many-to-many**).

Dans un réseau de communication, une communication multipoint peut être effectuée de trois façons différentes **[14, 15, 16]**:

- **Communication unicast :** à l'instar de la communication traditionnelle point-à-point qui implique seulement deux parties (une source, un récepteur), ce type de communication est basé sur les transmissions point à point où la source transmit un paquet unicast destiné à un seul récepteur. ces paquets sont généralement acheminés, par les routeurs, de la source jusqu'à l'arrivé de proche en proche au récepteur concerné.

Comme montre la figure **(2.1(a))**, le support de la communication de groupe par le biais d'une communication unicast nécessite l'ouverture simultanée de plusieurs connexions unicast et aussi l'envoie simultané des plusieurs copies de paquet autant des récepteurs (membres de groupe). Cependant, cette solution exige que la source doit connaître les identités de tous les récepteurs, ceci ne pas faisable pour un groupe de taille important tout en limitant le facteur d'échelle (la scalabilité). En outre, plusieurs copies de la même donnée peuvent être circulées sur les mêmes liens. Cette duplication consomme de façon indésirable les ressources du réseau (la bande passante) et gaspille la capacité du traitement de source (dû à la réplication des données). Par conséquent, les performances du réseau pourront dégradées, notamment avec la présence d'un nombre important de récepteurs.

- **Communication broadcast :** un type de communication point-à-multipoint où, contrairement à la communication unicast, une communication broadcast se repose sur une transmission point-à-multipoint de sorte que la source diffuse une seule copie de message à tous les nœuds impliquant toutes les parties du réseau (voir la figure **(2.1(b))**).

Cette solution s'avère plus convenable pour supporter une communication de groupe qu'une transmission point-à-point (en unicast). Sachant qu'un petit groupe s'intéresse par la réception, la diffusion dans un réseau large portée consomme une quantité excessive de ressources.

- **Communication multicast :** cette communication implique plusieurs parties de réseau et traite des communications point-à-multipoint (one-to-many) ou communications multipoint-à-multipoint (many-to-many) où une seule ou plusieurs sources transmettent en mode multicast des paquets multidestinataires destinés à un groupe constitué d'au moins deux récepteurs. Comme montre la figure **(2.1(c))**, la source diffuse une seule copie de son trafic à un groupe de récepteurs (diffusion sélectif). Cette copie sera acheminée par le réseau qui va la répliquer de façon optimale aux endroits où le chemin vers les destinataires diverge.

Par rapport aux modes des communications (unicast et broadcast), une communication multicast peut fournir un support efficace pour les communications de groupe où elle évite la réplication au niveau de la source et l'ouverture simultanée de plusieurs connexions avec une utilisation efficace de ressources de réseau (seulement $^{1}/_{\text{nombre de récepteurs}}$ de bande passante est requise). Ceci peut améliorer les performances de réseau, permettre le passage à l'échelle en termes de nombre de participants, réduire les coûts de transmission et augmenter la vitesse du transfert.

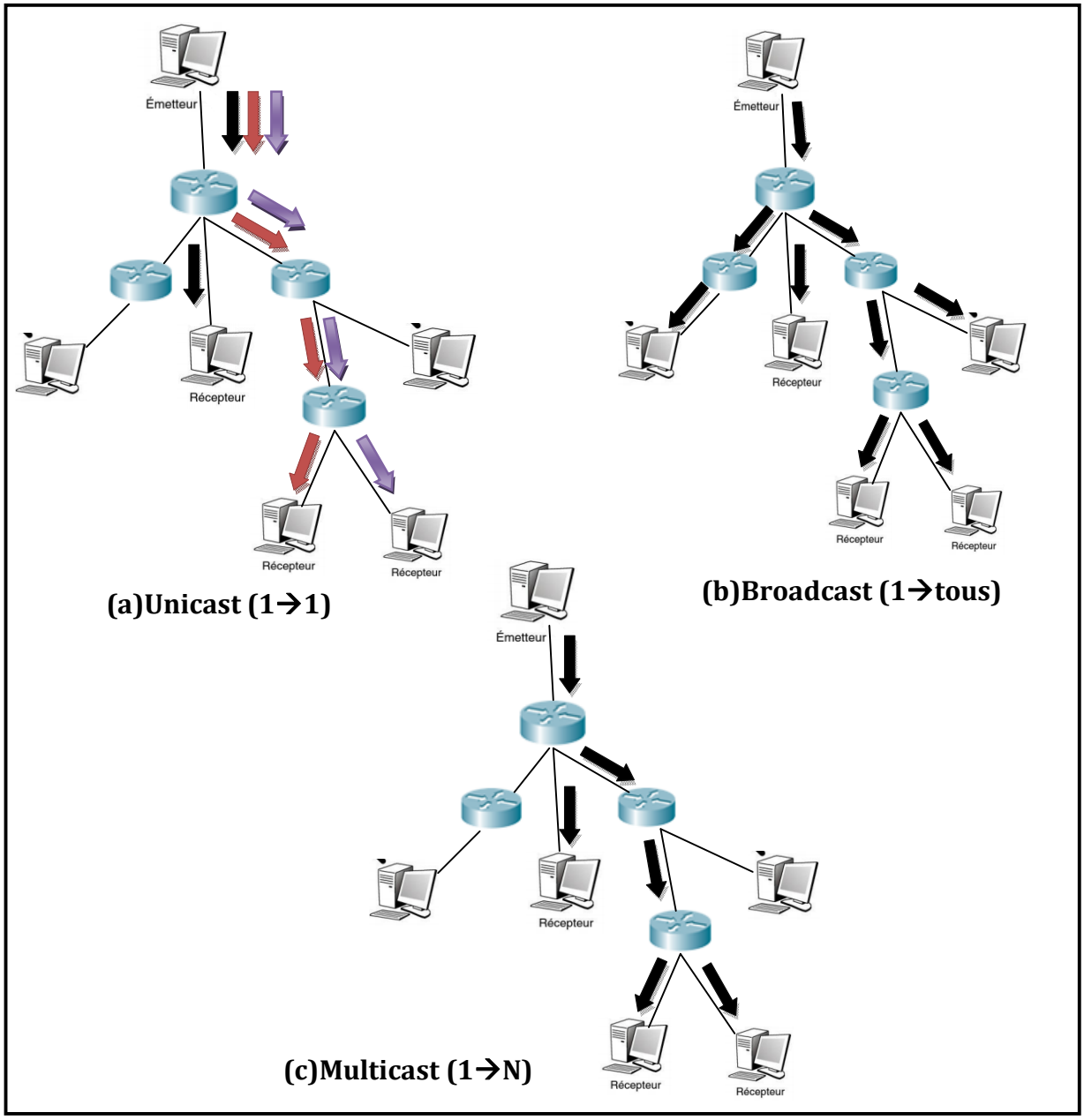

Figure 2.1: Schémas de communication multipoint.

En premier lieu, les applications multipoints restent brisées d'être largement déployées dans les réseaux et particulièrement les réseaux IP, du fait du facteur limitatif de la scalabilité des communications point-à-point dominantes et l'absence de support pour les communications multipoints (modèle de référence OSI point-à-point, architecture TCP/IP point-à-point). Cependant, cette situation a été changée avec le travail de Deering **[13]** vers la fin des années quatre vingt où il est proposé un modèle de service multicast afin de supporter les communications multipoints dans les réseaux IP (Internet). Cette proposition ouvre la voie à la généralisation de ce support dans les réseaux de communication, que nous allons traiter dans la section suivante.

3. Support du multicast dans les réseaux de communication

Comme nous avons traité dans la section précédente, le multicast a prouvé ses capacités étonnantes d'économiser, par rapport à l'unicast et le broadcast, des précieuses ressources de bande passante et des capacités réseaux, tout en évitant la réplication et l'ouverture simultanée de plusieurs connexions. En effet, il s'avère donc plus avantageux non seulement pour les utilisateurs des applications multipoints, mais aussi pour le réseau de transport.

Pour qu'un réseau supporte une communication de groupe, il vaut offrir un service de groupe, précisément un service multicast. Pratiquement, la fourniture du service de communication multicast à usage général et efficace implique multiples fonctionnalités à plusieurs couches de l'architecture générique des réseaux de communication. La figure **(2.2) [14, 17]** ci-dessous illustre les couches et les fonctionnalités impliquées.

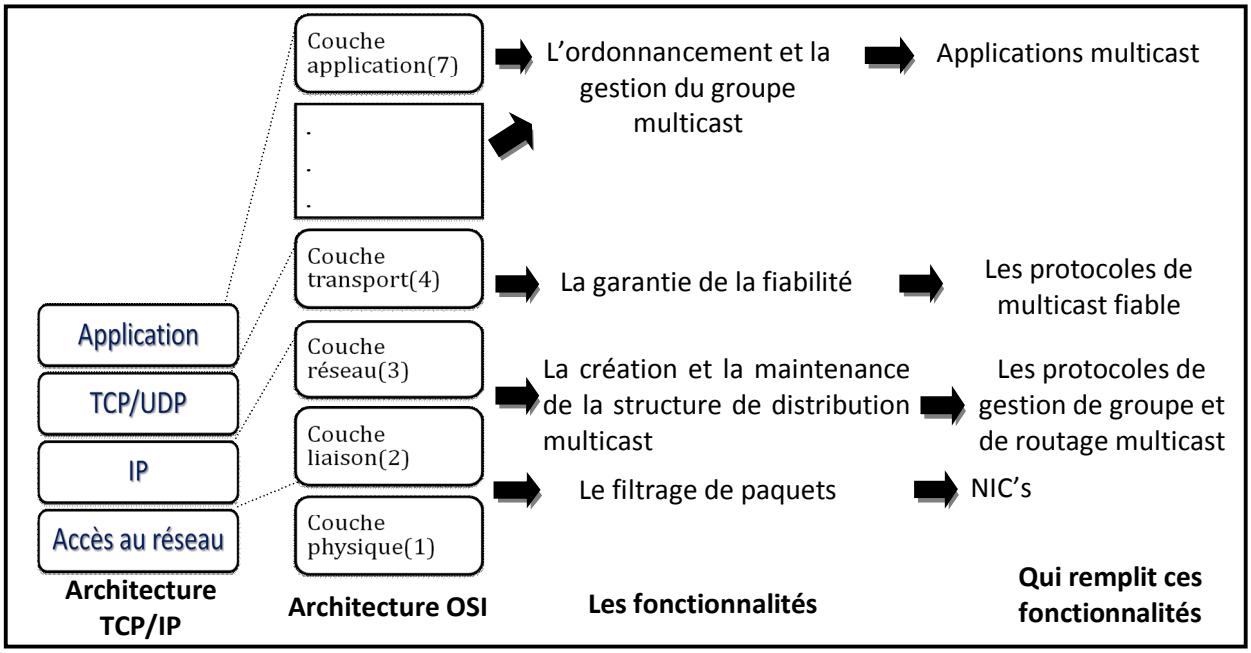

Figure 2.2: Couches et fonctionnalités impliquées par un service multicast.

Au minimum, un service multicast devrait offrir plusieurs fonctionnalités de base **[19]**:

- Gestion de l'appartenance au groupe ;
- Maintenance des chemins de distribution de données ;
- La réplication et la transmission de contenu ;
- La congestion et le contrôle d'erreur.

L'objectif est de satisfaire les utilisateurs, les opérateurs de réseau et les fournisseurs de contenu. L'offre de ces fonctionnalités implique multiples couches comme suit :

- **La couche liaison de données :** la couche liaison de données offre un support matériel au service multicast où ses deux fonctions essentielles se rapportent à l'adressage de groupe. La première fonction est principalement implémentée au niveau de la sous couche MAC dans les réseaux multi-accès, où les protocoles d'accès au médium partagé ont la possibilité de distinguer les adresses physiques de groupe (adresse physique multicast). De même, à l'aide de la fonction de filtrage des paquets « multicast filters », l'adaptateur réseau (NIC) peut délivrer, au hôte appartient à un groupe donné, les trames MAC avec l'adresse physique de groupe approprié. En voici quelques réseaux offrant ce support : **Ethernet**, **Token Ring**, **Token Bus** et **FDDI** (Fiber Distributed Data Interface),

- **La couche réseau :** afin de supporter des communications multicast au niveau de la couche réseau, trois mécanismes complémentaires doivent être définis et mis en œuvre **[15] :**
  - Adressage : pour communiquer avec un groupe de récepteurs, il vaut avoir une adresse de groupe (adresse multicast) permettant d'identifier l'ensemble de destinataires faisant partie de ce groupe. De plus, il doit y avoir un mécanisme pour qu'une adresse multicast logique et l'adresse multicast physique correspondante, de la couche liaison, puissent s'associer.
  - Enregistrement dynamique : pour qu'un réseau puisse savoir quels sous-réseaux ont besoin de recevoir le trafic d'un groupe multicast, il doit avoir un mécanisme de gestion de groupe permettant à des terminaux de joindre ou de quitter dynamiquement ce groupe.
  - Routage multicast : en plus des adresses et gestion de groupe, la couche réseau doit offrir un support de routage pour les groupes où le réseau doit de construire des structures de distribution multicast permettant aux sources d'envoyer des paquets vers tous les membres de groupes identifiés par l'adresse de groupe. Ceci est basé sur les informations collectées par le protocole de gestion de groupe.

  En outre, ces mécanismes doivent être adaptés au type des liaisons fournies dans la couche liaison, à savoir: liaisons point-à-point, liens de diffusion (Ethernet, WLAN) et liens d'accès multiples sans diffusion(ATM) où le service multicast peut profiter les avantages de la diffusion fournie naturellement par certains réseaux **[19].**

- **La couche transport :** le transport multicast fiable ajoute des garanties, pas nécessairement comme le TCP unicast fiable, au modèle de livraison de groupe où il garantit la livraison fiable de données transmises en multicast sur les structure de distribution construites par des protocoles de routage multicast de niveau réseau. Additionnement aux : contrôle d'erreur, contrôle de flux et de congestion, il garantit aussi certains types d'ordonnancement.

- **Les couches supérieures :** pour certains protocoles, plusieurs aspects liés à la fiabilité sont manipulés au dessus de la couche de transport. L'ordonnancement et la gestion de groupe, par exemple, peut être assurés par les couches supérieures, qui ont également la capacité de recouvrir les pertes et de contrôler le flux. On parle ainsi du **Multicast applicatif.**

3.1 Multicast dans le réseau Internet

Dans le contexte d'Internet, le support des communications multipoints a été initialement introduit avec le travail de Deering (1980) (**RFC 1112**) **[13]** par la définition d'un modèle de service **multicast IP** intégré au niveau réseau, qui se base sur le protocole IP sans altérer le modèle générale du réseau Internet. Le multicast IP offre un service de groupe efficace, permet la gestion des membres des groupes et la livraison d'informations. Donc, il répond aux exigences d'un service multicast générique, notamment dans les points suivants **[15, 20]**:

- **Adressage multicast :** l'identification du groupe est répandu par une adresse multicast IP (de niveau réseau), ou adresse de groupe, qui désigne un groupe arbitraire de terminaux IP pouvant recevoir le trafic émis vers lui. L'attribution des adresses multicast IP est contrôlée par l'IANA (Internet Assigned Numbers Authority), qui réserve la plage d'adresse [224.0.0.0, 239.255.255.255], de la classe D, pour les communications multicast. Cette adresse peut être: une adresses statique, dynamique, permanente, temporaire, privée ou publique. Pratiquement, la source envoie des datagrammes multicast, avec une adresse source unicast et une adresse destination multicast IP, vers les membres du groupe identifiés par cette adresse. La figure **(2.3)** représente le format d'une adresse multicast IP **[15]**.

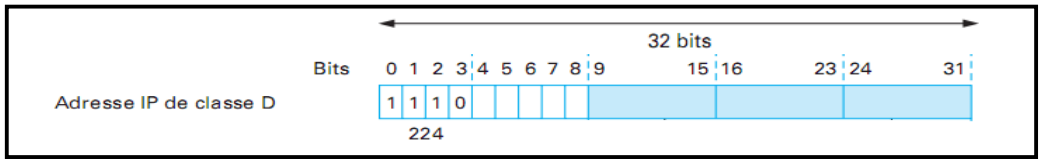

Figure 2.3: Format des adresses multicast IP.

Il existe aussi des adresses Ethernet multicast (adresses MAC physique) qui désignent un groupe dynamique d'équipements physiques au niveau liaison. Pour que les trames Ethernet multicast puissent être traitées et aiguillées (filtrage multicast), il est nécessaire de:

- distinguer les adresses Ethernet multicast et unicast : les adresses MAC Ethernet utilisent alors un champ OUI réservé spécifiquement pour les adresses multicast IP ;
- traduire et associer à toute adresse multicast IP (logique) une adresse Ethernet multicast (physique) correspondante.

La figure (**2.4**) illustre la correspondance entre adresse IP et adresse Ethernet multicast **[15]**.

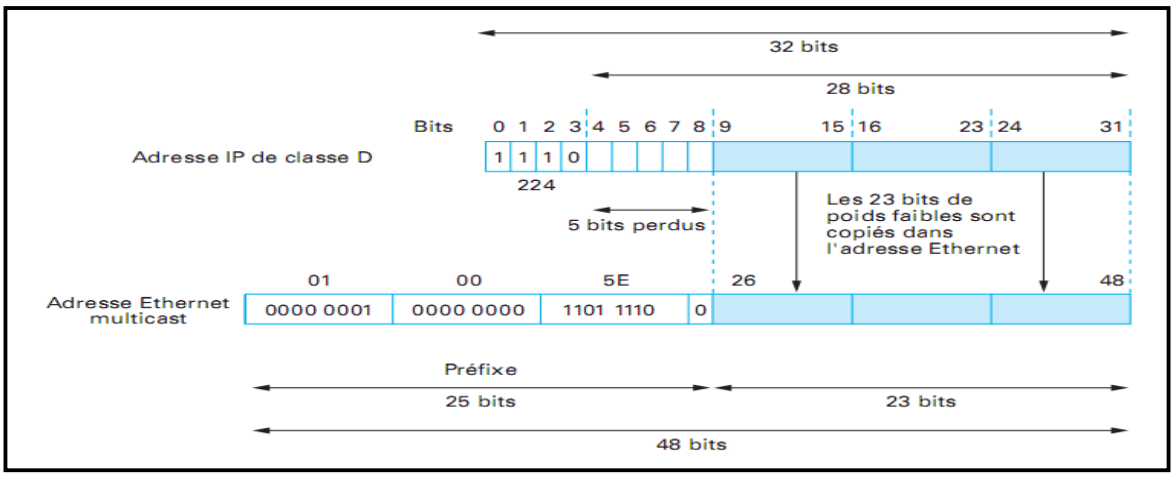

Figure 2.4: Correspondance entre adresse IPv4 et adresse Ethernet multicast.

- **Gestion d'adhésion aux groupes :** le multicast IP est basé sur la notion du groupe. Un récepteur donné doit souscrire dans un groupe multicast, identifié par une adresse multicast, pour qu'il puisse recevoir le trafic destiné à lui. Pour cela, un protocole de la gestion de groupe est nécessaire pour permettre aux hôtes de joindre ou quitter un quelconque groupe multicast de façon dynamique, et informer le routeur multicast local de l'existence d'un ou de plusieurs récepteurs appartenant à un groupe derrière chacune de leurs interfaces. Ce groupe n'a pas de limite : physique ou géographique où les terminaux multicast peuvent être localisés sur n'importe quel sous-réseau de l'Internet ; numérique où la taille d'un groupe multicast peut varier d'un seul terminal à tous les terminaux du réseau Internet.

Les protocoles de gestion de groupe multicast les plus utilisés dans le contexte d'Internet sont : le protocole **IGMP** (Internet Group Management Protocol) **[13]** en IPv4 et le protocole **MLD** (Multicast Listener Discovery) **[21]** en IPv6.

- **Routage multicast :** une fois le groupe multicast est formé, il est désormais d'acheminer le trafic multicast vers les membres dispersés dans le réseau. Ceci nécessite une fonction de routage de groupe qui suite un ensemble de chemins partant généralement de la source. Cette tâche délicate est à la responsabilité du protocole de routage multicast, qui est fondé sur un algorithme de routage multicast afin de construire l'arbre de distribution multicast reliant les membres de groupe. Ceci en se basant sur les informations collectées et fournies par le protocole de la gestion de groupe. Les protocoles de routage multicast peuvent construire des **arbres spécifiques à une source** ou des **arbres partagés,** et peuvent être en **mode épars** ou en **mode dense**. Au niveau de la littérature, plusieurs protocoles de routage multicast Internet ont été développés, les protocoles: **PIM**(Protocol Independant Multicast) **[22]**,

MOSPF(Multicast Open Shortest Path First) **[23]**, **CBT**(Core Based Trees) **[24]** et **DVMRP**(Distance Vector Multicast Routing Protocol) **[25]** sont les plus cités.

La couche réseau basée sur le multicast IP, qui est une extension de service datagramme unicast IP, offre un service de délivrance one-to-many ou many-to-many à moindre effort sans aucune garantie sur la livraison fiable de données. En effet, certaines applications multicast, qui ne peuvent tolérer la perte de quelques données, restent peu satisfaites par le service fourni et exigent, toute fois, un service multicast fiable au dessus du multicast IP. Cette fiabilité devenu indispensable et fait appel aux mécanismes de multicast fiable dans les couches supérieures, que nous allons détailler par la suite.

4. Multicast fiable dans les réseaux de communication

Le souci de la couche réseau est de fournir un support efficace pour un grand nombre d'applications multicast, où elle assure un service de délivrance au mieux (best effort delivery). En revanche, certaines de ces applications, en plus de l'efficacité de routage, nécessitent des services supplémentaires, et en particulier la fiabilité des échanges. En fait, la fiabilité des communications multicast est liée forcement aux divers exigences de ces applications.

4.1 Exigences des applications

Les exigences des applications pour le multicast fiable sont largement variées que les applications elles-mêmes, les plus essentielles sont (**RFC 2357) [26, 27] :**

- Certaines applications peuvent tolérer la perte de quelques données tandis qu'elles exigent des délais restrictifs de livraison, une délivrance avec un délai borné "Time-bounded Delivery".
- Certaines applications sont peu sensibles à la contrainte de temps, mais elles exigent une fiabilité (totale ou partielle) de délivrance.
- Certaines applications exigent la confirmation de la délivrance à tous les récepteurs.
- Certaines applications impliquent plusieurs sources des données tandis que d'autres ont une seule source de données. Cette exigence soulève une question concerne la robustesse des mécanismes multicast fiable sous-jacents avec un nombre important d'expéditeurs.
- Certaines applications nécessitent que la livraison de message obéir à un ordre total tandis que d'autres ne le font pas.

Avec la multitude des exigences, le problème de la fiabilité des échanges apparaître plus complexe à traiter en communication multicast qu'en communication point-à-point (unicast).

4.2 Fiabilité des communications multicast

4.2.1 Définition de la fiabilité

Selon la définition traditionnelle **[14]**, un service fiable se réfère à la transmission, dans l'ordre correct, sans erreurs et sans duplications, de toutes les données en disposant à l'application un canal de communication sans pertes, ni erreurs de transmission.

Néanmoins, l'association de la fiabilité avec un service multicast implique une extension de cette définition. Dans le contexte des environnements multicast, le large sens de 'la fiabilité' comprend les trois aspects suivants **[11]**:

- **La délivrance sans erreur :** la délivrance sans erreur se réfère à la livraison éventuelle de toutes les données à tous les récepteurs.
- **L'atomicité:** l'atomicité garantie que tous les récepteurs ou aucun d'entre eux reçoivent le message. Il peut être réalisé en veillant à ce que « une fois un membre (la majorité) de groupe délivre un message, le reste du groupe doit délivrer le message dans un temps court ».
- **L'ordonnancement:** les types d'ordre pour un service multicast fiable sont **[17, 11]**:
  - Un ordre global : toutes les données de tous les expéditeurs sont livrées à tous les récepteurs dans la même séquence correcte et même ordre général.
  - Un ordre par source : les unités de données provenant d'une source sont livrées au récepteur dans le même ordre qu'ils ont été émis par cette source. Il n'ya pas de règle d'ordonnancement spécifié entre les unités de données transmises depuis plusieurs sources.
  - Un ordre total : précise que de multiples flux multicast provenant de plusieurs expéditeurs sont livrés de façon séquentielle à chaque récepteur et sont reçus dans le même ordre relatif à chaque récepteur.
  - Un ordre causal : ce qui maintient une estampille pour les relations de précédence entre les messages multicast.

4.2.2 Niveaux de fiabilité

Grâce à la multiplicité des applications, on peut distinguer plusieurs niveaux de fiabilité **[19]**:

- **Fiabilité partielle (Best effort):** ce type de fiabilité est fourni par les protocoles de routage multicast ou de transport multicast avec mécanisme de recouvrement FEC, où aucune garantie de bonne livraison (sans erreurs et sans pertes) de toutes les données n'est assurée. Ce type est aussi exigé généralement par les applications tolérantes la perte de quelques données (les applications multimédia en temps réel comme exemple).

- **Fiabilité totale de niveau transport:** la mission naturelle des protocoles de transport est, en l'absence d'un problème de communication majeur, d'offrir un service de transmission totalement fiable (sans erreurs, sans pertes) de bout en bout. Autrement dit, ils garantissent la bonne livraison de toutes les données à tous les récepteurs, au dessus d'un service de livraison à moindre effort. C'est le type de service fourni dans la majorité des protocoles de transport multicast fiable définis par l'IETF. Les applications de transfert de fichiers sont un exemple pour les applications nécessitant une fiabilité totale;

- **Fiabilité totale de niveau Applicatif:** les services de fiabilité au niveau transport ne sont pas généralement suffisant pour obtenir le type de la garantie strict. Cependant, un niveau applicatif supplémentaire est utilisé afin de garantir la livraison de contenu vers le groupe de destinataires, même en cas de coupure prolongée de l'un d'entre eux (par exemple, en raison d'un problème de connectivité réseau). Généralement, une application dédiée sera utilisée.

4.2.3 Challenges de conception

Contrairement à l'unicast fiable, où un seul protocole de transport (TCP) est actuellement utilisé pour répondre aux besoins de livraison fiable d'un large éventail d'applications, un service multicast fiable ne peut répondre qu'aux besoins spécifiques d'applications qui ont des exigences différentes en matière de fiabilité. En outre, plusieurs points critiques, semblent des défis, mettent l'assurance d'un service multicast fiable une tâche difficile **(RFC 2887),** notamment **[19, 29]**:

- **la scalabilité:** il s'agit essentiellement la robustesse des mécanismes de multicast fiable lors du passage à l'échelle d'un nombre important de récepteurs.
- **Le contrôle de congestion:** en cas de congestion le trafic du multicast fiable, dans les sessions multicast, ne doivent avoir un impact négatif sur le reste du trafic sur le réseau et doivent permettre une partage équitable des ressources de réseau (un comportement équitable vis à vis des flux TCP dans le cas du réseau Internet).
- **L'hétérogénéité:** au sein d'un groupe important, les récepteurs ont une forte chance d'être largement hétérogènes en point de vue du réseau d'accès (bande passante, pertes et délai de transmission) et des capacités (énergie, CPU, mémoire).
- **La qualité de service:** le service fourni doit s'adapter aux caractéristiques du réseau afin d'obtenir la qualité du service de transport spécifiée par l'application.

- **La sécurité:** ce point est adressé par le groupe **SMUG** (Secure MUlticast Group) de l'IETF. La sécurité appliquée au multicast est encore plus complexe, qu'en unicast, du fait des problèmes de la dynamicité du groupe et l'anonymat des membres.
- **Faire face aux besoins très variées des différentes applications et de leur modèle de transmission:** streaming, à la demande, push, avec ou sans contraintes temps-réel. Une solution universelle, applicable partout, n'est donc guère envisageable.
- **Faire face aux différents modèles du groupe:** qui peuvent être : fermés (on connaît les membres fixes), semi-fermés (les membres sont connus mais évoluent dynamiquement), ouverts (on ne connaît ni le nombre ni l'identité des membres).
- **Contraintes de réseau sous-jacent:** les propriétés du réseau, dans lequel l'application est déployée, peut se contraindre la conception d'un service multicast fiable (le support des liens bidirectionnels pour les messages d'acquittements en feedback de la part des récepteurs). Néanmoins, dans certaines circonstances, il est possible que cette conception puisse s'appuyer sur certain degré supplémentaire d'aide à partir les éléments du réseau.

Afin d'aborder le problème de la fiabilité des communications multicast, la fourniture d'un service multicast fiable, par le biais des protocoles multicast fiable au niveau transport, pour supporter au mieux les différentes besoins des applications multipoint fiables déployées dans un réseau donné devient une exigence plutôt qu'une nécessité. Etant donné que le nombre de participants de telles applications se multiplie continuellement, ces protocoles doivent faire face aux problèmes, ci-dessous, liés au passage à l'échelle d'un grand nombre de récepteurs (scalabilité) pour qu'ils soient performants.

4.3 Enjeux de la mise à échelle du service de communication fiable

Dans la plupart des scénarios des communications de groupe, les applications exigeantes des services de communication fiable impliquent un grand nombre de participants. Dans ce contexte, le problème de la mise à l'échelle 'scalabilité' doit être traité, notamment avec un niveau élevé de fiabilité exigée.

La mise à l'échelle d'un protocole de transport multicast, assurant la fiabilité du service de communication, recouvre globalement sa capacité à accroître la taille du groupe qu'il est en mesure de gérer sans influence sur ses performances, pratiquement dans les deux aspects liés au mécanisme de contrôle d'erreur, comme montré ci-après **[19, 30]** :

- **La mise à l'échelle du trafic de contrôle:** cet aspect concerne le trafic du contrôle (signalisation) généré par le protocole, où les récepteurs envoient généralement des messages de contrôle à l'émetteur pour signaler l'état de la réception des données à leurs niveaux. Ainsi, l'émetteur risque d'être saturé par le traitement des demandes de retransmission ou même les acquittements positifs (proportionnels au taille du groupe) résultant toutefois un gaspillage de bande passante. De même, les liens sources risquent d'entrer en congestion. Ceci référence au problème de l'implosion des acquittements en feedback.

- **La mise à l'échelle des retransmissions:** avec un groupe de taille large, la retransmission en unicast de plusieurs copies du paquet demandé peut conduire ainsi à un trafic de réparation (proportionnel à la taille du groupe) non supporter par les capacités de la source et même du réseau (écroulement de la source, gaspillage de la bande passante), là où un nombre important de récepteurs demandent la retransmission du même paquet perdu (peut être tous les récepteur si la perte surgisse au niveau des liens sources) . Cependant, cette charge peut être allégée par la retransmission d'une seule copie de paquet perdu en multicast vers le groupe en entier. Néanmoins, la plupart des pertes de paquets ne sont pas corrélées, et différents récepteurs peuvent avoir différents taux de perte. Donc, le trafic de réparation destiné au groupe en entier et non localisé à ses récepteurs souhaités conduit au problème de la localité de réparation (localité de perte) avec le non objectivité de la consommation de bande passante.

4.4 Mécanismes de l'assurance de fiabilité

Pratiquement, pour assurer un transfert fiable de données, deux tâches principales sont requises : la détection et le recouvrement (la réparation) des erreurs ou des pertes. Ces deux tâches sont accomplies par les protocoles de niveau transport où ils implantent un mécanisme de contrôle d'erreurs, orientés par le niveau de fiabilité souhaité (totale ou partielle), permettant de récupérer éventuellement les pertes ou erreurs survenus dans une communication multicast. Le choix d'un mécanisme adéquat dépend grandement de la topologie du réseau sous-jacent et du service ciblé par le protocole de transport.

Les mécanismes populaires dans ce contexte, que nous exploiterons par la suite, sont **[18, 28]**: **ARQ** (Automatic Repeat Request) et **FEC** (Forward Error Correction) et parfois la combinaison de les deux (solutions hybrides).

4.4.1 Mécanisme des requêtes de retransmission (Automatic Retransmission Query)

Cette approche représente une forme de redondance temporelle qui consiste à la répétition des données dans une période de temps selon le schéma de retransmission 'à la demande'.
Son principe de fonctionnement est fondé sur les acquittements, positifs 'ACK' ou négatifs 'NACK', provenant de la part des récepteurs pour détecter ou signaler les pertes des données d'application, ou même l'état de la congestion du réseau.

Afin de détecter une situation de perte, deux classes peuvent être distinguées. Dans la classe « sender-initiated », la source a la responsabilité de détecter les paquets perdus, non acquittés positivement par au moins un récepteur, après un « time out ». Dans sa contrepartie, classe « receiver-initiated », chaque récepteur peut détecter la perte, proprement dite, sur: l'expiration d'un délai de garde, la réception d'un paquet altéré ou la découverte d'un saut dans les numéros de séquence des paquets reçus. Pour éventuellement récupérer les paquets de données perdus, des requêtes, comme un acquittement négatif (NACK), seront élaborées afin de les rapporter et demander leur retransmission à une source ou un autre nœud ayant des copies en cache. Ces requêtes peuvent être transmis en plusieurs modes, à savoir : point à point (unicast) où la requête est dirigée directement vers la source ou le responsable du sous-groupe (serveur local), apte à répondre; multipoint (multicast) vers le groupe en entier, pour assurer un recouvrement local par les récepteurs.

En plus, suite à la détection de la perte d'un acquittement positif (ACK) ou la réception d'un acquittement négatif (NACK), une phase de retransmission sera entamée et/ou un mécanisme d'évitement de congestion sera déclenché. Le schéma de retransmission peut être:

- **orienté-émetteur** (**Sender-oriented):** la source est la seule apte à retransmettre les paquets.
- **orienté-récepteur (Receiver-oriented):** implique les récepteurs dans la retransmission.
- **Router-assisted:** les routeurs actifs intervient dans la retransmission.

En outre, la retransmission peut être de point à point (unicast), où elle est dirigée directement vers le récepteur concerné individuellement, ou multipoint (multicast) pourvue qu'elle aille être reçue par le groupe en entier.

Ce mécanisme fournit une fiabilité totale, convient pour les applications non interactives et pour les réseaux avec une probabilité de perte hétérogène. En outre, il traite de façon efficace les pertes partagées.

4.4.2 Mécanisme de correction d'erreur d'expédition (Forward Error Correction)

Ce mécanisme est basé sur l'une de forme de redondance spatiale qui consiste à additionner des informations redondantes (code correcteur) aux paquets transmis, pour les utiliser dans la reconstruction des paquets perdus.

Pratiquement, les protocoles divisent les paquets originaux des données en des petits sous-paquets, puis ils ajoutent, à chacun, des informations redondantes permettant de reconstruire le paquet original. À la réception de nombre suffisant de ces sous-paquets (pas forcement le tous), le récepteur pourra reconstruire le paquet original des données à partir d'informations redondantes de sous-paquets bien reçu réassemblés.

Cette approche est principalement utilisée pour recouvrir les pertes indépendantes dans les réseaux à des pertes probablement homogènes. Elle réduit le nombre des retransmissions et fournit une livraison de court délai (attractive pour les applications interactives en temps réel). Néanmoins, elle reste assez utilisée à cause de l'importance du trafic réseau généré, le savoir des cas échéants de la perte pour produire les informations redondantes nécessaires, la mauvaise performance en cas de la congestion et la fourniture d'une fiabilité partiale.

5. Multicast fiable dans le réseau Internet

Le Multicast IP est un service réseau datagramme qui n'assure pas la délivrance fiable du trafic multicast exigée par les applications multicast fiables d'Internet. En fait, cette fiabilité peut être satisfaite par un protocole de transport multicast. Cependant, le développement d'un protocole de transport universel est contraint par le concept « **one-size-fits-all** » **[20]** et l'adaptation du protocole TCP de transport unicast fiable dans le contexte multipoint constitue un large problème. Comme montre la figure **(2.5) [16]**, les applications multicast d'Internet peuvent s'appuyer sur un protocole de couche de transport spécialisé opérant au-dessus d'UDP ou sur des protocoles de transport fiables opérant au dessus de la couche IP.

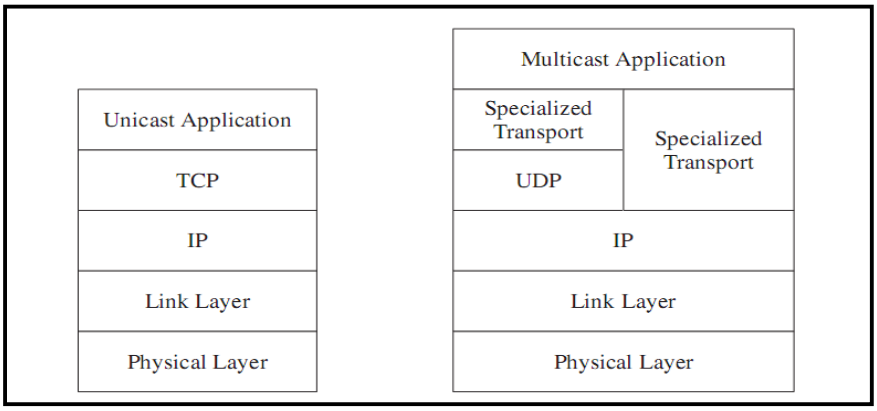

Figure 2.5: Pile de protocoles pour le transport fiable.

Dans ce contexte, IETF se préoccupe à la normalisation des travaux actuels dans le domaine des communications multipoints fiables **[30].** L'objectif du groupe de travail **RMT** (Reliable Multicast Transport) d'IETF est de proposer un standard concernant les protocoles de transport multicast sur Internet, où l'accent est met sur les protocoles de transport fables conçus pour diffuser les données d'une source vers un groupe de récepteurs (communication one-to-many).

Comme il existe de très nombreuses applications demandant un tel service avec des besoins variées, le RMT étudie la standardisation de deux familles de protocoles :

- Un protocole basé sur des acquittements négatifs (NACK Based protocol).
- Un protocole (Asynchronous Layered Coding protocol) utilisant le code correcteur FEC.

5.1 Approches du multicast fiable

Plusieurs protocoles de multicast fiable ont été développés pour l'Internet afin de garantir la fiabilité au niveau transport. La section suivante nous présente cette pluralité.

5.1.1 Taxonomie des protocoles de transport multicast fiable

Le but des protocoles de transport multicast fiable est de garantir la délivrance des données pour fournir un service de communication multicast fiable aux applications consommatrices. Cette fiabilité consiste à : détecter les pertes, puis de faire les recouvrir. En effet, les méthodes utilisées pour ce but, par la richesse des approches de multicast, peuvent être distinguées selon les points suivants : qui est le responsable de la détection des pertes?, comment les erreurs sont signalées ?, et comment les paquets perdus seront retransmis ? **[17]**.

Selon le **RFC 2887 [29],** la plupart de ces approches supportent un certain degré d'assistance de réseau sous-jacent tandis que d'autres ne la supportent pas. En effet, elles peuvent être classifiées en deux classes principales **[31]**:

- **Approches de bout-en-bout (ne support pas une assistance de réseau):** seulement les membres du groupe multicast, à les extrémités de réseau, peuvent être intervenus dans le processus de recouvrement, tandis que le réseau sous-jacent véhicule les données échangées dans la communication sans aucune contribution dans ce processus. Dans telles approches, la retransmission peut être dirigée par la source, ou être distribuée entre les récepteurs.

- **Approches basées sur le support du réseau*:*** relativement au degré d'assistance de réseau, deux classes d'approches peuvent être envisagées **[28, 29]** :

- **Approches basées sur serveur (Server-based):** des nœuds supplémentaires, autres que les expéditeurs ou les destinataires de trafic multicast, peuvent être utilisés pour aider à la livraison des données ou l'agrégation des acquittements en feedback. Ces nœuds doivent présenter sur la structure de distribution multicast, ou de contrôle logique, pour seulement fournir une assistance au protocole de multicast fiable.

- **Approches basées sur le support de routeur :** on désigne multicast fiable avec le support de routeur où il peut contribuer dans le processus de recouvrement. Ce support peut être divisé en deux catégories, à savoir: une catégorie utilise le support minimal du routeur de sorte qu'il redirige les demandes de retransmission (NACK) au répondeur (réplier) approprié, pour réduire le problème de l'implosion des acquittements en feedback et restreindre la portée des retransmissions et des demandes de retransmission. Et celle qu'utilise des routeurs actifs (ou des serveurs actifs co-localisés avec les routeurs) avec une extension des services actifs afin d'offrir une solution générale et flexible pour le multicast fiable.

De plus, avec le traitement des trois points évoqués ci-avant, les méthodes de recouvrement des pertes utilisées par ces approches sont classifiées en **[32]**:

- **Sender-Initiated (Sender-Reliable):** une approche centralisée où l'expéditeur a un contrôle total et exige que tous les récepteurs doivent répondre chacun par un acquittement positif (*ACK*), afin de détecter et retransmettre les paquets perdus.
- **Receiver-initiated (Receiver-reliable):** une approche distribuée où la charge de détection de pertes est distribuée entre les récepteurs (tout en permettant le passage à l'échelle) tandis que l'expéditeur puisse avoir un contrôle limité. Cette classe est aussi subdivisée en:

  - **Sender-oriented :** dés qu'un récepteur détecte une perte, il transmit en unicast un acquittement négatif(NACK) vers la source qui a la possibilité de retransmettre le paquet perdu (retransmission orientée-émetteur).
  - **Flat, receiver-oriented:** le récepteur transmit en multicast (diffisuion sélective) le NACK, alors que tout autre récepteur qui contient les données en question puisse répondre et émettre la réparation demandée (retransmission orientée-récepteur).
  - **Structure-based, Sender-oriented/receiver-oriented:** le récepteur émet le NACK à un contrôleur local, qui le supprime ou le agrège avec d'autres, pour être redirigé en amant (ou vers les nœuds suivants) dans la structure. Le contrôleur local peut également retransmettre les données manquantes, en réduisant ainsi l'effet sur les récepteurs qui n'ont pas effectivement perdus les paquets.

- **Combinaison de Sender-Initiated et Receiver-initiated (approche hybride):** cette approche hybride vient d'assurer une livraison fiable mutuelle où les pertes au niveau des liens sources seront détectées de façon rapide et la charge de retransmission est répartie de façon idéale entre la source et les récepteurs. en plus, la source peut vider son buffer sans risque de lourde attente (une gestion efficace de buffer).

Après la constitution d'un contexte générale, nous allons au-delà de la classification pour explorer les différentes stratégies de recouvrement, et les protocoles qu'elles incorporés.

5.1.2 Stratégies de recouvrement des pertes

A. Stratégies de bout-en-bout

A.1 Approches Sender-Initiated (Sender-Reliable)

À l'instar du mécanisme unicast fiable TCP, la détection et la retransmission des paquets perdus, dans ces approches, sont initiées par la source, où chaque récepteur doit transmettre, pour chaque paquet reçu, un acquittement positif (ACK) unicast destiné à la source qui va les collecter. À l'expiration du délai d'attente, si la source manque quelconque ACK, comme signal de perte, elle va invoquer une procédure de retransmission. Dans ce contexte, la source peut être surchargée par le traitement des acquittements simultanés tout en créant un énorme fardeau administratif à son niveau (un point central de défaillance). Cette situation peut mener à un taux de pertes élevé dû à la congestion. Les protocoles de cette classe souffrent de problème de l'implosion des acquittements positifs en feedback qui peut sacrifier le facteur d'échelle. Pour remédier ce problème, une solution consiste à distribuer la charge de détection de pertes sur chaque récepteur **[17, 26]**. **NAPP [33]** est un protocole typique de cette classe.

A.2 Approches Receiver-initiated (Receiver-reliable)

L'aspect critique de ces approches est que chaque récepteur soit responsable de détecter les pertes qui surgissent à son niveau de sorte qu'elles déchargent totalement la source de cette responsabilité. Dés qu'un récepteur détecte une perte de paquet, par une erreur de transmission, un numéro de séquence manquant ou un délai de garde expiré, il envoie, en effet, un acquittement négatif (NACK). Suivant la destination de NACK, qui désigne le responsable de la retransmission, deux types d'approches qu'on puisse les distinguer.

A.2.1 Approches Sender-oriented

Un acquittement négatif (NACK) unicast sera transmit vers la source, qui est le responsable de retransmettre le paquet perdu (retransmission orientée-émetteur).

L'utilisation des NACKs , qui sont peu fréquents que les ACKs, réduit d'une manière considérable la charge des messages de contrôle au niveau de la source ainsi que la consommation de la bande passante du réseau. Néanmoins, dans les situations où les pertes surgissent sur les liens sources, qui probablement affectent tous les récepteurs, la source peut avoir un nombre important des NACKs, tout en résultant cependant le problème d'implosion de NACKs. En outre, les récepteurs peuvent souffrir d'un temps de latence de recouvrement, relativement à la longueur du chemin entre la source et le récepteur.

A.2.2 Approches Flat, receiver-oriented

Pour remédier les problèmes ci-indiqués, la tâche de retransmission est attribuée, de façon distribuée plutôt qu'un seul point central de défaillance, aux récepteurs qui se communiquent affin de l'accomplir et d'assurer notamment un recouvrement local. Les protocoles de cette sous classe suivent le modèle générique des protocoles **RINA** (Receiver-initiated with NAK avoidance) **[34]** qui ont adopté une approche basée sur les temporisateurs (timers) afin de supprimer les NACKs dupliqués. À la détection d'une perte de paquet, le récepteur attend une période aléatoire avant qu'il puisse demander la retransmission. Le temporisateur de l'hôte le plus proche du point de perte est probablement le premier qui expire. Cet hôte est élu comme un demandeur (requestor), où il envoie un NACK, en multicast (diffusion sélective), demandant le paquet de données perdu au groupe. Afin d'éviter la redondance, les hôtes qui ont également perdu le même paquet, entendent cette demande et suppriment les siens. Ce comportement empêche le problème d'implosion de NACKs. N'importe quel hôte, qui a une copie de ce paquet en cache, peut répondre à cette demande. Uniquement, celui qui est élu comme répondeur (replier), le plus proche de demandeur, peut diffuser en multicast la réparation demandée vers le groupe entier (retransmission orientée-récepteur).

Cette approche est particulièrement robuste quant au changement de topologie, puisqu'elle ne dépend d'aucun nœud intermédiaire pour faire la suppression de NACKs et de retransmissions. L'inconvénient majeur de l'approche réside dans les problème de localité de réparation et d'exposition des récepteurs (à cause de la diffusion multicast au groupe entier) qui peuvent être allégés par la restriction de la portée de retransmission à un sous-groupe de récepteurs (pour des raisons de scalabilité, la suppression des NACKs est mieux utilisé localement). En outre, la retransmission orientée-récepteur met une contrainte de taille illimitée au niveau des récepteurs pour que le processus de recouvrement soit performant. Le protocole **SRM** (Scalable Reliable Multicast) **[35]** est l'exemple typique basé sur cette approche.

B. Stratégies basées sur le support du réseau

Dans ces approches, les protocoles de transport multicast fiable acceptent un degré donné d'assistance de réseau sous-jacent de deux sorts comme suit **[29]**:

B.1 Stratégies basées sur serveur (Server-based)

B.1.1 Approches Structure-based, Sender-oriented/receiver-oriented

Cette classe d'approches regroupe les membres de groupe en deux structures, à savoir: arbre ou anneau tout en organisant les membres d'un groupe dans des zones administrativement limitées **[34]**.

- **Les protocoles basés sur arbre (Tree-based):** les protocoles basés sur arbre partitionnent la structure de distribution multicast en sous-groupes formant une hiérarchie à plusieurs niveaux. Comme montre la figure **(2.6)**, un arbre logique de contrôle (arbre d'acquittement) qui admet la source comme racine et les récepteurs comme feuilles peut être construit. Chaque sous-groupe de l'arbre a un leader, qui peut être un récepteur désigné ou un serveur dédié.

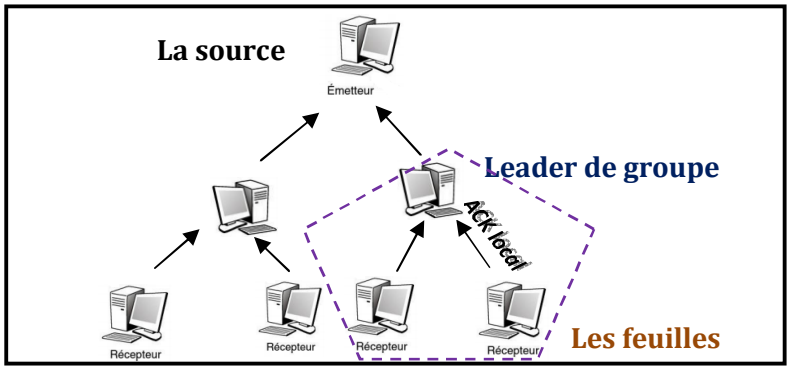

Figure 2.6: Diagramme basique pour le protocole Tree-based [34].

Un leader de groupe est le responsable des retransmissions dans son propre groupe local, en maintenant en cache les paquets reçus de données pour le recouvrement local des pertes. Dans la structure d'arbre d'ACK, les acquittements des nœuds fils (référencés par ACK local ou NACK local) dans un sous-groupe sont envoyés au leader de sous-groupe, plutôt qu'ils contactent directement la source. Ce dernier agrège également et/ou supprime les acquittements identiques, ainsi qu'il puisse prendre la décision de supprimer les paquets en cache en fonction des ACKs agrégés afin de maintenir le passage à l'échelle (la scalabilité) à un grand nombre de récepteurs.

Le souci principal de ces approches est de limiter la portée des acquittements et des retransmissions pour réduire les problèmes de l'implosion en feedback et d'exposition des récepteurs, préserver la bande passante, minimiser la latence de recouvrement et travailler correctement avec une mémoire de taille finie.

Cependant, leur inconvénient provient de la gestion d'un grand nombre de récepteurs désignés ou de serveurs dédiés, où l'échec d'une machine pourra bientôt créer un énorme fardeau administratif. Bien que l'arbre construit soit souvent sous-optimal et moins robuste aux changements de la topologie du réseau sous-jacent. En voici les protocoles **LBRM** (Log-Based receiver Reliable Multicast) **[36]**, **TMTP** (Tree-based Multicast Transport Protocol) **[37]** comme des exemples typiques de protocoles basés sur cette approche.

- **Les protocoles basés sur anneau (Ring-based):** À l'origine sont développés pour fournir un support pour les applications qui exigent un multicast atomique et un ordre total de transmissions à tous les récepteurs.

Comme montre la figure **(2.7)**, un protocole basé sur anneau regroupe les membres de groupe en anneau logique (anneau de récepteurs). L'idée de base est de désigner un récepteur jouant le rôle d'un site jeton (Token site), qui va acquitter positivement les paquets reçus à la source. Par conséquent, le problème d'implosion des acquittements en feedback sera allégé. En outre, les acquittements positifs sont aussi utilisés pour garantir l'atomicité, aider les autres récepteurs à détecter les pertes et pour horodater les paquets de sorte que tous les nœuds récepteurs ayant un ordre global de paquets pour les délivrer à la couche application.

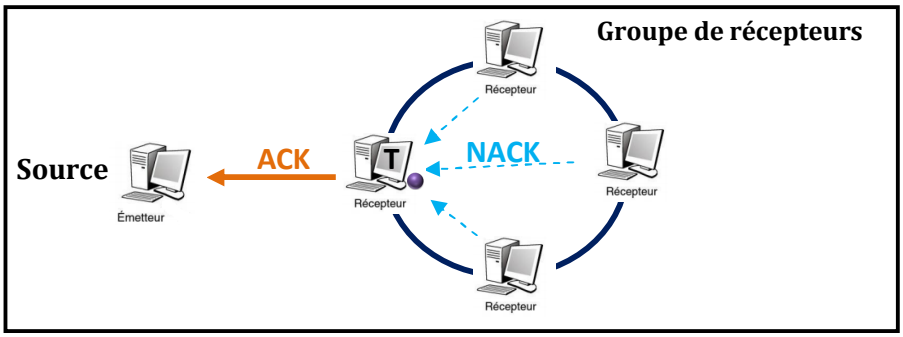

Figure 2.7: Diagramme basique pour le protocole Ring-based [34].

Suite à l'expiration d'un délai de garde sans la réception d'un ACK à partir du site jeton, la source retransmet les paquets. Ainsi, pour la retransmission sélective des paquets perdus, les récepteurs envoient des NACKs au site jeton.

Le site jeton doit être choisit, parmi l'ensemble des récepteurs, à tour de rôle où le jeton pourra passer, par le biais d'ACK envoyé à la source, au membre suivant de l'anneau des récepteurs dés que le nouveau site ait correctement reçu tous les paquets que l'ancien site. Ce dernier peut vider les paquets en mémoire dés le départ du jeton, alors que la source ne supprimera les siens qu'à la réception d'un ACK/jeton. **TRP** (Token Ring Protocol) **[38], RMP** (Reliable Multicast Protocol) **[39]** sont des exemples typiques.

B.2 Stratégies basées sur le support de routeur

Les protocoles de multicast fiable viennent pour remédier le problème de la fiabilité au niveau transport. Cependant, leur performance peut être souvent améliorée avec le support des routeurs fonctionnant au niveau réseau, selon les deux axes suivant **[11]:**

- **Support minimal du routeur:** dans cet axe, les demandes de retransmission traversant un routeur, ainsi que les répondeurs les plus convenables sur ses liens directs seront maintenus à son niveau. En exploitant ces informations, il deviendra désormais capable de rediriger les demandes de retransmission (NACK) au répondeur (replier) approprié afin de réduire le problème de l'implosion des acquittements en feedback et de restreindre la portée des retransmissions. Ce support semble tout à fait une solution vitale pour la classe des approches Flat, receiver-oriented**.** En voici les protocoles **LMS** (Light-weight Multicast Services) **[40] et RMCM** (Reliable Multicast for Core-based Multicast trees) **[41]** comme exemples typiques**.**
- **Routeurs actifs:** sachant que les approches basées sur les arbres soient les plus satisfaisantes en termes du facteur d'échelle, leurs performances restent toutefois en fonction de l'optimalité et l'efficacité de l'arbre logique construit, qu'est souvent difficile à maintenir. Ce problème peut être résolu en utilisant directement les routeurs constituant l'arbre de distribution multicast sous-jacent, qui peuvent contribuer, de façon actif, pour assurer un transport multicast fiable. Cette hypothèse a été réalisée avec l'expérience des technologies des réseaux actifs dans le domaine des communications de groupe. Contrairement au support minimal des routeurs dédiés et figés, cette approche réseau offre une solution plus générale et flexible du fait qu'elle déploie des services actifs au niveau des routeurs dans le but de faire **[26]**:
  - Le cache des paquets de données au niveau des routeurs actifs, pour assurer localement le recouvrement (récupération) des pertes tout en garantissant une bonne répartition de la charge de recouvrement ;
  - l'agrégation et / ou la suppression des acquittements en feedback pour la restriction de la portée des demandes de retransmission ;
  - La diffusion des retransmissions en multicast partiel (subcast) afin de limiter sa portée aux récepteurs concernés par la perte tout en résolvant le problème de la localité de réparation.

Les protocoles **AER** (Active Error Recovery) **[42]**, **ARM** (Active Reliable Multicast)**[43]**, **DyRAM** (Dynamic Replier Active reliable Multicast) **[44]** et **AMRHy** (Active Multicast Reliable Hybrid protocol) **[45]** sont des exemples représentatifs de cette approche.

En résumé, la figure **(2.6),** ci-dessous, montre cette classification ainsi que quelques protocoles de transport multicast fiable illustratifs :

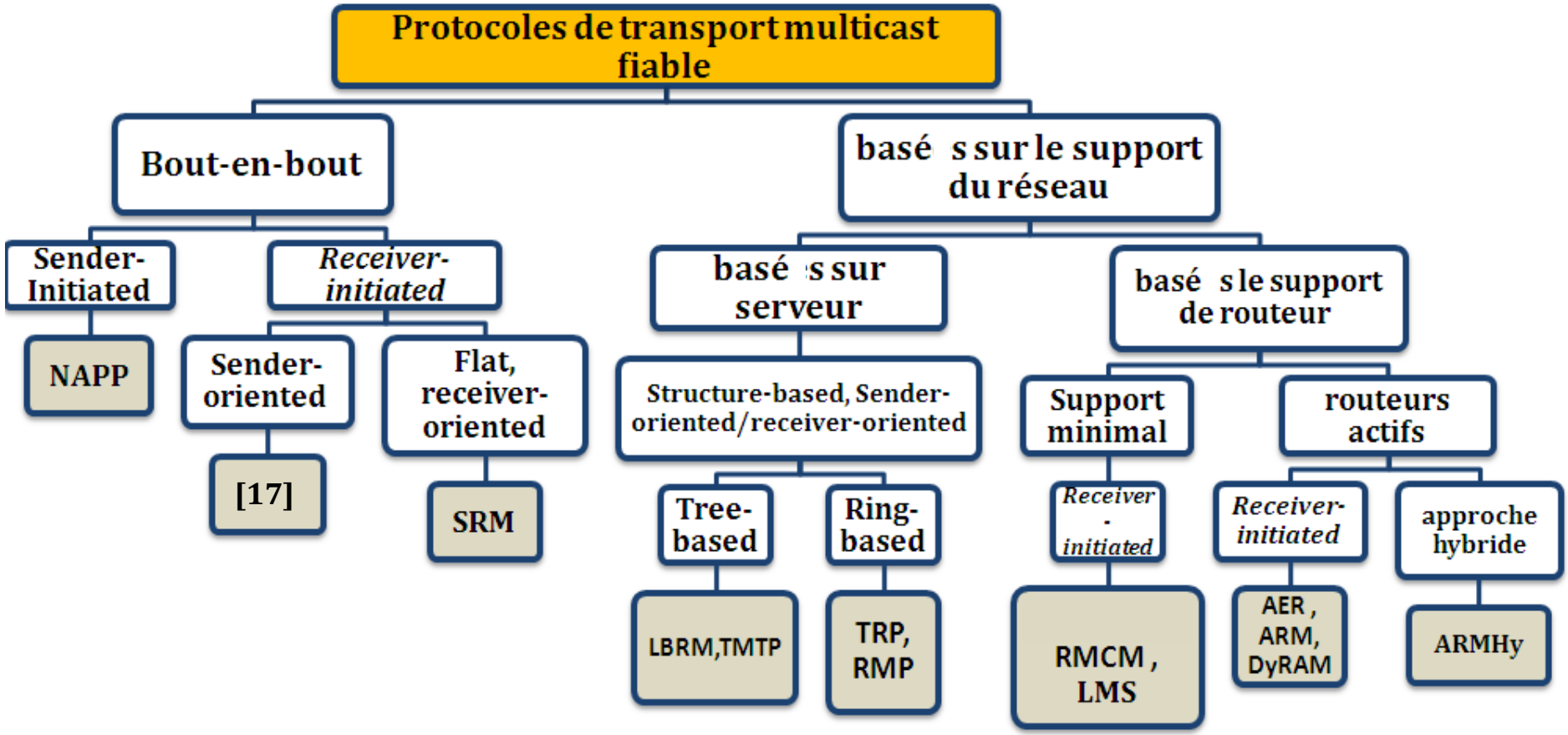

Figure 2.8: Taxonomie des protocoles de transport multicast fiable.

6. Conclusion

Notre objectif visé, dans ce chapitre, est de constituer un état de l'art autour de la fiabilité des communications multicast dans les réseaux IP filaires, Internet comme étude de cas. Tout d'abord nous avons présenté brièvement le support du multicast dans les réseaux de communication en générale, et le réseau Internet en particulier. Dans ce contexte, le modèle du service réseau multicast IP, qui a été motivé par le travail judicieux de Deering, définit les techniques utilisées pour permettre une distribution efficace à grande échelle de l'information destinée à un groupe d'utilisateurs de large population. En plus de l'adressage multicast et la gestion d'adhésion dynamique au groupe multicast, ce service répond au problème de l'acheminement de manière efficace le trafic vers l'ensemble de ses abonnés par le biais des protocoles de routage multicast.

Cependant, les protocoles de routage multicast basés sur le multicast IP, qui suit la vision de son ancêtre unicast IP, n'assurent qu'une délivrance de best effort. Certaines applications multicast fiables, en plus de routage efficace, exigent une livraison fiable. Pour assurer cette fiabilité, qui fait l'objet des travaux de standardisation du groupe de travail RMT, plusieurs solutions (approches) de niveau transport ont été proposées afin de répondre au mieux aux besoins des applications spécifiques plutôt qu'un usage général. Ces approches sont divisées généralement en deux grandes familles : Approches de bout-en-bout et celles qui sont basées sur le support du réseau.

Par la suite, nous allons projeter ce support sur les réseaux sans fil et en particulier les réseaux sans fil ad hoc.

Multicast dans les réseaux sans fil

1. Introduction

Le plein essor de la technologie sans fil et l'avènement des équipements, de communication et de traitement, sans fil et mobiles ont motivé la prolifération du déploiement des applications mobiles impliquant une collaboration entre un groupe de participants.

En effet, l'utilisation des communications multipoints efficaces pour supporter les communications de groupe dans les réseaux sans fil est devenue de plus en plus une nécessité cruciale. Bien que le multicast soit le meilleur service de communication qui offre cette efficacité, le support de ce service dans les réseaux sans fil, où les ressources fournies sont limitées, demeure un objectif capital.

Le présent chapitre aborde le support de multicast dans les réseaux sans fil. Après une présentation concise des motivations argumentatives et les domaines d'applications, nous entreprenons sur le traitement des problèmes majeurs qui se relèvent lors de ce support: la gestion des groupes multicast, le routage et la fiabilité des communications, précisément dans les réseaux sans fil ad hoc.

2. Motivations du support de multicast

L'objectif du multicast, dans un réseau de communication, vise à assurer une utilisation efficace de la bande passante et des ressources de réseau. Ceci nous motive aussi à supporter le multicast dans le contexte des réseaux sans fil, là où les ressources fournies sont limitées (bande passante, énergie, capacité de stockage et de traitement) et la qualité de liaison sans fil est variante, afin de parvenir à une utilisation efficace des ressources dans les points suivants:

- **L'optimisation de l'utilisation de la bande passante :** À l'opposition d'unicast et de broadcast, le multicast permet à une (ou plusieurs) source de transmettre simultanément une même copie de ses données à tous les récepteurs. Elle envoie une seule copie de paquet traversant exactement une seule foi chaque lien de la structure de distribution dans le réseau. C'est le réseau (routeurs) qui va dupliquer cette copie sur le lien (interface de sortie) en cas de besoin, jusqu'à ce que la copie du paquet atteigne chacun de récepteurs visés **[46]**.

C'est une manière d'imposer à un nœud de ne recevoir qu'un seul exemplaire d'un paquet, tout en évitant l'envoie de plusieurs copies simultanément autant de récepteurs, les traitements associées à cette réplication au niveau de la source et le gaspillage indésirable de la bande passante dû à la duplication inutile des paquets sur le même lien surchargeant le réseau.

- **La minimisation de la quantité d'énergie consommée :** Avec une transmission en multicast, la source n'envoie qu'un nombre minimum des copies de paquets vers des destinataires différents. Ceci minimise davantage la consommation d'énergie lors de la transmission et du traitement au niveau de la source.

En outre, un nœud mobile peut consommer de l'énergie pour envoyer et recevoir des paquets, bien que la duplication des paquets soit la mission des nœuds constituant la structure de distribution. Cette manière de faire, n'implique qu'un certain nœud de réseau (nœuds routeurs) intervenant à la commutation des paquets, qui fonctionne de façon réactive (mode **émission** et/ou **réception**), alors que les autres restent inactifs (mode **veille**). Par conséquent, la consommation d'énergie sera réduite au minimum et la durée de vie de réseau sera maximisée.

Le multicast peut aussi profiter de la nature de diffusion du support sans fil pour maximiser le nombre des nœuds récepteurs d'une transmission. En fait, la puissance d'émission doit être égale au maximum entre les puissances d'émission de l'ensemble. Ceci va conserver l'énergie des autres nœuds inclus dans cette zone en manifestant le concept de **« Wireless multicast advantage » [47]**.

- **L'amélioration de l'efficacité de la liaison sans fil :** En exploitant la propriété inhérente de la diffusion de liens radio lors de l'envoie de données en multicast, une seule copie de paquet transmis peut être délivrée directement à l'ensemble des nœuds récepteurs qui sont situés à l'intérieur de la zone de couverture du nœud source, et relayée (dupliqué) aux autres destinations qui sont en dehors, tout en évitant sa réplication au niveau de la source et améliorant l'efficacité du support sans fil. Cela donne une raison judicieuse pour l'utilisation des communications multicast dans les réseaux sans fil **[48]**.

À l'instar, le service multicast fourni un support efficace pour les applications mobiles orientées-groupe, sachant qu'il assure le passage à l'échelle en termes de nombre de participants, la réduction des coûts de transmission et de traitement, la livraison de données en temps réel (respecter le délai de bout-bout) et l'augmentation des vitesses de transfert.

3. Domaines d'applications du multicast

Dû à ses motivations judicieux, nous constatons que le multicast s'avère le meilleur service de communication pour soutenir les applications nécessitant des communications multipoint.

Actuellement, ce service est supporté dans divers domaines d'applications dans le contexte des réseaux sans fil, avec variétés d'exigences souhaitées selon le type d'application come suit:

- **Les services du multicast dans les réseaux de 3^{éme} génération (réseaux 3G) :** Les réseaux mobiles de 3^{éme} génération améliorent les anciennes générations (1G, 2G) des réseaux cellulaires, en termes de capacité des ressources (bande passante) et des types supportés de données (voix, vidéo, données), pour déployer des services et applications extensibles (multimédia, MMS). Plusieurs communautés travaillent sur la standardisation des systèmes dans cette génération, comme l'**UTMS** et l'**ETSI,** qui fournissent un débit maximum entre **64kb/s - 2Mb/s** et un accès aux services d'Internet et services spécifiques d'UMTS. Avec cette tendance, plusieurs fournisseurs de services tente d'offrir multiples services, tels que : TV Mobile, la distribution de contenu multimédia et les communications Peer-to-Peer, aux leurs abonnés, en utilisant les communications multicast pour mieux utiliser les ressources de réseaux. Ces services exigent une délivrance fiable et en temps opportun **[16]**.

- **Les systèmes de transport intelligents ITS (Intelligent Transportation Systems) :** L'émergence des technologies de l'information et de la communication dans le domaine de transport aide à l'apparition des systèmes de transport intelligents. Ces systèmes, basés principalement sur les communications sans fil, sont appliqués sur divers champs d'activité via la diffusion en multicast des informations pertinentes au groupe des conducteurs concernés, munis d'équipements mobiles reliés au système. De nos jours, plusieurs systèmes ont été développés. Les systèmes d'aide à la navigation (**GPS, GSM)** et les **SAGT** (Systèmes d'Aide à la Gestion de Trafic) sont les plus utilisés. Ces systèmes exigent l'exactitude des informations de localisation transmises (communications fiables et ordonnées).

- **Le commerce mobile (m_commerce) :** Le commerce mobile est une discipline émergente du commerce électronique, qui implique des équipements mobiles, des applications, middleware et des réseaux sans fil, déployée uniquement dans les environnements sans fil tout en éliminant les contraintes physiques et temporelles des produits (vendre ou acheter n'importe quoi, n'importe où et n'importe quand). Pratiquement, les applications du commerce mobile orientées-groupe, comme vente à l'enchère mobile, exigent une connectivité permanente, des opérations atomiques de transaction et un service multicast fiable et sécurisé **[49]**.

- **L'enseignement à distance :** L'évolution des technologies de communication mène à l'avènement des nouvelles technologies d'enseignement à distance telles que : ' par correspondance' avec les services postaux, 'l'université virtuelle' sur Internet et 'l'étude mobile' avec les réseaux mobiles.

Ces technologies, qui peuvent être synchrones (le web et la vidéo conférence) ou asynchrones(les enregistrements audio et vidéo), nécessitent une bande passante élevée et des communications multicast en temps-réel pour la qualité de visionnement **[49].**

- **Communications de groupe dans les réseaux ad hoc :** Dû à la simplicité d'installation des réseaux ad hoc, certaines applications des missions critiques ont été largement déployées dans ces réseaux, et notamment dans les domaines militaires, les opérations de secours après une catastrophe et les réseaux de capteurs. Sachant que dans la plupart des situations, les nœuds de réseau se communiquent afin d'accomplir une tâche commune, ces applications nécessitent des communications multipoint de type **one-to-many** ou **many-to-many**, cas du milieu militaire, et exigent aussi un délai minimum de bout en bout et une communication multicast fiable et sécurisée **[11]**.

L'étude des exigences des applications susmentionnées, nous nous éclairons que le multicast pourrait soutenir et fournir les services nécessaires pour ces applications. En outre, l'émergence des technologies des réseaux cellulaires (2G, 3G) et réseaux ad hoc (réseau de capteurs, MANET, VANET)), et la popularité du déploiement des applications collaboratives, nous amènent à explorer le support du service multicast dans un environnement sans fil.

4. Multicast dans les réseaux sans fil

Le multicast, comme nous avons montré auparavant, fournit une solution naturelle aux communications multipoint dans les réseaux sans fil, pourvu qu'il réduise la charge de la source et utilise efficacement la bande passante, l'énergie et les ressources du réseau.

En fait, la fourniture d'un service multicast dans les réseaux sans fil doit offrir, au minimum, les fonctionnalités de base sus-indiquées **[18]**:

- l'identification et la gestion des groupes multicast ;
- la construction et la maintenance d'une structure de distribution de données multicast ;
- l'acheminement des paquets multicast à travers cette structure ;
- et le contrôle d'erreur et de congestion.

Cependant, les caractéristiques de réseau sans fil peuvent perturber la fourniture de ces fonctionnalités dans certains niveaux de l'architecture.

4.1 Gestion d'adhésion au groupe multicast

Dans un réseau sans fil avec infrastructure-fixe (réseaux cellulaires), les fonctions du corps de réseau ne sont pas affectées.

Dans la situation où l'infrastructure est constituée par un réseau filaire Internet ou Ethernet (extension de réseau IP), on peut motiver l'adoptation du protocole IGMP (RFC 1112) **[13]**, de gestion de groupe multicast dans l'Internet, aux réseaux sans fil en apportant des modifications sur lui.

Etant donné que les nœuds mobiles à l'intérieur d'une cellule ne puissent recevoir que les messages de requête IGMP ou de rapport provenant de leur AP. Le routeur multicast doit envoyer un message de requête par point d'accès et retransmettre itérativement le message de rapport envoyé par un nœud mobile, pour les recevoir par tous les nœuds mobiles **[49]**.

De plus, certains réseaux sans fil (GSM et GPRS) fournissent des liaisons point-à-point, qui nécessite la collection des informations supplémentaires (une liste d'hôtes par groupe ou de groupes par hôte) afin de communiquer les messages d'IGMP sur chaque liaison **[50]**.

Le phénomène du temps "**leave latency**", où un hôte quitte le groupe et l'émission vers celui-ci devra arrêter, peut être aussi augmenté davantage dans le contexte des réseaux sans fil en raison des paquets retardés (au niveau liaison (MAC)) ou perdus dues au taux d'erreur élevé **[49]**. En effet, la bande passante peut être gaspillée **[51]**. Pour adresser ce problème-ci, une de solutions **[50],** qui ont été envisagées pour réduire le délai de latence, est basée sur des messages de joindre/quitter un groupe de façon explicite. Des autres alternatives combinent cette technique avec un schéma d'acquittement **[52]** ou reposent sur la retransmission des requêtes basée sur l'histoire des liens et des utilisateurs **[52].**

En plus de la dynamicité d'adhésion, le mécanisme de gestion doit aussi superviser la mobilité des membres du groupe multicast (changement intercellulaire ou inter-sous-réseaux). En effet, une version modifiée d'IGMP dénotée **WGMP** a été proposée **[51].**

Au contraire, dû à l'absence d'une infrastructure fixe, les réseaux sans fil ad hoc n'offre pas un environnement trivial à l'adoptation du protocole IGMP. Néanmoins, la gestion d'adhésion au groupe peut être intégrée (incorporées) dans le protocole de routage multicast.

Après avoir constitué le groupe multicast, il deviendra désormais acheminer, de manière efficace, le trafic multidestinataire généré par la source vers l'ensemble des membres. Ceci traduise qu'une transmission en multicast d'un message nécessite une technique de routage multicast afin d'assurer sa délivrance aux membres concernés, que nous allons découvrir par la suite.

4.2 Routage multicast dans les réseaux sans fil

Le routage multicast est un sous-problème de routage, voire inhérent à la fourniture du service multicast, qui consiste à trouver une structure recouvrant tous les membres d'un groupe multicast pour les livrer les données concernées **[53]**.

D'abord, la source envoie une seule copie du paquet multidestinataire à un groupe dynamique des récepteurs actifs, dans des endroits différents, en même temps. Pour les atteindre, le chemin de livraison nécessite la création de plusieurs suites ordonnées de branches, dérivés vers les membres de groupe, à travers le réseau tout en construisant une structure de distribution reliant les membres du groupe multicast **[26]**. Celle-ci doit être mise à jour à chaque changement de membres. Ces fonctionnalités sont assurées par des protocoles de routage multicast en utilisant les informations d'appartenance collectées par les protocoles de la gestion des groupes, ou les opérations intégrantes dans le protocole de routage lui-même (cas des réseaux ad hoc).

À l'opposition des réseaux filaires, le routage multicast ne traite seulement la dynamicité du groupe, mais aussi le changement dynamique dominant la topologie des réseaux sans fil dû à la mobilité des membres ou du groupe lui-même **[20].** Par conséquent, il semble important de développer des mécanismes de routage multicast prenants les points suivants **[53]:**

- la minimisation de la charge du réseau (éviter la duplication inutile des paquets, les boucles de routage et la concentration du trafic sur un lien ou un sous-réseau).
- la capacité de concevoir des chemins optimaux avec fonctions de coût différentes (ressources disponibles, la connectivité de nœud, le délai de bout-en-bout).
- la minimisation du nombre maintenu des informations d'état sur le réseau sous-jacent.
- la fourniture d'un support de base pour une transmission fiable en dépit des changements fréquentiels de routes.
- la scalabilité qui est primordiale pour les communications de groupes comme facteur d'échelle en présence d'un nombre important de récepteurs dans le groupe.

En plus, ces protocoles doivent être pris en considération le type des liaisons utilisé dans la couche de liaison (mode de transmission utilisé) ainsi que la compatibilité avec les protocoles des couches supérieures afin de leur fournir les services désirés **[19].**

Comme nous avons susmentionnés, les réseaux sans fil avec infrastructure étendent les fonctionnalités basées sur IP aux nœuds mobiles sans altérer le corps du réseau (infrastructure fixe représente un sous-réseau d'Internet). Néanmoins, les questions soulevées par le routage multicast dans ce contexte se limitent à la mobilité des nœuds hôtes.

Etant donné que le Mobile IP (RFC 3220) **[8]** soit le mécanisme de base utilisé pour gérer la mobilité dans les réseaux basés sur IP unicast, de façon qu'un nœud mobile puisse changer son emplacement sans condition de changer son adresse IP. L'organisation IETF a proposé deux approches pour fournir le multicast en basant sur Mobile IP : **BT** (bidirectional tunneling) et **remote subscription [54]**. Ainsi, **MoM** (Mobile Multicast) et **RBMoM** (Range-Based Mobile Multicast) **[46]** ont été proposées comme des extensions de ces approches. Tandis qu'une autre alternative combine le Multicast IP avec le Mobile IP afin de supporter le multicast mobile.

Néanmoins, dû à l'absence d'une telle infrastructure, cette hypothèse est invalide pour les réseaux sans fil ad hoc. Additionnement à l'absence d'une infrastructure-fixe, leurs caractéristiques conduisent à déduire que le problème de routage multicast devienne de plus en plus compliqué dans ces environnements, qu'il faut nous traiter.

4.2.1 Routage multicast dans les réseaux sans fil ad hoc

Par nature, les réseaux sans fil entraînent un certain nombre de problèmes n'ayant pas d'équivalent dans le contexte des réseaux filaire.

En plus de l'absence d'une infrastructure fixe, les réseaux ad hoc héritent les problèmes traditionnels des réseaux sans fil tels que : l'affaiblissement de la bande passante, collision et interférence, limitation de la puissance et de la portée de transmission, la non fiabilité des liens sans fil. Entre autres, ils présentent les problèmes d'une topologie fortement dynamique et multi-saut, du terminal caché et des nœuds ayant des ressources de fiable capacité dans leur configuration mobile (MANET).

Ces problèmes mettent des défis face au développement, ou l'adoption, des mécanismes de routage multicast qui doit garantir la construction d'une structure multicast robuste et efficace dans cet environnent hostile.

4.2.2 Enjeux de la conception d'un protocole de routage multicast

La plupart des caractéristiques (non déterministes) de réseaux ad hoc font plusieurs enjeux sur la conception des protocoles de routage multicast, notamment **[11, 55, 56]**:

- **la robustesse** : la mobilité de façon arbitraire des nœuds résulte des pertes significatives des paquets acheminés dues aux changements fréquentiels de la topologie. Dans ce cas, le protocole de routage multicast doit être robuste suffisamment pour qu'il résiste au changement de la topologie et en effet atteindre un ratio élevé de délivrance.

- **l'efficacité et l'overhead de contrôle:** dû à la limitation de la bande passante du médium sans fil, le protocole de routage multicast doit utiliser efficacement cette ressource de sorte qu'il améliore sa capacité disponible. Ceci par la minimisation du nombre des paquets de contrôle par rapport aux ceux de données pour rendre compte un service multicast efficace.
- **La consommation d'énergie :** l'autonomie de la batterie des nœuds peut contraindre la durée de vie du réseau en totalité. Pourvu que cette durée soit maximisée, le protocole doit implanter des techniques de sauvetage d'énergie minimisant sa consommation.
- **La sécurité, la fiabilité et la scalabilité** : du fait de la vulnérabilité aux attaques du support sans fil, et de son caractère non fiable, certaines applications déployées dans ces réseaux exigent des communications multipoint fiables et sécurisées. En plus, le protocole doit faire face les problèmes rencontrés à grande échelle, afin de fournir le support souhaitable.
- **La qualité du service et la gestion des ressources** : L'assurance de la qualité de service(QoS), dans les applications multimédia, nécessite la réservation des ressources requises. Néanmoins, dans les réseaux ad hoc, là où les ressources fournis sont limitées, les mécanismes de routage multicast doivent assurer une utilisation et une gestion efficace des ressources volatiles afin de supporter un service de qualité acceptable.
- **La dépendance du protocole de routage unicast** *:* Si un protocole de routage multicast repose sur un protocole de routage unicast particulier, il est impraticable pour ce protocole de travailler dans des réseaux hétérogènes. Par conséquent, il est souhaitable que le protocole de routage multicast soit indépendant de tout protocole de routage unicast spécifique.
- **L'adaptabilité :** Sachant que le déplacement arbitraire des nœuds résulte la rupture des liaisons et la création des autres, le protocole doit réagir rapidement à ces événements pourvu qu'il s'adapte au changement dynamique de la topologie tout en réduisant la perte de paquets.

4.2.3 Protocoles de routage multicast pour les réseaux ad hoc

Nous avons su auparavant que l'objectif d'un protocole de routage multicast est de créer et de maintenir une structure multicast de délivrance avec la considération des contraintes contournées sur l'environnement (ressources limitées, l'absence d'une infrastructure, changements imprévisibles et imprédictibles). Pour que ce protocole soit performant dans ce contexte, il doit baser sur des opérations distribuées lors de l'acheminement des paquets (routage décentralisé), bénéficier de sa propriété d'auto-organisation et exploiter la propriété 'multi-saut' de la topologie.

Pour son fonctionnement, le protocole repose sur un algorithme de routage afin d'exploiter les informations d'appartenance au groupe et de construire la structure multicast nécessaire. Dans les réseaux ad hoc, trois catégories d'algorithmes de base ont été utilisées **[11]:**

- **Inondation simple** : aucune structure de délivrance n'est construite, l'idée est d'inonder le réseau (*flooding*) où chaque nœud rediffuse (sans garder) le message reçu vers ses voisins. Cette approche est mieux adaptée aux changements fréquentiels de la topologie, dans des scenarios fortement mobiles, et ne nécessite que peu de ressources (mémoire, CPU). Bien qu'elle engendre plusieurs problèmes (redondance, tempête de diffusion «*broadcast storm*»).
- **Approche proactive :** les chemins vers toutes les destinations possibles sont précomptés au début et stockées dans la table de routage. Pour que les informations de routage stockées soient maintenues à jour, elles seront distribuées périodiquement dans le réseau.
- **Approche réactive** : les chemins entre les nœuds sont crées à la demande et en réponse à la requête de création (mécanisme de requête-réponse).

Dans les dernières décennies, plusieurs efforts tentent de développer des protocoles de routage multicast pour ces réseaux. En fait, la conception de ces protocoles suit l'axe chronologique suivant: l'adoption des solutions existantes pour les réseaux filaires conventionnels aux MANET, l'extension des protocoles unicast dans les réseaux MANET avec le support de multicast, ou bien le développement des nouveaux protocoles.

Afin de normaliser un protocole de routage multicast, le groupe de travail MANET de l'IETF présente plusieurs propriétés désirables de ce dernier, en incluant : l'acheminement distribué, découverte de route à la demande, sécurité et l'absence de boucle de routage.

4.2.3.1 Taxonomie des protocoles de routage multicast

Pour comparer et analyser les différents protocoles de routage multicast, il est préférable de les classifier afin de distinguer leurs caractéristiques et de découvrir les relations internes entre eux.

D'après la littérature **[11]**, nous pouvons distinguer deux grandes classes des protocoles. Une classe de protocoles conçus uniquement pour des applications spécifiques (dépend aux applications), tandis que l'autre classe soit conçue pour un souci général. Cette dernière est aussi classée selon multiples critères. Dans cette section, nous nous intéressons aux deux principales critères de classification, entre elles, ci-dessous **[11, 56, 57]:**

a- Classification basée sur le niveau (la couche) dans la plie des protocoles

Les protocoles de routages multicast peuvent être implémentés sur différents niveaux de l'architecture, avec fonctionnalités spécifiques pour supporter les communications multicast.

- **La couche réseau multicast (Network Layer Multicast):** la majorité des protocoles de routage multicast sont implémentés au niveau (couche) réseau, qui a la mission d'acheminer les paquets entre chaque paire source-destination en basant sur les informations de routage, pour relayer les paquets, maintenues dans les nœuds intermédiaires du réseau sous- jacent. Ces derniers se coopèrent afin de livrer les paquets à la destination.

- **La couche applicative multicast (Application Layer Multicast):** ou **overlay multicast**, l'idée est de former un réseau superposé « *overlay »,* constitué par les nœuds membres du groupe multicast (infrastructure virtuelle), au sommet du réseau physique sous-jacent. Comme montre la figure **(3.1) [56]**, chaque lien dans l'infrastructure est représenté sous forme d'un tunnel unicast. Cette couche implémente les fonctionnalités spécifique au multicast (l'adhésion au groupe, routage multicast), et les fonctions du transport, au-dessus de la couche réseau de base assurant les fonctions minimales (service datagramme, routage unicast). En voici des protocoles typiques : **AMRoute** (Ad Hoc Multicasting Routing Protocol) **[58]** et **PAST-DM** (Progressively Adapted Sub-Tree in Dynamic Mesh) **[59]**.

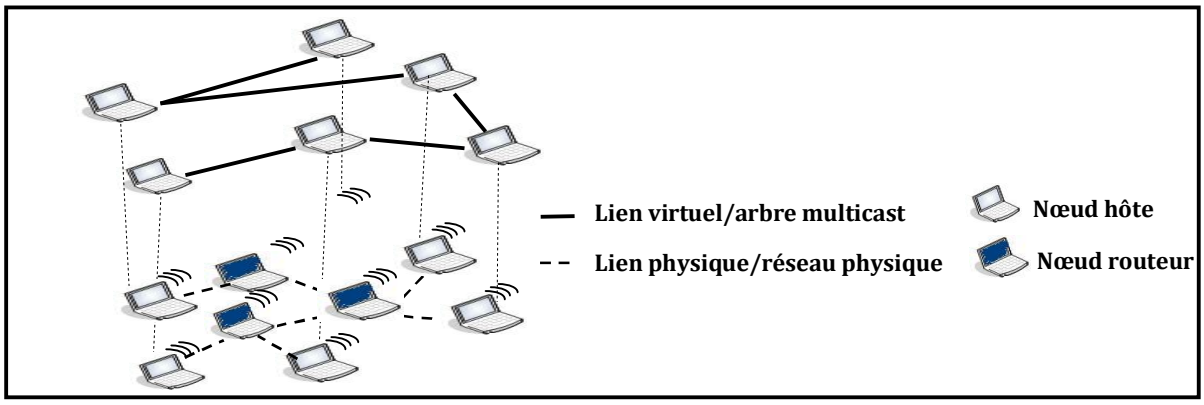

Figure 3.1: Illustration de la couche applicative multicast

- **La couche MAC multicast (MAC Layer Multicast):** dû au nature multi-saut du réseau ad hoc, les paquets acheminés peuvent être relayés par plusieurs sauts. En outre dû à l'non fiabilité des liens sans fil, ils sont susceptibles d'être perdus, au niveau d'un saut de chemin emprunté, avant qu'ils puissent arriver à leurs destinations. En effet, un mécanisme de recouvrement de perte à chaque saut doit être implanté afin d'assurer un routage fiable, et améliorer également l'efficacité des communications multicast. Ceci dans la couche MAC multicast.

Des exemples typiques de ces protocoles sont**: BMW** (Broadcast Medium Window) **[60]**, **RMAC** (A Reliable Multicast MAC Protocol for Wireless Ad Hoc Networks) **[61]**.

b- Classification basée sur la topologie

L'organisation des nœuds de réseau dans une structure de distribution multicast constitue sa topologie. Dans les réseaux ad hoc, nous pouvons distinguer deux grands types de structure:

- **Tree-based multicast** : similairement aux réseaux filaires et les réseaux cellulaires, un chemin de distribution unique est créé entre la source et chaque destination, l'union de ces chemins forme ainsi un arbre multicast dont sa racine la source ou le nœud cœur, et ses feuilles les membres du groupe. La figure **(3.2)** illustre un réseau et son arbre multicast correspond**.**

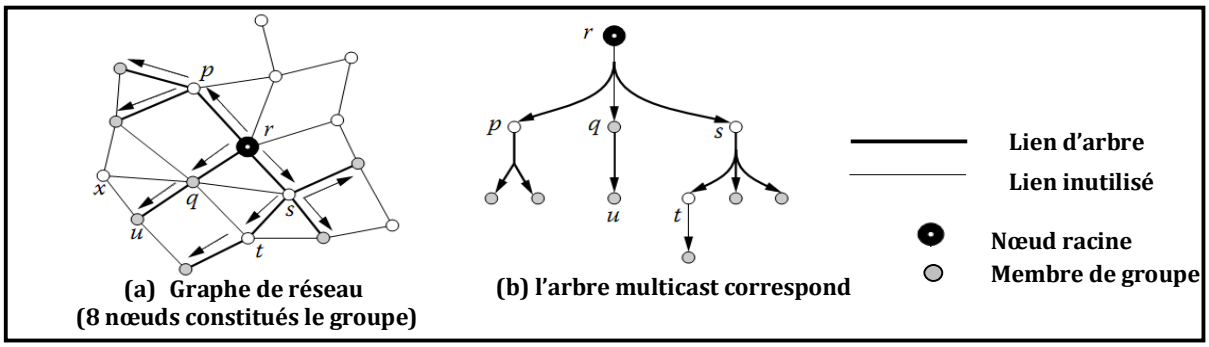

Figure 3.2: Arbre multicast [11]

En plus, deux types d'arbre multicast ont été envisagés, à savoir, *Source-Tree-based* et *Shared -Tree-based.* Dans le premier type, pour le même groupe un arbre par source doit être construit, chacun est raciné par la source propriétaire. Bien que dans le type Shared -Tree-based, un seule arbre multicast, recouvrant tous les membres et partagé par toutes les sources, va être créé. Cet arbre a comme racine le nœud cœur « **core node** » dont sa fonction est de distribuer les paquets de données multicast aux membres du groupe concerné.

La structure d'arbre minimise le nombre des nœuds routeurs relayant les paquets. Ceci permet d'obtenir une haute efficacité de routage et un overhead de contrôle minimum. Cependant, sa fragilité la rend moins robuste en dépite des changements dynamiques de la topologie, dans les environnements mobiles, tout en provoquant des boucles de routage.

Les protocoles basés sur arbre multicast les plus cités au niveau de la littérature sont: **ADMR** (Adaptive Demand Driven Multicast Routing Protocol) **[62], MAODV** (Multicast Ad Hoc On-Demand Distance Vector) **[63]**.

- **Mesh-Based multicast** *:* un seul maillage multicast (multicast mesh), spécifique pour les réseaux mobiles ad hoc (MANET), recouvrant tous les membres du groupe multicast est construit. Cette structure maillée (mesh) est constituée par un ensemble de nœuds interconnectés via multiples liens, où une route construite inclue les nœuds ayant une haute redondance de connectivité avec la maille multicast, comme montre la figure **(3.3)**.

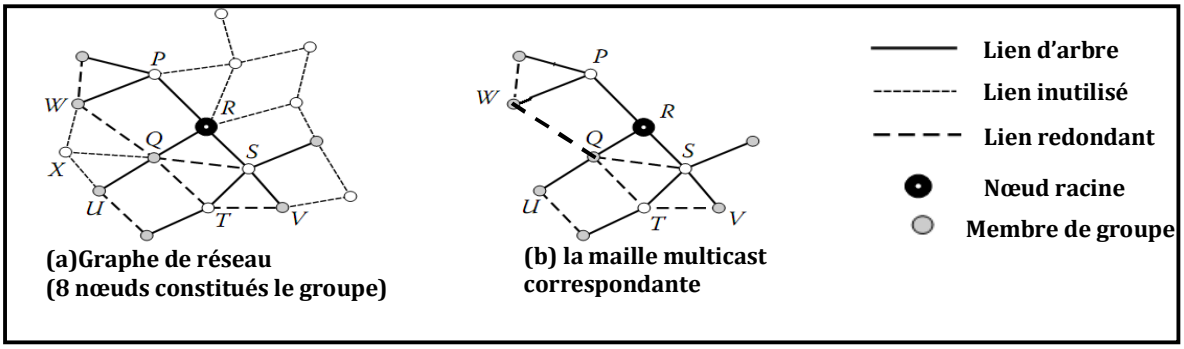

Figure 3.3: Maille multicast [11]

Cette redondance a la tendance d'enrichir la connectivité entre les membres de groupe au regard du changement fréquentiel de la topologie, dû à la mobilité ou à la déconnexion (batterie déchargé) des nœuds. Donc, de multiples routes peuvent exister entre une paire source-destination. En outre, la découverte de la route et la construction de la maille en treillis sont réalisées: soit à l'aide de diffusion (broadcast), soit en utilisant des nœuds cœurs.

Contrairement à l'arbre, la structure maillée est plus robuste dans les environnements mobiles avec un ratio élevé de délivrance de paquets. Cependant, elle est moins efficace en raison des paquets de contrôle dupliqués (gaspillage de bande passante et d'énergie).

En voici quelques exemples typiques des protocoles basés sur arbre multicast **ODMRP (**On-Demand Multicast Routing Protocol) **[64]** et **CAMP** (Core-Assisted Mesh Protocol) **[65]**.

- **Approche hybride** : Cette approche tente de combiner l'approches basée sur maille et celle basée sur arbre, pour bénéficier de: la robustesse et l'efficacité. Cette combinaison assure une multiplicité de chemins entre la source et les destinations afin de minimiser la reconfiguration de la topologie et un routage efficace de paquets entre eux. Le protocole **MCEDAR [66]** est un exemple typique des protocoles de routage multicast hybride.

- **Approche sans état (stateless)** : Pour améliorer la performance des mécanismes de routage à grande échelle, une alternative de protocoles tente d'inclure les informations de routage dans l'entête du paquet, qui peuvent être exploitées par les nœuds intermédiaires pour qu'ils savent commet retransmettre ou dupliquer le paquet. Le souci est de délivrer les paquets aux membres de petits groupes multicast, indépendamment à une structure de délivrance particulière, mais sur le coût d'élargir la taille du paquet. **DDM** (Differential Destination Multicast) **[67]**, **LGT** (Location Guided Tree construction algorithms) **[68]** sont des protocoles types.

c- Autres critères de classification

En résumé, la figure ci-dessous **(3.5)** schématise, en plus aux critères ci-avant, les autres critères de classification des protocoles de routage multicast ad hoc **[11, 56, 57]**.

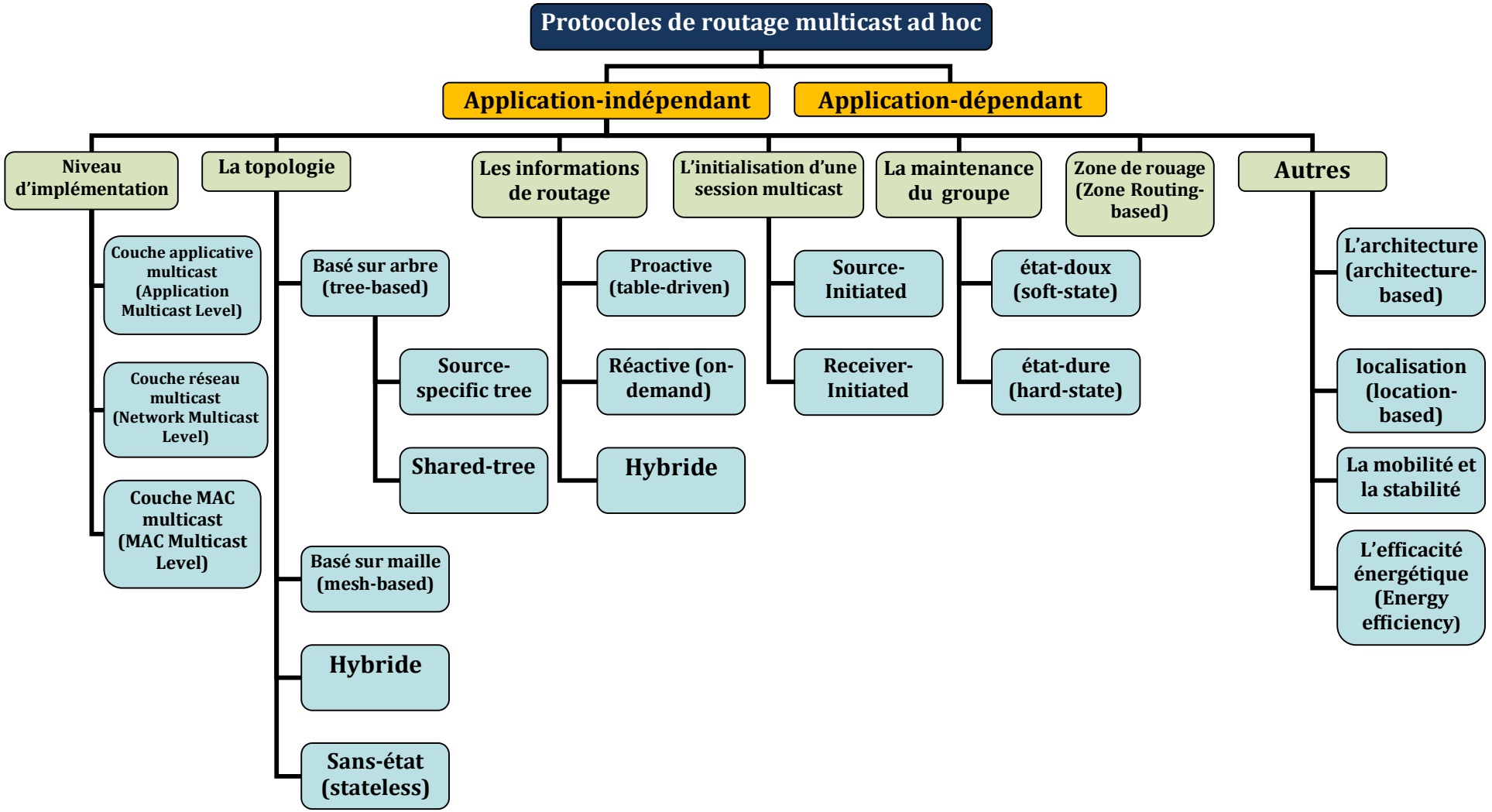

Figure 3.4: Taxonomie des protocoles de routage multicast dans les réseaux ad hoc

4.2.3.2 Présentation de quelques protocoles de routage multicast

En point de vue illustrative, nous choisissions de présenter une description concise des protocoles **MAODV** et **ODMRP**, de niveau réseau, les plus documentés dans la littérature.

- **Protocole MAOVD (Multicast Ad-hoc on-demand Distance Vector Routing protocol):** MAODV **[63]** est un protocole de routage multicast réactif ad hoc, obtenu par l'extension du protocole AODV dédié au trafic unicast, qui se repose sur une structure d'arbre multicast partagé par plusieurs sources (Shared-tree), pour livrer les paquets de données pour un groupe multicast. Les membres de l'arbre sont les membres du groupe et les nœuds intermédiaires (routeurs), reliant ces membres. L'initialisation d'une connectivité au groupe multicast est orienté récepteur (Receiver-Initiated) où le membre du groupe qui construit le premier l'arbre est le chef du groupe pour cet arbre, qui est responsable de maintenir le groupe par une diffusion périodique de messages 'Group-Hello' (GRPH) dans tout le réseau. La construction et la découverte des routes sont déclenchées de façon réactive (à la demande) dés qu'un nœud n'ayant pas une route valide désire transmettre des données, où la construction de l'arbre multicast se fait par la propagation des paquets RREQ, RREP et MACT. MAODV basé sur une approche d'état dur (réactive) pour la maintenance de l'arbre multicast du fait que l'entretien inclut la propagation périodique du message GROUP-HELLO (GRPH), entretien de la connectivité avec les voisins, le choix du Chef de groupe, la révocation d'adhésion et la fusion d'arbres.

- **Protocole ODMRP (On-Demand Multicast Routing Protocol):** Le protocole ODMRP **[64]** est un protocole de routage multicast basé sur les mailles, où la constitution du groupe multicast est initiée par la source (source-initiated) et la routes sont crées de façon réactive à la demande de la source. ODMRP utilise le concept de 'forwarding group' constitué par les nœuds participant à l'acheminement d'un paquet d'un voisin vers un autre. le processus de construction des routes entre les sources et les récepteurs, par La propagation des paquets JOIN DATA et JOIN TABLE, est déclenché lorsqu'une source désire envoyer des données mais elle manque des informations de routage. L'ensemble des routes construites constituent ainsi un maillage de nœuds ou le forwarding group. Les informations d'appartenance et les routes sont actualisées, proactivement (état-doux), par les sources en envoyant périodiquement les paquets JOIN DATA.

4.2.3.3 Discussion des protocoles présentés

Les protocoles de routage multicast que nous avons vus visent à assurer l'acheminement efficace des paquets de données multicast sans aucun mécanisme pour garantir leur délivrance idéale (sans perte, sans duplication). Autrement dit, ils offrent un service de délivrance à moindre effort (fiabilité de type best effort). En effet, nous pouvons supposer que les paquets seront perdus ou arrivés dans le désordre durant la transmission, tout, en provoquant des services différés aux couches supérieures.

Par conséquent, le développement des mécanismes fournissant un service multicast fiable, pour assurer la garantie de la délivrance des données d'application multidestinataire, à tous les membres du groupe, en dépit des échecs des liens de communication ou de nœuds, s'avère une exigence plutôt qu'une nécessité. Dans les réseaux sans fil, à cause de leurs caractéristiques, la fourniture de tel service demeure un problème complexe. Dans la section suivante, nous allons traiter ce problème en détaille.

5. Multicast fiable dans les réseaux sans fil

Par nature, le taux élevé d'erreurs est toutefois l'un des limites des réseaux sans fil, qui face la livraison sans perte potentielle des données jusqu'au bout (les membres de groupe).

En plus de la congestion(débordement des files d'attente) et des coupures de liaisons après une déconnexion de nœuds, cas des réseaux filaires, les paquets peuvent être perdus sur plusieurs niveaux de l'architecture sans fil, notamment au niveau réseau durant la phase de routage dus à la mobilité, le handover, la distance entre la station de base et les mobiles, la densité du réseau (mode dense ou épars) et la reconfiguration de la structure, ou au niveau liaison dus à la non fiabilité de la liaison radio et aux problèmes de transmission (interférences, contention, terminal caché). Par conséquent, plusieurs récepteurs peuvent être affectés par une perte ou un lien congestionné dans plusieurs points dans la structure de distribution.

En outre, certaines applications multipoint déployées dans les réseaux sans fil, telles que : les champs de batailles, les opérations de secours, l'enseignement en ligne, sont peu sensibles à la contrainte de temps, mais non tolérées aux pertes. En effet, elles, en plus de l'efficacité du routage, exigent une fiabilité totale ou partielle de délivrance de leurs données (garantie indispensable). Cette exigence est la mission d'un protocole de multicast fiable.

De plus, ces mécanismes, qui peuvent être combinés avec protocoles de multicast à moindre effort (best-effort), reposent sur des politiques pour détecter et recouvrir les pertes produises sur plusieurs niveaux afin d'assurer la fiabilité désirée.

En effet, la conception des protocoles de multicast fiable suite deux axes orthogonaux, un axe des mécanismes utilisés pour assurer la fiabilité et l'autre du niveau (couche de la pile des protocoles) sur le quel ils ont été implémentés **[69]**. Dans les suivantes sous sections, nous allons entamer une description de ces deux axes.

5.1 Catégories des mécanismes du recouvrement de pertes

Dans les réseaux sans fil, trois grands mécanismes, offrant chacun un niveau différent de fiabilité, ont été implantés pour la récupération des erreurs détectées comme suit :

5.1.1 Mécanismes basés sur requêtes de retransmission automatique (ARQ-based)

Par analogie aux réseaux filaires, Cette approche peut être aussi implantée dans le contexte des réseaux sans fil. En fait, son principe consiste à retransmettre 'à la demande' les paquets de données supposés perdus. Ceci en se focalisant sur les acquittements, positifs 'ACK' ou négatifs 'NACK', provenant de la part des récepteurs, en mesure de signaler une perte détectée, voire même un état de congestion, et éventuellement d'élaborer une demande de retransmission, ou d'invoquer une procédure de contrôle de congestion.

En plus de deux classes, sender-initiated et receiver-initiated, qui peuvent être envisagées afin de clarifier la responsabilité de la détection des pertes, deux autres questions clés sont notamment soulève lors de la considération de ces mécanismes en conception. La première question relative à l'attribution de la tâche de retransmission des paquets perdus demandés, qui peut être à la charge de la source elle-même pour retransmettre, schéma de retransmission **Sender-originated**, ou être chargée aux récepteurs ou aux nœuds intermédiaires, tout au long de la structure de distribution, en stockant les paquets relayés dans un buffer afin d'accomplir cette tâche. On parle de schéma **Receiver-assisted (neighborhood-oriented)** et **Router-assisted (fixed-neighborhood-oriented)** respectivement**.**

Ces nœuds peuvent être des nœuds fixes spécifiques (stations de base ou point d'accès) dans les réseaux cellulaires, ou n'importe quel membre de la structure multicast du réseau ad hoc.

En outre, le stockage des paquets (mettre en cache) dans une mémoire tampon, la deuxième question, a la tendance d'améliorer la fiabilité. Cependant, Il ouvre toutefois un débat concernant la gestion de la mémoire du stockage à faible capacité dans les nœuds mobiles afin de l'utiliser de façon efficace **[69]**.

Du fait de leur simplicité et leur capacité d'assurer une fiabilité totale de délivrance, les mécanismes basés sur ARQ sont favorisés dans le contexte des réseaux sans fil. Or, ils présentent certaines limites, héritées naturellement des réseaux filaires, notamment **[69]**:

- Un temps de latence important de : détection, recouvrement et délivrance ;
- une gestion complexe de cache qui peut influencer la latence de recouvrement ;
- la disponibilité d'un cache de taille illimitée exigée par la classe receiver-initiated ;
- les problèmes de l'implosion d'acquittements en feedback et du surcoût de retransmission avec un grand nombre de récepteurs couplé par la capacité de diffusion des liens radio ;
- la retransmission des paquets de réparation en multicast (ou en broadcast) conduit aux problèmes de la localité de perte, la congestion et le fardeau administratif dans la source.

5.1.2 Mécanismes basés sur correction d'erreur d'expédition (FEC-based)

Ces mécanismes sont aussi utilisés dans les réseaux filaires. Son principe consiste à diviser les paquets originaux de données en des petits sous-paquets. Afin de reconstruire le paquet original, elle ajoute des informations redondantes (code correcteur) à chaque sous-paquet avant d'être transmit. À partir de ces informations et à la réception d'un nombre suffisant de sous-paquets, le récepteur devra être capable de reconstruire le paquet original des données.

Cette approche est mieux adaptée aux réseaux sans fil dont les liens de communications sont unidirectionnels (technologies GSM et GPRS qui fournissent des liaisons point-à-point), bien qu'elle minimise la latence de recouvrement, mais sur le coût d'une fiabilité partiale. En outre, elle est moins performante en cas de la congestion, génère davantage du trafic réseau, nécessite le savoir les cas échéants de la perte pour être productible **[69, 11]**.

5.1.3 Mécanismes basés sur techniques de dissémination Gossip et épidémique

Le principe de ces mécanismes repose sur une inondation contrôlée de façon probabiliste. En fait, leur idée basée sur un échange cyclique des messages gossip (gossip messages), entre chaque membre du groupe et un sous-groupe gossip (gossip subgroup), aléatoire, des autres membres, afin de détecter et recouvrir les messages perdus. Donc, ils assurent une fiabilité probabiliste. Les messages échangés, peut contenir les paquets de données récemment reçu ainsi que les paquets sollicités, sont transmis en broadcast (diffusion) local pour les nœuds voisins ou en unicast pour un nœud sélectionné au hasard parmi une liste prédéfinie. En effet, les paquets perdus seront recouvrés, en mode paire-à-paire (p2p), à partir du message gossip reçu (qui peut contenir les paquets demandés) ou du message de réparation dédié.

En outre, les performances d'un protocole multicast à base de la technique gossip sont liées étroitement aux paramètres suivants : (1) le choix du sous-groupe gossip approprié pour échanger les messages gossip; (2) l'adoption de la stratégie de retransmission de type fournir (gossip-push) ou celle de type demander (gossip-pull) et (3) la fixation de la période optimale de l'échange gossip **[70]**.

En raison de leur caractère probabiliste, ces techniques semblent tout à fait convenables pour un environnement ad hoc qu'il caractérise par une nature non déterministe. Entre autres, elles sont faciles à déployer, robustes à l'échec, extensibles et indépendantes de la topologie du réseau sous-jacent. Ainsi, elles minimisent la latence de recouvrement mais sur le coût d'une fiabilité probabiliste du fait que les paquets soient probablement délivrés à chaque membre de groupe.

5.2 Niveau (couche) d'implémentation

Sachant que les pertes dans les réseaux sans fil surgissent sur plusieurs niveaux de l'architecture (couche liaison et réseau), les solutions envisagées pour recouvrir ces pertes doivent fournir un service multicast fiable de plusieurs niveaux (fiabilité de bout-en-bout, fiabilité de saut-par-saut). Nous rapprocherons à ces niveaux dans cette section.

5.2.1 Niveau transport

Selon le modèle de conception '**application-layer framing'**, favorisé par le groupe de travail **RMTP** d'IETF, les mécanismes du recouvrement sont implémentés séparément dans la couche transport au dessus des protocoles de routage généraux afin d'assurer une fiabilité de bout-en-bout. Son soucie est d'assurer l'indépendance du protocole de transport multicast fiable de tout protocole de routage multicast sous-jacent, pour bénéficier de toute amélioration de ce dernier. En revanche, cet intérêt est moins intéressant dans un réseau ad hoc du fait que la plupart des nœuds sont à la fois des hôtes et des routeurs. De plus, dans des circonstances où la topologie est dynamique et multi saut, la fiabilité de bout-en-bout peut être perturbée dans les couches basses due aux pertes ou temps de latence **[11]**.

5.2.2 Niveau réseau

Afin d'assurer une meilleure performance dans les réseaux ad hoc, des protocoles de routage multicast fiable, où la fonctionnalité de la fiabilité est intégrée conjointement avec le protocole de routage multicast au niveau de la couche réseau, pourront être implantés sur tous les nœuds (nœuds hôtes et routeurs) de la structure de distribution. Ceci est motivé par l'argument judicieux de bout en bout qui manifeste la possibilité d'implémenter

les fonctionnalités des couches hautes dans les couches basses, pourvue que les caractéristiques des liaisons sans fil et la mobilité des nœuds soient traités efficacement.

5.2.3 Niveau liaison

Les protocoles de multicast fiable, implémentés au niveau transport et réseau, tentent de recouvrir les paquets perdus à cause des problèmes de congestion et de routage, tandis que la majorité des pertes sont produites au niveau liaison dues à la qualité du médium sans fil (propagation du signal) et aux problèmes de collision, d'interférence et de terminale caché. En effet, la couche liaison (couche MAC) a une grande responsabilité pour offrir un support de transmission fiable (liaisons sans fil fiable) pour les communications multicast.

Contrairement aux couches hautes qui assurent une fiabilité de bout-en-bout, la couche liaison implante des mécanismes de recouvrement (basés sur ARQ) pour assurer une transmission faible entre un nœud et ses sauts successeurs voisins à sa portée (une fiabilité de saut-par-saut). Cette fiabilité est souhaitable, car elle réduit le délai de transmission de bout en bout. En revanche, elle peut influencer l'assurance de la fiabilité dans les couches hautes.

5.2.4 Conception inter-couche (Cross-layer)

En vue de la dépendance des transmissions sans fil, toute modification au niveau des protocoles doit être prise avec prudence pour ne pas obérer la performance du réseau.
En effet, les couches d'une architecture sans fil doivent être coordonné pour s'adapter au changement de l'état du réseau sous jacent.

Le principe de conception inter-couche (cross-layer) permet aux couches d'échanger des informations d'état afin d'adapter et d'optimiser la performance du réseau. Autrement dit, le partage de l'information permet à chaque couche d'avoir une image globale des contraintes et des caractéristiques du réseau, afin de se coordonner pour prendre les meilleures décisions optimisant les performances du réseau **[11]**.

Avec la synthèse de l'union des deux axes précédents, nous pouvons constater que plusieurs protocoles de multicast fiable puissent être développés. Ces derniers n'ont pas de **one-size-fits-all** où ils supportent les besoins spécifiques des applications spécifiques.

Par analogie aux réseaux filaires, ils doivent considérer les points critiques suivants: le facteur d'échelle 'la scalabilité', le contrôle de congestion, l'hétérogénéité des nœuds et la sécurité **[19]**. En outre, ils doivent résoudre les problèmes inhérents à une communication de groupes qui surgissent à grande échelle tels que : l'implosion en feedback des paquets

de contrôle, la répartition de la charge de recouvrement des pertes, l'exposition des récepteurs et l'influence des récepteurs de faible capacité sur le groupe (drop to zero) **[26]**.

Dans les réseaux sans fil avec infrastructure, comme nous avons vu, le phénomène de handover (changement intercellulaire) et l'éloignement de la station de base des nœuds mobiles peuvent motiver la perte des paquets de données multicast. Cependant, les solutions envisagées, de multicast fiable, sont basées sur les nœuds fixes ou les stations de base (administration centrale) pour la retransmission des paquets perdus. Nous notons notamment le développement des protocoles multicast fiable **RMDP [71]** et **RM2 [72]** dans ce contexte.

En revanche, l'absence de l'infrastructure-fixe et de l'administration centrale, le taux élève des pertes de différentes natures, par rapport aux réseaux sans fil avec infrastructure, et les caractéristiques relatives aux réseaux sans fil ad hoc vont compliquer les choses. Ces contraintes mettent des défis contre l'adoptation des protocoles multicast fiable et rendent l'offre du service multicast fiable un problème important que nous devrons traiter.

5.3 Multicast fiable dans les réseaux sans fil ad hoc

Dans les réseaux ad hoc, comme susmentionné, la congestion, une topologie dynamique et multi-saut et les contraintes d'énergie et des ressources de faible capacité de leurs nœuds conduisent à des pertes imprédictibles, et des challenges que nous allons présenter.

5.3.1 Enjeux et défis de la conception d'un protocole de multicast fiable

Les caractéristiques des réseaux ad hoc imposent un travail davantage pour concevoir et développer des mécanismes de multicast fiable mieux adaptées aux enjeux suivants **[73]**:

- **Changements fréquents et imprévisibles de la topologie** *:* pour qu'un protocole puisse s'adapter aux changements fréquents et imprévisibles, il doit générer des messages de contrôle en fonction des informations autour de la topologie prélevées de réseau sous-jacent. En effet, le réseau pourra congestionner en obstruant la délivrance des paquets de données. Par ailleurs, le protocole doit minimiser son besoin d'information instantanée d'état au sujet du réseau pourvu qu'il soit robuste et s'adapter à l'environnement dynamique.
- **Congestion et collision** *:* dans un réseau ad hoc, les nœuds se communiquent par le biais d'un médium sans fil partagé (zones de couverture en intersection). Dû essentiellement à la nature broadcast du lien radio, ce partage peut mener aux problèmes de concurrence d'accès et interférences entre les nœuds voisins (s'il y a des paquets à transmettre) en résultant le phénomène de la collision au niveau des nœuds récepteurs. Cette situation peut être

aggravée avec un grand nombre de nœuds dans les réseaux denses. Dans ce contexte, le réseau peut être congestionné, en fonction du trafic de réseau, du fait de dépassement des capacités de buffers au niveau des nœuds surchargés. cependant, le protocole de multicast fiable doit prendre en compte le contrôle de congestion et de flux afin d'améliorer les performances du réseau et d'assurer un partage équitable des ressources de réseau.

- **Les contraintes de l'énergie et de la bande passante**: Dans des scénarios denses, le nombre de transmissions peut être augmenté en générant des données redondantes et un overhead de contrôle. Cette situation résulte un gaspillage des ressources limitées (bande passante et énergie). En effet, les protocoles de multicast fiable doit minimiser le nombre des nœuds concernés par la transmission ainsi que les messages de contrôle générés afin de préserver la bande passante et de maximiser la durée de vie de nœuds.

Etant donné la forte mobilité des nœuds, l'approche d'inondation (*flooding*) reste viable pour servir la fiabilité désirée. Avec l'augmentation de la mobilité, cette inondation soulève un problème d'insuffisance, en cédant la voie aux autres alternatives de multicast fiable.

5.3.2 Protocoles de multicast fiable

Pendant les dernières décennies, une pluralité de protocoles ont été développés dans la littérature en raison des exigences très diverses des applications multicast. Ces protocoles sont classés selon leur garantie de fiabilité en deux grandes classes, à savoir, **protocoles déterministes** et **ceux probabilistes.** Nous détaillons par la suite les plus cités **[73, 74]:**

A. Protocoles déterministes

Dans cette classe, les protocoles garantissent la délivrance réussite de tous les paquets de données (100% de paquets délivrés) selon le critère 'accepter par tous ou aucun', où le paquet reçu ne sera délivré que tous les autres membres l'aient accepté.

A.1 Protocole RMA (Reliable Multicast Algorithm)

Le protocole RMA **[75]** est un protocole basé sur la stratégie ARQ (ACK-based) de famille sender-initiated qui assure la délivrance fiable des messages à plusieurs récepteurs dans un réseau MANET. RMA suppose que les sources aient une connaissance totale de tous les membres d'une (des) session(s) multicast par le biais des informations d'adhésion maintenues dans la table multicast au niveau de chaque source, où chaque nœud du réseau peut joindre, via la diffusion du message JOIN, ou quitter, via la diffusion du message LEAVE, une session multicast à tout moment. Pour qu'il puisse acheminer les messages

multidestinataire, RMA repose sur une structure de graphe pondéré non orienté et des informations de routage maintenues dans la table de routage, < Destination IP Address, Next Hop IP Address, Bandwidth of the link, Lifetime of the link, Membership count of the link >, au niveau de chaque nœud du réseau, de sorte que le chemin optimal soit sélectionné en basant sur la métrique de la durée de vie (life time) afin d'améliorer la fiabilité des opérations de routage multicast. La connectivité entre les nœuds est assurée via la diffusion périodique des messages HELLO tandis que les tables de routage et de multicast vont être mises à jour pendant la propagation des messages d'appartenance (JOIN, LEAVE) et d'acquittement (MACK, BMACK).

Lorsqu'une source désire envoyer des données, elle transmit, à une liste extraite des membres de la session multicast à laquelle la source est adhérée, en unicast des messages MKNOWN aux récepteurs ayant des adresses inscrites comme des adresses de destination dans la table de routage de la source, et en diffusion des messages MUNKNOWN aux autres membres non atteignables par la source. Plusieurs adresses destinations qui se partagent le même saut suivant (next hop), peuvent être agrégées dans un seul message, tout en aboutissant au minimum le nombre des messages expédiés et minimisant la consommation de la bande passant. Après l'envoie de ces messages, la source arme un délai d'attente 'WAIT_TIME' dans lequel elle collecte les acquittements (ACKs plats) provenant des récepteurs. À la réception d'un message MKNOWN par un nœud intermédiaire, il va actualiser sa table de routage par les nouvelles informations tout en le relayant s'il existe une route valide ou le diffusant autrement (vise versa pour le message MUNKNOWN). Tandis que, sa réception par un récepteur engendre l'émission, en retour, d'un message d'acquittement MACK à la source si le chemin inverse est validé, ou la diffusion d'un message d'acquittement BMACK. À l'expiration du délai armé sans avoir collecté les acquittements de tous les membres de la session, la source va déclencher un processus de retransmission.

a. Technique de recouvrement des pertes

Une fois que la source détecte l'absence d'un ou plusieurs acquittements, elle constate que le message multicast envoyé soit perdu. Donc, elle va entreprendre son retransmission, selon le schéma de retransmission Sender-originated, aux membres qui n'ont pas encore acquittés où elle procède à l'envoie du message MUNKNOWN avec un drapeau 'RETRANSMIT' (indicateur de retransmission). Si un récepteur reçoit ce message pour la première fois, il va répondre à la source avec un message d'acquittement MACK via le chemin inverse préétabli,

ou avec un message d'acquittement BMACK en diffusion autrement. Cette procédure est répétée un nombre prédéfini de tentatives jusqu'à la collection de tous les acquittements.

b. Limites du protocole RMA

- Étant basé sur la classe sender-initiated, le protocole va souffrir du problème d'implosion d'acquittements en feedback et un énorme fardeau administratif au niveau de la source dû à l'absence de la contrôle de congestion, tout en limitant sa scalabilité.
- la connaissance totale de l'ensemble des récepteurs suggérée par le protocole réduise négativement le gain du multicast.

En effet, le protocole RMA a eu mauvais compromis entre la fiabilité et le passage à l'échelle.

A.2 Protocole ReACT (Reliable, Adaptive, Congestion-Controlled Adhoc Multicast Transport)

Le protocole ReACT **[76]** est un protocole de transport développé afin d'assurer une livraison multicast fiable et en temps opportun dans certains scénarios de réseaux MANET. Son idée principale est de surmonter les insuffisances du protocole RALM **[77]**, avec la contribution de la récupération des pertes issues des différentes sources (congestion, erreurs de transmission). Pour cela ReACT utilise les informations fournies, auprès de l'échantillonnage de la file d'attente sur chaque récepteur multicast au niveau MAC, pour différencier les sources de ces pertes et, notamment, pour déterminer le mécanisme de recouvrement convenable (source-based recovery ou receiver-initiated localized recovery).

a. Technique de recouvrement des pertes

Afin de recouvrir les pertes issues de différentes sources, le protocole ReACT introduit deux composants principaux :

- **Recouvrement basé sur la source (Source-based recovery):** Ce composant assure le recouvrement des paquets perdus dus à la congestion globale du réseau sous-jacent, selon le schéma de retransmission Sender-originated. Initialement, et avec l'hypothèse d'éviter la congestion dés le début, la source envoie les paquets de données en multicast à une vitesse de transmission spécifiée par l'algorithme de contrôle de congestion et elle maintienne une liste 'Receiver List' vide. À la réception d'un paquet, le récepteur le stocke dans son tampon (buffer) puis le délivrera à la couche applicative dans un ordre séquentiel. À la détection de la situation de congestion signalée par un NACK provenant de la part d'un récepteur donné, la source constate que les paquets soient probablement perdus. Dans ce cas, elle va entreprendre à la réparation des pertes tout en: ajoutant ce récepteur dans la liste

“Receiver List”, gardant trace du temps de latence de bout en bout via l'horodatage (timestamp), collectant les NACK générés toutes les ‘MIN_FEEDBACK _INTERVAL’secondes et diminuant sa vitesse de transmission. Dans cette phase, elle émet un nouveau paquet ou retransmit en multicast un paquet de réparation au feedback receiver (sélectionné de la liste des récepteurs) qui est le seul autorisé de y répondre, en basant sur l’approche envoyer– et–attendre (send -and-wait), avec un ACK en unicast indiquant le numéro de la séquence du paquet demandé, ou l’obtention de tous les paquets avec succès. Avec l’obtention de tous les paquets demandés, le feedback receiver va être retiré de la liste en choisissant un autre de façon circulaire (round-robin). Cette procédure sera répétée jusqu’à ce que la liste soit vidée tout en réajustant la vitesse de transmission à la valeur initiale.

- **Recouvrement local (Local Recovery):** additivement au recouvrement basé sur la source, ReACT introduit un mécanise de recouvrement local où les paquets perdus, dus aux erreurs de transmission, sont recouvris localement à partir des membres proches selon le schéma de retransmission Receiver-assisted. Le souci de ce composant est d’empêcher la source de réduire sa vitesse de transmission inutilement, de la décharger d'une partie significative du processus de retransmission tout en distribuant équitablement la charge de recouvrement entre la source et les récepteurs, de minimiser la portée de la retransmission et la latence de recouvrement et de préserver le délai de livraison de bout en bout.

En fait, chaque membre du groupe maintient dans une table de membres ‘membre table’ :< member Id, Route, Hop Count, Is Congestion, Reliability, Timestamp >, des informations autour ses parents membres immédiats ayant le potentiel d’être des nœuds de recouvrement (recovery node), qui vont être mises à jour via les champs < memberId, reliability > de l’en tête du paquet de données multicast véhiculé.

À la détection d’une perte de paquets, avec une hypothèse de perte de transmission, le récepteur tente d’abord de la réparer localement. Pour cela, il s’échange des paquets de requête/réponse avec un nœud de recouvrement sélectionné depuis sa table des membres, en choisissant le nœud à jour, non-congestionné, le plus proche (un nombre minimum de sauts) et ayant la plus haute fiabilité. Ce dernier peut répondre s’il avait les paquets demandés, ou rejeter la demande autrement. À la réception d’un rejet de demande, le récepteur demandeur va répéter la procédure en choisissant un autre nœud de recouvrement. Dans le cas échéant, où le nœud concerné par la perte est congestionné (sa file d’attente MAC est débordée) ou l’ensemble de leur nœuds de recouvrement sont congestionnés, il envoie un acquittement négatif (NACK) pour signaler la congestion à la source, qui va déclencher le processus de recouvrement basé sur la source.

b. Contrôle de congestion

ReACT utilise un schéma de contrôle de congestion basé sur la vitesse où le trafic est envoyé à une vitesse prédéfini jusqu'à la détection de la situation de congestion menant au réajustement de la vitesse de transmission.

Tout d'abord, la source transmet initialement les paquets de données à la vitesse estimée pendant la période de sondage, avec un paquet de sondage. À la réception d'un NACK provenant d'un récepteur donné, la source le considère comme un signal de congestion globale du réseau tout en invoquant une procédure de retransmission couplée avec un processus de contrôle de congestion afin de réajuster sa vitesse de transmission (régulier le taux d'envoie) jusqu'à l'élimination de ce signal, où elle reviendra au taux initial d'envoi.

c. Limites du protocole ReACT

- Les problèmes de la localité de perte et l'exposition de retransmission où certains récepteurs peuvent être submergés par le traitement inutile des paquets de données déjà reçus en vue de l'envoie des réparations en multicast.
- L'écroulement de la source et le problème de l'implosion des NACKs en feedback avec l'échec répétitif du processus de recouvrement local (après plusieurs tentatives).
- la difficulté de déterminer la source des pertes (la congestion ou les erreurs de transmission) et de les détecter (jusqu'à l'arrivée du prochain paquet de données) dans un environnement ad hoc hostile.

A.3 Protocole ReMHoc (A Reliable Multicast Protocol for Wireless Mobile Multihop Ad Hoc Networks)

ReMHoc **[78]** est un protocole de transport multicast fiable, de la classe receiver-initiated, basé sur NACK qui tente d'assurer une délivrance éventuelle de données multicast pour tous les membres du groupe multicast. Son idée de base est inspirée du protocole SRM **[35]** de réseaux filaires où il utilise un mécanisme de suppression basé sur les temporisateurs aléatoires (random timer-based) et distribue le fardeau (la charge) du recouvrement sur tous les membres du groupe (schémas de retransmission Sender-originated et Receiver-assisted).

Chaque source envoie en multicast des paquets de données 'DATA', ayant des numéros de séquence croissants, vers tous les membres du groupe multicast où ils gardent en cache une copie de chaque nouveau paquet DATA bien reçu. après la réception d'un ensemble de paquets DATA consécutifs, certains récepteurs peuvent détecter la perte des paquets dont leurs numéros de séquence sont manqués. En effet, chacun récepteur demandeur

“requestor” arme séparément son temporisateur de demande ’request timer’ avec le nombre des sauts entre la source et lui. Le récepteur demandeur dont son ‘request timer’ est expiré en premier lieu, le plus proche de la source, envoie immédiatement en multicast un acquittement négatif “REQUEST” afin de demander la retransmission du paquet DATA perdu. Les autres récepteurs, qui ont également les mêmes demandes de réparation, entendent cette demande et suppriment les siens en réinitialisant leurs temporisateurs.

N'importe quel membre du groupe (source ou récepteur) qui a une copie en cache du paquet DATA demandé, initialise d’abord son temporisateur de réparation ’repair timer’ avec le nombre des sauts entre ce récepteur et le “requestor”, puis il attend son expiration. Le récepteur répondeur “replier” dont son “repair timer” est expiré en premier lieu, le pus proche du récepteur demandeur, envoie immédiatement en multicast son ‘REPAIR’. Les autres récepteurs qui peuvent aussi y répondre à la demande entendent ce paquet de réparation tout en désarmant leurs temporisateurs (ils se comportent comme s’ils ont déjà les envoyés). Cette solution est particulièrement robuste quant au changement de topologie, minimise la latence de recouvrement, réduise la duplication inutile des paquets de réparation et empêche le problème d'implosion de requête et de réparation, tout en assurant une scalabilité maximale.

En outre, si un récepteur n'a pas reçu le dernier paquet ‘END’ pendant une longue durée, il déclenche un temporisateur de pulsation ‘heartbeat’. À l’expiration de celui-ci, il expédie en multicast un paquet ’HB’, aux membres du groupe. Chacun membre va chercher dans son cache l’existence d’une copie dont son numéro de séquence est supérieur à celui indiqué dans ce paquet. Si c’est le cas, il réagit comme le cas de réparation par l’envoie du paquet REPAIR_END, tout en assurant la mise à jour de la réception des paquets DATA manquants.

a. Limites du protocole ReMHoc

Étant basé uniquement sur les NACK, l’inconvénient majeur de ce protocole réside dans le problème de la localité de réparation et l’exigence d’un cache de taille illimitée, entre autre:

- l’émission des paquets de contrôle et de réparation en multicast nécessite une structure de distribution propre à chaque membre du groupe qui va créer un overhead additionnel au niveau du protocole de routage multicast sous-jacent.
- L’overhead de contrôle dû à l’absence d’un nombre limité de demandes de retransmission.
- le dysfonctionnement du protocole dans un environnement fortement mobile dû à la dépendance des temporisateurs de demande et de réparation au nombre de sauts.

A.4 Protocole ARMPIS (Active Reliable Multicast Protocol with Intermediate node support)

Le protocole ARMPIS **[79]** est un protocole de transport multicast fiable basé sur la stratégie ARQ (NACK), de la classe receiver-initiated. Le protocole s'articule sur l'aspect actif des nœuds intermédiaires (le support des routeurs actifs) afin d'améliorer la fiabilité de communication multicast à grande échelle dans un environnement ad hoc. Les nœuds intermédiaires regroupent: les membres de groupes, les nœuds routeurs (convoyeurs des paquets de données) et leurs voisins (à leur portée de transmission). C'est-à-dire tous les nœuds qui entendent les paquets de données multicast.

Tout d'abord, la source envoie en diffusion (broadcast) des paquets originaux de données, avec numéros de séquence consécutifs, qui vont être livrés aux membres du groupe par le biais du protocole de routage multicast MRDC. Pendant l'acheminement des paquets de données et avant de les rediffuser, chaque nœud routeur intermédiaire, pour la première fois, met de façon probabiliste une copie en cache, établie le chemin inverse vers la source et actualise sa 'liste de paquets relayés' avec les informations nécessaires (inclus dans l'entête du paquet) pour éviter son traitement autre fois. Dans le cas échant (un paquet original de donnés ou de réparation dupliqué), il va le rejeter. Notant que chaque paquets de données rediffusé par un nœud routeur soit entendu par ses voisins qui ont à leur tour le mettent en cache avec une probabilité. À l'insu, si un récepteur donné détecte la perte d'un ou plusieurs paquets de données, il va déclencher une technique de recouvrement (récupération).

a. Technique de recouvrement des pertes

À la détection des pertes au niveau d'un ou plusieurs récepteurs, ils demandent leur retransmission via des NACK générés. Un message NACK peut contenir: <identificateur de groupe (@groupe), identificateur de source (@source), liste de références> où chaque référence correspond à une requête (demande) de retransmission. Dés qu'un récepteur détecte des numéros de séquence manquants, il va les inscrire dans le tableau de réparation 'local repair array' et exécuter l'algorithme de recouvrement suivant:

- il vérifie régulièrement son tableau local de réparation. **Si** ce dernier n'est pas vide **alors:**
  - il émet un NACK en diffusion locale, contenant les 'L' premiers numéros de séquence, à ses voisins immédiats tout en armant un délai d'attente;
  - il met ces 'L' numéros de séquence dans le tableau des requêtes 'request array';
  - il supprime du tableau des requêtes, pendant le temps d'attente, les numéros de séquence des paquets de réparation reçus;

- À l'expiration du délai d'attente, **s'**il reste encore quelques numéros de séquence dans son tableau des requêtes **alors:**
  - il engendre un message NACK en unicast, incluant ces numéros comme références, au saut suivant sur le chemin inverse vers la source;
  - et ajout aussi ces numéros au tableau d'envoie 'sent array'.
- À la réception d'un NACK en unicast par un nœud routeur en amont, il:
  - cherche d'abord les paquets demandés dans son cache pour y répondre.
  - supprime les numéros de séquence qui apparaît aussi dans ses tableaux (de réparation, des requêtes et d'envoie) ;
  - met les numéros de séquence restants dans 'local repair array' pour agréger les NACKs;
  - retire les informations correspondantes à ces numéros de sa 'liste de paquets relayés' pour qu'il puisse retransmettre les paquets récupérés pour une deuxième fois;
  - enfin, il envoie un NACK en diffusion locale, incluant les numéros de séquence stockés dans son tableau local, pour interroger ses voisins.

De la même façon, les étapes précédentes seront répétées jusqu'à ce que tous les paquets demandés soient trouvés ou un message NACK en unicast atteigne la source, qui a le potentiel de recouvrir tous les paquets demandés restants. De plus, le protocole de routage multicast livre en diffusion les paquets de données, de la qualité 'réparation' indiquée par un drapeau dans l'en-tête du paquet, aux nœuds demandeurs, en transitant seulement les nœuds routeurs n'ayant pas des informations concernantes le paquet relayé. En constatation, ARMPIS distribue la charge de retransmission de sorte qu'il combine les schémas de retransmission Sender-originated, Receiver-assisted et Router-assisted, et limite la portée de retransmission sur des zones géographiquement fermées pourvu d'alléger le problème de localité de perte.

b. Stratégie de gestion du cache

Avec le protocole ARMPIS, chaque nœud maintien un tampon mémoire qui sert comme une cache des paquets reçus, gérée selon la stratégie 'FIFO probabiliste'. Lors de la réception d'un paquet de données, le nœud interroge un générateur de valeur aléatoire de distribution uniforme pour générer un nombre aléatoire entre 0 et 1. Si le nombre aléatoire est plus petit à une certaine probabilité 'p', le nœud stocke ce paquet en le mettant selon la stratégie FIFO (premier arrivé premier servi). Sinon, le paquet sera délivré sans être stocké. L'idée derrière cette technique est d'assurer une cache distribuée des paquets de données avec un nombre minimum de paquets dupliqués en cache, en dépite de la limitation de mémoire (capacité de stockage) et de la mobilité des nœuds intermédiaires.

c. Limites du protocole ARMPIS

- La durée de vie du buffer de cache est inversée proportionnellement à la charge du trafic qui est augmentée linéairement avec une haute probabilité de cache.
- Plusieurs nœuds candidats pour la retransmission du paquet perdu peuvent entrer en collision au niveau du récepteur en augmentant davantage le surcoût de retransmission.
- Le problème d'exposition des récepteurs existe toujours, car les paquets de réparation seront retransmis en broadcast (délivrés par le protocole de routage sous-jacent).
- La vérification périodique des tableaux de numéros de séquence dans les nœuds intermédiaires résulte une consommation de leurs capacités de traitement et d'énergie.
- Le problème de la tempête de diffusion 'Broadcast Storm' des paquets de contrôle et de réparation qui peut être aggravé dans les scénarios du réseau dense et à grande échelle.

A.5 Protocole STRM (Source Tree Reliable Multicast for Ad-Hoc Networks)

Le protocole STRM **[80]** est un protocole de transport multicast fiable de la classe receiver-initiated basé sur ACK périodique et développé pour supporter les applications basées sur le transfert des données en masse (fichiers, images, paquets de logiciel) dans un réseau ad hoc, afin de garantir la délivrance d'une séquence contigüe ordonnée des paquets de données d'un seul expéditeur à multiples récepteurs. Le protocole STRM adopte une approche basée sur arbre "Tree-based' du réseau Internet où il construit un arbre de contrôle logique (ACK tree) au niveau transport, au dessus d'une structure maillée multicast de distribution de la couche réseau sous-jacent, pour la réparation locale d'erreurs et l'évitement du problème de l'implosion des ACK en feedback. La racine de cet arbre est l'expéditeur tandis qu'il regroupe les récepteurs dans des groupes locaux dont le leader de chacun représente un serveur de réparation "Forward Server (FS)", qui a la responsabilité de réexpédier les paquets de données multicast provenant de l'expéditeur vers, et d'agréger des ACKs hiérarchiques depuis, tous les récepteurs de son groupe local dans un intervalle régulier. Son idée innovatrice, en face de la mobilité dans les réseaux MANET, est la sélection dynamique des nœuds FS à partir de l'ensemble des nœuds fils de l'expéditeur (y compris l'expéditeur lui-même), en utilisant l'algorithme "Selection Forward Server Process (SFSP)". Après un nombre défini de tentatives et à l'absence d'un ACK de l'un des nœuds FS, il constate que celui-ci soit en dehors de sa portée radio tout en réexécutant l'algorithme de sélection.

a. Comportement des différentes entités du STRM

- **Entité d'expéditeur:** l'expéditeur découpe les blocs de données en paquets de données de taille fixe, qui portent des numéros de séquence partant de '0'. Ensuite et dans un intervalle

de temps régulier T_{send}, il transmit en multicast, avec un taux limité à: W_s * Packet_size / T_{send} et en fonction des places disponibles dans la fenêtre de transmission 'transmission window (W_s)' et des tampons de FS, un nombre limité des paquets de données vers ses nœuds FS qui vont à leur tour les réexpédier vers les récepteurs de leurs groupes locaux avec une copie gardée en cache pour assurer le recouvrement local des pertes par la suite. À l'insu, l'expéditeur arme un délai d'attente, égale au temps d'envoie d'un paquet ACK, pour recevoir les ACKs de ses nœuds FS où les paquets de données acquittés seront mis dans la fenêtre de mémorisation 'memory window (W_m)'. À l'expiration de ce délai sans la réception de tous les acquittements, il suppose qu'une perte soit produite tout en retransmettant le paquet.

- **Entité de récepteurs :** à l'instar d'expéditeur, les récepteurs utilisent chacun une fenêtre de réception 'receive window(W_r)' pour stocker les paquets de données qui ont été reçus mais ne forment pas ensemble une suite contigüe de séquences (unité des données d'application (ADU)) pour être délivrés à la couche applicative. Par ailleurs, chaque récepteur envoie, à chaque période T_{ack} , un paquet de contrôle (ACK) au nœud FS ascendant de son groupe locale tout en lui informant par les paquets bien reçu et ceux qui sont manqués.

b. Technique de recouvrement des pertes

Le protocole STRM met en œuvre une retransmission sélective de paquets, qui se focalise sur un bit-map 'B' (liste binaire de taille 'W_r '). La valeur 'N'du dernier bit de la liste 'B' indique la bonne réception des paquets, dont le numéro de séquence inférieur à 'N', alors que les numéros de séquence supérieurs à 'N' et indiqués par la valeur '0' dans cette liste permettent la détermination des paquets manqués par l'expéditeur et les nœuds FS. En fait, l'expéditeur et chaque nœud FS vérifient à chaque T_{retx} leurs files d'attente de retransmission 'Q_{retx}' comportant le numéro de séquence et liste des récepteurs demandeurs du paquet. Si le nombre des demandeurs est supérieur à un seuil donné, le paquet de réparation sera retransmit en multicast. Or, il sera retransmit en unicast vers les récepteurs concernés.

c. Limites du protocole STRM

- l'arbre logique construit est moins robuste aux changements de la topologie du réseau.
- l'exigence de mettre en cache tous les paquets de données reçu, provoque le débordement de la mémoire tampon de nœuds FS.
- la source et ses liens deviennent surchargés en affectant les performances du réseau.

A.6 Protocol HCP (Hop by Hop Multicast Transport for Mobile Ad Hoc Wireless Networks)

HCP (Hop-by-Hop Congestion Protocol) **[81]** est un protocole de transport multicast fiable, qui fournit ainsi un contrôle de congestion de saut-par-saut (hop-by-hop) pourvu d'éviter l'influence du rythme de récepteur le plus lent. À l'opposition des approches précédentes, il implante aussi ces fonctionnalités (de niveau transport) dans le corps du réseau sous-jacent où en plus de la commutation de paquets, chaque nœud routeur de l'arbre multicast assure une fiabilité de saut-par-saut et contribue dans le processus de contrôle de congestion.

Pour chaque flux (identifié par la couple(S, G)) et au niveau de chaque nœud, HCP fait recourir sur le protocole routage multicast ASSM (Ad hoc State Setup Multicast Protocol) pour établir l'état d'acheminement multicast (multicast forwarding state) et les buffers par flux, pendant la propagation du message ASSM Join dans l'arbre multicast. Bien qu'il établie l'état de transport (transport state) et alloue un tampon applicatif (couche application). Après l'établissement d'états et suite à l'arriver des paquets de la couche d'application (cas de la source) ou de parent dans l'arbre multicast, HCP met ces paquets dans le tampon associé. Avec l'algorithme d'ordonnancement de traitement d'attente équitable 'Fair Queueing(FQ)', l'ordonnanceur (Scheduler) va servir de façon cyclique ces paquets en fonction d'informations (feedback) en provenance de la couche MAC, de sorte qu'il empêche le débordement de la file d'attente IP (au niveau réseau). Ensuite et afin de les réexpédier, HCP choisira aléatoirement un nœud parmi la liste des nœuds fils, au quel le paquet vaut envoyer en unicast à l'aide de l'échange de RTS/CTS au niveau MAC (un schéma de diffusion semi-fiable) tout en mémorisant une copie de chaque paquet transmit avec succès. Alors que les nœuds fils restants reçoivent le paquet à travers l'écoute promiscuité. En effet, multiples nœuds descendants reçoivent quelques paquets de façon fiable au niveau MAC (fiabilité de saut-par-saut) et d'autres par 'snooping'. Ceci à la tendance d'améliorer la fiabilité de bout en bout au niveau supérieur par l'exploitation de l'avantage de multicast sans fil, mais sur le coût que certains paquets seront probablement perdus.

a. Technique de recouvrement des pertes

À la détection des numéros manquants de séquence, HCP va demander la retransmission des paquets perdus directement de la source à l'aide des acquittements négatifs 'NACKs' (schéma de retransmission Sender-originated). Pour cela, le récepteur demandeur met un conteneur 'request container' des couples (L1, L2) des paquets manquants, dans le message périodique ASSM Join de rafraichissement. Pendant sa propagation, HCP examine son conteneur

et détermine l'existence des paquets demandés dans le buffer approprié. Les paquets existes vont être planifiés pour la retransmission en les enfilant dans la file de retransmission et supprimant leurs couples proprement dit depuis le conteneur, pou éviter sa duplication. S'il reste encore des tuples, le mécanisme ASSM va poursuivre la transmission du message en amont jusqu'à la source qui va répondre éventuellement aux demandes restantes. Cette manière de faire réduit le nombre de paquets de contrôle circulés. Quant à la retransmission des paquets, HCP les traite avec la même priorité (égalité) qu'un nouveau paquet à transmettre en aval. Pour cela l'ordonnanceur enfile un paquet de la file de retransmission pour être retransmit vers le récepteur concerné tout en offrant une fiabilité de bout-en-bout.

b. Contrôle de congestion

HCP implante un mécanisme de contrôle de congestion de saut-par-saut basé sur le crédit, de sorte que le taux de transmission varié relativement aux différentes bandes passantes disponibles. Chaque nœud (source et nœuds routeurs de l'arbre multicast) maintient des compteurs des buffers disponibles par flux autant de ses nœuds voisins en aval. Les valeurs de ces compteurs seront actualisées via les informations du buffer disponible récupérées par l'écoute promiscuité (snooping), pendant le relayage d'un paquet par un nœud fils qui sert comme un feedback passif. En effet, relativement à ces informations un nœud peut transmettre un nouveau paquet à ces nœuds fils qui ont possédé des espaces disponibles supérieures au seuil 'available-thresh', ou il attend jusqu' à leur obtention des espaces au-delà du seuil. Ceci empêche le débordement des tampons des nœuds descendants.

c. Limites du protocole HCP

- un récepteur est obligé d'attendre le prochain message généré afin de signaler la perte.
- la gestion de mémoire tampon au niveau de l'application reste un défi.
- la duplication de retransmission et le problème de sécurité.

B. Protocoles probabilistes

Au contraire des protocoles déterministes, ces protocoles tentent d'atteindre un taux élevé de livraison avec une grande probabilité. En outre, ils font recourir à des hypothèses restrictives quant à la connaissance totale des membres de groupe ou de la topologie de réseau sous-jacent, ainsi qu'à une récupération de paquets perdus basée sur l'échange des messages Gossip en mode paire-à-paire (p2p) selon le schéma '*Receiver-assisted*'. En générale, ils ont conçus pour les applications qui ne sont pas sensibles à des petites incohérences entre les participants.

B.1 Protocole RDG (Route Driven Gossip)

Le souci du protocole RDG **[83]** est d'assure un multicast fiable probabiliste dans les réseaux Ad hoc. Il fonctionne au sommet d'un protocole de routage unicast ad hoc à la demande (DSR (Dynamic Source Routing) en supposition), qui lui fournit des informations de routage utiles pour le processus de gossip. Ce protocole est utile par de nombreuses applications critiques, notamment les services de sécurité (la gestion des clés distribués, la distribution de certificat pour les infrastructures à clé publique). Au contraire du protocole AG **[82]**, RDG se repose uniquement sur des vues partielles autour des membres du groupe. Dans la session 'JOIN' les nœuds peuvent rejoindre le groupe comme suit:

- Le nœud qui souhaite joindre un groupe annonce son existence pour les autres membres du groupe en inondant le réseau avec le message 'GROUP REQUEST'.
- À la réception de ce message, les autres membres vont actualiser leurs vues actives (AView) avec l'(ID) du nouvel membre et pourront également répondre, avec une probabilité 'P_{reply}', par le message 'GROUP REPLY'.
- Après avoir reçu la réponse 'GROUP REPLY', l'initiateur met également à jour son (AView).

Après la jonction au groupe et durant la session 'GOSSIP', chaque membre exécute périodiquement (tous les T ms) une tâche de commérage (gossip task) pour la dissémination et la retransmission des paquets de données où ils s'échangent des messages gossip en mode 'push' conduit par une route spécifiée 'route-driven'. Dans cette tâche, chaque membre doit:

- générer un message gossip qui inclut les paquets stockés dans Buffer.new, l'identificateur (pid) du paquet manquant le plus récent, les membres qui ont quitté le groupe (leurs ID indiqués dans le champ 'rview') et les nouveaux membres du groupe;
- envoyer le message généré à un ensemble 'F' (fanout) d'autres membres choisis au hasard à partir de sa vue active (AView) en empruntant les routes rapportées par le protocole de routage unicast sous-jacent;
- supprimer le paquet de données qui a été disséminé plus qu'un τ_q (quiescence threshold) nombre de fois du 'Buffer.new' et l'ajouter dans le 'Buffer.old'.

Dés qu'un membre du groupe reçoit un message gossip, il va :

- supprimer le membre obsolète à partir de ses vues active(AView) et passive (PView);
- ajouter ce dernier à Remove View (RView) ;
- ajouter le nouveau membre du groupe à sa vue ;
- mettre à jour le tampon 'Buffer.new' avec les nouveaux paquets et les délivrer à la couche sus-jacente;
- répondre à l'initiateur du message quant à paquet sollicité.

a. Technique de recouvrement des pertes

À l'opposition de l'hypothèse que l'initiateur pourra les récupérer autrement via le processus de gossip, les paquets manquants seront recouvris durant la session 'GOSSIP' selon deux cas :

- Le membre recevant le message gossip peut retransmettre le paquet sollicité en réponse si ce paquet ne serait disséminé une autre fois (stocké dans le tampon 'Buffer.old').
- Un paquet reçu en réponse sera délivré à la couche supérieure à condition qu'il soit encore manqué. Le tampon 'Buffer.old' sera met à jour aussi en conséquence.

b. Limites du protocole RDG

- L'utilisation d'une technique probabiliste n'assure que les paquets soient probablement délivrés aux membres du groupe (fiabilité probabiliste).
- Ainsi, son utilisation dans plusieurs cycles peut engendrer des données redondantes dans les réseaux ad hoc denses.

B.2 Protocole EraMobile (Epidemic-based Reliable and Adaptive multicast for mobile ad hoc networks)

Le protocole EraMobile **[84]** adopte une approche épidémique bio-inspirée qui se repose sur la propagation des messages gossip afin de garantir la livraison à tous les récepteurs. Par analogie à la propagation d'une rumeur ou d'un virus (infection aléatoire de proche en proche à portée locale), il distribue la charge de la dissémination de données entre les nœuds, sans recourir à une inondation ni aux chemins de routage prédéfinis (aucune structure de distribution n'est maintenue). EraMobile supporte les applications orientés groupe fiables et moins-sensibles au facteur du délai de livraison. Au contraire aux protocoles AG **[82]** et RGD **[83]**, Il ne nécessite pas une vue partielle ou global sur le réseau ni des informations supplémentaires sur les nœuds voisins ou les membres du groupe pour l'échange du message gossip. Son processus de fonctionnement se déroule en cycles de commérage (gossip rounds), initiées par un temporisateur gossip en fonction du paramètre 'gossip interval'. En générale, l'ensemble de ses opérations sont assurées par les trois unités fonctionnelles sous-indiquées :

- **Unité de dissémination de données:** les opérations de cette unité peuvent être regroupées dans les phases suivantes :
  - *Génération de données:* une fois qu'un nouveau paquet de données ait produit, le nœud source va le transmettre en diffusion à ses voisins à proximité. Ensuite, la distribution des données sera complètement entreprise par un mécanisme de commérage (gossip) à travers des communications pair-à-pair.

- *construction et propagation du gossip digest:* la dissémination des données est accomplie par plusieurs cycles de gossip dans lesquels des messages gossip, portants le 'digest' (résumé) des données d'expéditeur, vont être propagés.

  À chaque cycle de gossip :

  - un nœud scanne son tampon de données et collecte les 'ID' des paquets dont leurs compteurs '*gossip counts*' (incrémentées à chaque cycle) sont inferieurs au nombre de fois définit par le paramètre '*stability threshold*' ;
  - ensuite, les 'ID' collectées des paquets de données seront regroupés dans un message de gossip avec un entête de gossip (gossip header) portant l'ID de la source et ce du groupe multicast concerné ;
  - ce message sera propagé via une diffusion a portée locale en exploitant la propriété inhérente de diffusion du support sans fil, où un nœud dans un groupe multicast diffuse localement les messages gossip à un sous-ensemble de nœuds (nœuds voisins) dont sa population est changée dynamiquement en raison de la mobilité des nœuds, ainsi que du mécanisme d'adaptabilité intégrant au protocole.

- *réception du message gossip :* dés qu'un nœud reçu un message gossip et à l'existence d'un certain identifiant stocké dans le tampon des paquets manquants, en comparant les identifiants des paquets placés dans le contenu du message avec les siens, il peut demander la transmission de(s) paquet(s) relatif(s) au(x) le(s) identifiant(s) de l'expéditeur du message. Cette demande peut être établie via des messages de requêtes '*Request message*' portant les ID des paquets demandés, tout en satisfaisant les deux conditions suivantes :

  - un nœud peut demander, par cycle de gossip, un nombre de paquets limité par le paramètre '*requestLimit*', afin de prévenir la saturation (congestion) du réseau.
  - un nœud ne peut pas demander un paquet de données qui a été demandé récemment pendant un temps prédéterminé, afin d'éviter la redondance des données transmises.

- *réception du message de requête :* lors de la réception du message de requête par un nœud, il peut transmettre les paquets de données relatifs au demandeur à condition qu'il n'atteigne pas le nombre limité '*transmission Limit*' des paquets transmis pour ce cycle. Autrement, la transmission peut être effectuée par différents nœuds sur plusieurs cycles de gossip.

- **Unité de gestion de tampons :** Cette unité effectue des tâches critiques pour la fiabilité et l'efficacité du protocole, elle maintient les tampons du protocole et assure la délivrance de données dans l'ordre FIFO.

- *maintenance des tampons:* au moyen d'un mécanisme Ramasse-miettes, le protocole gère le tampon des données où un paquet ayant un compteur '*gossip count*' supérieure ou égal au seuil '*stability threshold*' sera retiré du tampon. En plus, il contrôle aussi le tampon des paquets manquant où un paquet manquant, qui n'a pas pu être récupéré après le seuil de stabilité ou reçu, sera retiré à partir de ce tampon.
- *délivrance dans l'ordre FIFO :* tout paquet non dupliqué reçu est enfilé, par l'unité de dissémination de données, dans le tampon de données avec un ordre FIFO. à l'absence d'un décalage dans leur ordre, l'unité de gestion de tampons va délivrer les paquets de ce tampon à la couche supérieure, ou va attendre la réception des paquets manquants ou la déclaration de leur perte autrement.

- **Unité d'adaptabilité :** Ainsi il s'adapte à différentes densités de nœuds (réseau dense, réseau épar)EraMobile tente de permet de s'adapter aux changements imprévisibles des conditions de réseau. Pour cela, l'unité d'adaptabilité estime, périodiquement et pendant '*adaptivity period* ', le nombre des voisins immédiats observés autour d'un nœud tout en ajustant dynamiquement ses paramètres relativement au niveau de la densité de ces nœuds. En fonction de ce niveau, les nœuds envoient les messages gossip plus fréquemment pour profiter de liens éphémères dans les zones épares, ou diminuent le taux de diffusion afin de ne pas gâcher la bande passante limitée dans les zones denses.

a. Limites du protocole EraMobile

- une latence considérée de délivrance et une redondance avec l'agrandissement des membres participent dans la délivrance de parquets.
- un tampon de données de taille plus importante peut conduire à élargir de plus en plus la taille des messages gossip avec une probabilité de congestion dans les réseaux denses.

5.3.3 Comparaison et synthèse des travaux étudiés

Les protocoles que nous avons vus dans la section précédente, ont été développés afin d'assurer des communications de groupe fiables dans les réseaux sans fil ad hoc, tout en garantissant la propriété de la scalabilité. Pour atteindre cet objectif-ci, nous notons que certains d'entre eux tentent d'apporter des modifications sur des approches adoptées développées pour les réseaux filaires, tandis que d'autres exploitent une ou plusieurs caractéristiques spécifiques de ces environnements. Néanmoins, les solutions envisagées fournis des degrés variés de fiabilité dans des conditions suggérées de réseau. Après l'étude des travaux susmentionnés, nous pouvons synthétiser les remarques suivantes :

- **Protocoles de multicast fiable basés sur l'inondation:** ces approches présentent leur capacité d'assurer un niveau supérieur de fiabilité avec le passage à l'échelle (scalabilité maximale) sans aucun mécanisme de recouvrement n'est utilisé. Cependant ceci dans des conditions préférables où le réseau est fortement mobile (non statique). Nous remarquons que la fiabilité soit dégradée considérablement au non satisfaction des conditions idéales dues au changement du taux de densité ou de trafic d'une manière intuitive, avec un coût de scalabilité limitée.

- **Protocoles déterministes :** cette famille de protocoles implantent le mécanisme ARQ de recouvrement au dessus (voire même en intégration avec) les stratégies de dissémination des paquets de données de moindre effort afin de garantir quasiment 100% de paquets délivrés à tous les récepteurs (fiabilité totale de bout-en-bout) dans tous les scénarios. Cependant, ils ont potentiellement impliqué par les problèmes liés au point critique du passage à l'échelle. Comme il a été montré dans le protocole **RMA,** celui a souffert du problème de l'implosion des acquittements (ACK) en feedback au niveau de la source par l'impact négatif des interactions directes avec la source (classe Sender-initiated). Cet inconvénient est contourné en limitent l'interaction à un seul récepteur à la fois pour la récupération des paquets, tout en déchargeant la source de la responsabilité de détection des pertes, comme il à été signalé par les protocoles **RALM** et **ReACT** de la classe receiver-initiated, ou en utilisant une technique d'agrégation basée sur une structure hiérarchique adopté par le protocole **STRMP**. En outre, du fait que ces protocoles étant basés sur une approche centralisée de retransmission en multicast de type 'sender-originated', nous constatons qu'ils ne garantissent qu'une scalabilité limitée, avec une latence de recouvrement qui subit leur efficacité et un énorme fardeau administratif au niveau de la source menant probablement à congestionner le réseau. Comme il à été indiqué, les protocoles **RALM** et **ReAct** ont implanté un mécanisme de contrôle de congestion basé sur fenêtre et vitesse, respectivement, cependant la source doit soumettre aux contraintes des récepteurs de faibles capacités.

Il y' a des solutions envisagées qui ont adopté des approches développés pour les réseaux filaires pour remédier le problème de implosion des acquittements en feedback. Le protocole **ReMHOC** adopte une approche qui se focalise sur la suppression basée sur les temporisateurs aléatoires et décharge la source de la responsabilité de recouvrir les pertes en la distribuant entre les récepteurs. Bien que **ARMPIS** adopte une approche basée sur le support des routeurs actifs et répartit la charge de recouvrement entre les nœuds actifs du réseau afin d'éviter des points centraux d'échec dans le réseau. À l'opposition, le protocole **HCP** exploite

la topologie multi-saut dés réseaux ad hoc et implante un mécanisme de contrôle de congestion de saut-par-saut basé sur le crédit, dont le souci est de renforcer la fiabilité de bout-en-bout par une fiabilité de saut-par-saut et de traiter les phénomènes de la collision et de la contention da la couche MAC. Bien que les protocoles **ReMHOC**, **ARMPIS** et **HCP,** de la classe receiver-initiated, garantissent une scalabilité maximale, cependant les problèmes d'exposition des retransmissions et de localité de réparation ne sont pas traiter par ces protocoles. Nous remarquons ceci dans tous les protocoles déterministes que nous avons étudié, du fait que les retransmissions soient entreprises en multicast ou en diffusion (broadcast).

En constatation, nous pouvons conclure que les protocoles déterministes aient eu un mauvais compromis entre la fiabilité et le passage à l'échelle.

- **Protocoles probabilistes:** bien qu'ils se focalisent sur l'échange périodique des messages gossip entre les membres, cas des protocoles **AG** et **RDG**, ou la dissémination épidémique, cas de protocole **EraMobile**, basées sur des inondations contrôlées, les protocoles probabilistes peuvent récupérer les paquets perdus sans doute lié au problème d'implosion des acquittements, tout en garantissent la mise à l'échelle d'un nombre important de récepteurs; cependant sur le coût d'une augmentation considérable du trafic de réseau, une latence de recouvrement et également de délivrance. Etant basés sur un mécanisme de recouvrement probabiliste, les protocoles probabilistes atteignent un taux de délivrance élevé avec une haute probabilité (une fiabilité probabiliste). Donc, nous pouvons constater que les protocoles probabilistes assurent une fiabilité plus faible que les protocoles déterministes.

Le tableau suivant **(3.1)** est un récapitulatif qui synthétise certaines caractéristiques des protocoles sus-étudiés en termes de leur fiabilité (ratio de délivrance), scalabilité et contrôle de congestion, ainsi que d'autres points essentiels en relation avec les mécanismes utilisés pour améliorer leur fonctionnement.

protocole	Mécanisme de recouvrement	Ratio de délivrance	Schéma de retransmission	Implosion des acquittements en feedback	Retransmission de réparation	scalabilité	Contrôle de Congestion	Conception inter-couche (*cross-layer*)
	Basé sur inondation	maximal	-	-	-	maximale	-	-
RMA	Basé sur ARQ (*sender-initiated*)	maximal	Sender-originated	-	Multicast	Limitée	-	Informations fournies par le protocole de routage unicast sous-jacent
RALM	Basé sur ARQ (*receiver-initiated*)	maximal	Sender-originated	L'utilisation du feedback receiver	Multicast	Limitée	basé sur la fenêtre	-
ReAct	Basé sur ARQ (*receiver-initiated*)	maximal	Sender-originated	L'utilisation du feedback receiver	Multicast, Unicast Pour le recouvrement local	Limitée	basé sur la vitesse	Informations fournies par la couche MAC
ReMHOC	Basé su ARQ (*receiver-initiated*)	maximal	Receiver-assisted	suppression	Multicast	maximale	-	-
ARMPIS	Basé sur ARQ (*receiver-initiated*)	maximal	Sender-originated, Receiver-assisted et Router-assisted	Agrégation	broadcast	maximale	-	-
STRMP	Basé sur ARQ (*sender-initiated*)	maximal	Sender-originated	Agrégation	Unicast, multicast	limitée	-	-
HCP	Basé sur ARQ (*receiver-initiated*)	maximal	Sender-originated et Router-assisted	-	Multicast	maximale	Basé sur le crédit	Informations fournies par la couche MAC
AG	Basé sur Gossip	élevé en haute probabilité	Receiver-assisted	-	Unicast	maximale	-	Informations fournies par le protocole de routage multicast sous-jacent
RDG	Basé sur Gossip	élevé en haute probabilité	Receiver-assisted	-	Unicast	maximale	-	Informations fournies par le protocole de routage unicast sous-jacent
EraMobile	Basé sur dissémination épidémique	proportionnel	Receiver-assisted	-	Unicast	maximale	-	-

Dans la synthèse des travaux étudiés, nous avons concentré sur le traitement des points envisagés dans nos objectifs de recherche. Cette synthèse nous amène à la combinaison de l'approche adoptée basée sur les temporisateurs aléatoires et celle basée sur l'aspect actif des routeurs, pour remédier les problèmes en face de la garantie de la propriété de scalabilité et surtout répondre à notre problématique.

6. Conclusion

Dans ce chapitre, nous avons vu la projection du support de multicast sur les réseaux sans fil et en particulier les réseaux ad hoc. En premier lieu, nous avons traité le problème de la gestion d'adhésion au groupe qui est une tâche très compliquée et est généralement incorporée dans les mécanismes de routage multicast. Ensuite, nous avons étudié le problème du routage multicast en termes des défis de conception et de taxinomie des protocoles de routage multicast ad hoc. En fin, nous avons étudié les travaux actuels développés pour traiter le problème de fiabilité multicast dans les réseaux ad hoc avec une synthèse de cette étude.

Dans le chapitre suivant, nous allons entamer la proposition d'une solution qui assure la garantie de délivrance adapté aux environnements ad hoc, tout en utilisant efficacement les ressources disponibles et en garantissant la propriété de la scalabilité (la mise à l'échelle).

Proposition d'un protocole de transport multicast fiable pour les réseaux ad hoc

CHAPITRE 4

1. Introduction

Plusieurs efforts ont été élaborés dans la littérature afin de supporter les communications multicast dans le contexte des réseaux sans fil ad hoc. La plupart d'entre eux, comme nous avons étudié dans le chapitre précédent, mettent l'accent sur l'assurance d'un service multicast fiable dans le niveau transport.

Malgré cette pluralité, ils restent insuffisant et moins performant, pour satisfaire les besoins des multiples applications dans plusieurs scénarios, au regard des caractéristiques des réseaux ad hoc en imposant un compromis entre le délai de délivrance (ou de recouvrement) et le surcoût de retransmission d'une part, et entre la fiabilité et la scalabilité d'une autre part.

Dans ce contexte, nous allons proposer, au cours de ce chapitre, une nouvelle solution. Nous commencerons, tout d'abord, par les raisons qui motivent ce choix d'orientation, les caractéristiques du protocole proposé, ses détails en matière des structures de données et les algorithmes descriptifs du comportement de différentes entités (les sources, les nœuds intermédiaires et les récepteurs). En fin, nous terminerons ce chapitre par une conclusion.

2. Contexte

Dû aux caractéristiques impressionnantes d'auto-organisation et orienté-groupe des réseaux ad hoc et leur avènement à grande échelle, là où l'installation des infrastructures n'est pas aisée (voire impossible), plusieurs applications seront désormais déployées au sein de ces réseaux, notamment les applications des missions critiques dans les milieux militaires, les opérations de secours après une catastrophe et les réseaux de capteurs (**sensors networks**). Celles-ci nécessitent des communications de groupe (communications multipoints) de type **one-to-many** ou **many-to-many** et exigent que ces communications doivent assurer la délivrance sans erreurs (fiabilité totale) des informations critiques véhiculées par elles.

Néanmoins, à l'opposition aux réseaux filaires et les réseaux sans fil avec infrastructures, les réseaux ad hoc ont un taux élevé de pertes de différentes natures, particulièrement dans leur configuration mobile où les paquets peuvent être perdus dus à la mobilité arbitraire et imprédictible des nœuds, l'absence d'une infrastructure fixe, la densité du réseau et les erreurs de transmission liées étroitement à la propagation du signal, influencée par **les bruits**, l'**atténuation,** le phénomène du **fading** (**Evanouissement**), et aux problèmes de **collision**, d'**interférence** et de **terminale caché**.

Par conséquent, la délivrance de toutes les données jusqu'aux membres de groupe peut être affectée en menant à un **ratio faible de délivrance** (facteur de fiabilité). En outre, la majorité des protocoles de routage multicast développés pour ces réseaux n'assure qu'une **délivrance à moindre effort** (**fiabilité partielle**) des paquets de données multidestinataire à tous les récepteurs actifs. En effet, ces raisons peuvent motiver la nécessité cruciale des protocoles de transport multicast fiable afin d'améliorer le ratio de délivrance des protocoles de routage multicast best-effort sous-jacent.

3. Analyse des travaux étudiés

D'après la synthèse des travaux de transport multicast fiable que nous avons étudié dans le chapitre précédent, nous rappelons que la plupart de ces protocoles se reposent sur le mécanisme de recouvrement ARQ, qui est, contrairement aux deux autre mécanismes de recouvrement dans les réseaux sans fil, simple à mettre en œuvre et totalement décentralisé ; en outre, il réagit selon le principe « à la demande » et assure une fiabilité quasiment totale. Ces derniers ont prouvé leur supériorité dans les points forts suivants:

- La famille receiver-initiated permette le passage à l'échelle d'un grand nombre de récepteurs (scalabilité) par rapport à la classe sender-initiated.
- Étant utilisé l'approche de suppression de NACK basé sur les temporisateurs, le problème de l'implosion des acquittements (NACKs) en feedback peut être réduit au minimum.
- La retransmission en multicast des paquets de réparation est plus approprié que la retransmission en unicast, ceci peut réduire la duplication intitule de retransmission autant des récepteurs signalés la perte tout en assurant une utilisation efficace de ressources.
- La combinaison des trois schémas de retransmission sender-originated, receiver-assisted et router-assisted, analysée par le protocole **ARMPIS [79],** donne une bonne répartition de la charge de recouvrement des pertes avec une influence moins importante des récepteurs de faible capacité.

Cependant, ils ont toutefois présenté certaines limites, notamment :

- La transmission en multicast des paquets de contrôle et de réparation au groupe en entier à un impacte négatif sur la performance de protocole et de réseau lui-même de sorte que:
  - Le problème de localité de perte, qui met un défi contre le passage à l'échelle, ne soit pas résolu du fait que la retransmission à tous les récepteurs du groupe expose certains d'entre eux à des transmissions dupliquées et provoque une consommation inutile de la bande

passante et une augmentation de la latence de recouvrement (idem pour le cas du protocole ReMHoc **[78]**) **[20]**.

- Cette solution nécessite un service de routage m-vers-n qui n'est pas forcément disponible dans le protocole de routage multicast de type source-based et donc un overhead additionnel par le protocole sous-jacent peut dégrader la performance du réseau **[19]**.
- Le réseau puisse être congestionné en raison des transmissions en diffusion (broadcast) au niveau de la couche MAC menant aux collisions (contention ou interférence) **[85]**.

- Le schéma de retransmission **Receiver-assisted** nécessite que les récepteurs doivent mettre en cache une copie de tous les paquets de données reçus, ceci exige un espace de stockage illimité. Cette hypothèse est plafonnée par la contrainte des capacités limitées des mémoires de stockage de nœuds mobiles dans les réseaux ad hoc.

3. Solution proposée

Au regard des limitations évoquées ci-avant, nous parvenons à proposer un protocole de transport qui pallie à ces inconvénient. Néanmoins, du fait qu'il n'ya pas un protocole de transport multicast fiable de "one-size-fits-all" (usage général), notre solution vient pour supporter les applications multipoint de type many-to-many (plusieurs sources peuvent existées dans le même groupe multicast) qui exigent une fiabilité totale (de bout-en-bout) de délivrance tout en assurant une bonne utilisation des ressources avec un grand nombre de récepteurs.

Dans ce contexte, les approches basées sur les temporisateurs aléatoires (random timer-based), comme le cas du protocole ReMHOC, montrent leur capacité de supporter au mieux ce type-là, et présentent des avantages étonnant en termes qu'elles soient particulièrement robustes quant au changement de topologie et permettent de résoudre les problèmes inhérents à une communication de groupe qui surgissent à grande échelle.

Ces observations donnent une raison que nous pousse à adopter cette approche. en revanche, ses limites, susmentionnées, nous orientons vers une contribution de restreindre la portée des retransmissions aux récepteurs qui ont effectivement perdu le paquet de données (un recouvrement local) et des paquets de contrôle (une retransmission locale) pour réduire le nombre de retransmissions dupliquées générés afin d'assurer la scalabilité des retransmissions et des paquets de contrôle d'une part, et l'utilisation efficace des ressources de réseau tout en allégeant le problème de la localité de perte.

Dans le deuxième chapitre, nous présentons une approche Internet attractive, basée sur le support de routeur, pour restreindre la portée des retransmissions et des demandes de retransmission. Une catégorie utilise le support minimal du routeur afin de rediriger les demandes de retransmission (NACK) au répondeur (réplier) approprié, tandis que l'autre catégorie utilise des routeurs actifs (ou des serveurs actifs co-localisés avec les routeurs) pour l'agrégation et / ou suppression des acquittements en feedback et la récupération (recouvrement) locale.

Pour notre solution, nous choisissions de combiner l'approche précédente et celle basée sur le support des routeurs actifs avec une contribution des nœuds intermédiaires (routeurs) actifs dans le sens où ils ont la capacité de mettre en cache les paquets de données multicast et la possibilité de supprimer les messages de contrôle en feedback dupliqués pourvu qu'ils assurent un recouvrement local scalable et en temps opportun. Par la suite, nous allons présenter notre solution nommée « **WASRM** » pour **W**ireless **A**ctive **S**calable **R**eliable **M**ulticast.

4. Présentation du protocole WASRM

4.1 Objectifs du protocole WASRM

Le protocole WASRM englobe (combine) l'approche basée sur les temporisateurs aléatoires de la classe receiver-initiated et celle basée sur le support des nœuds intermédiaires actifs afin d'hériter des avantages relatifs à chacune d'entre elles qui permettent de résoudre les problèmes inhérents à une communication de groupes qui surgissent à grande échelle tels que : l'implosion des paquets de contrôle au niveau de la source, la répartition de la charge de recouvrement des pertes, l'exposition des récepteurs et l'influence des récepteurs de faible capacité sur le groupe et d'atteindre les objectifs de conception des protocoles de multicast fiable évoqués ci-avant, entre autres :

- Assurer une utilisation efficace des ressources de réseau (bande passante, énergie, capacité de stockage) tout en évitant les transmissions intitules par réduction du nombre des nœuds intervenus dans le processus de recouvrement (particulièrement dans le cas où des petites fractions de récepteurs qui ont effectivement perdus le paquet demandé dans des points différents).
- Minimiser le temps de latence de recouvrement.

4.2 Contribution du protocole WASRM

Ses idées cruciales résident dans les points suivants:

- **La contribution des nœuds intermédiaires (routeurs) dans le processus de recouvrement :** les nœuds intermédiaires, par définition, ont une fonction de nature passive où ils relayent les paquets en transit aux destinataires à travers la structure de distribution multicast. Ces derniers peuvent devenir actifs dans le sens où ils mettent en cache une copie des paquets de données pour une future retransmission « recouvrement local ». Ainsi, ils gardent des informations autour des paquets de contrôle (requêtes) afin de limiter le nombre des requêtes dupliquées et restreindre leur propagation dans la structure (suppression locale). Cette contribution à la tendance de limiter la portée des demandes de retransmission et des réparations tout en allégeant le problème de la localité de perte d'une part, et de réduire au minium le nombre des retransmissions dupliquées en réponse d'une autre part.
- **La transmission fiable des paquets de contrôle et de réparation:** un récepteur (membre de groupe) peut expédier en unicast les paquets de requête et de réparation au nœud intermédiaire directe en amant (upstream) afin de :
  - éviter l'overhead additionnelle par le protocole de routage multicast sous-jacent, particulièrement de type source-based, pour offrir un service de m-à-n où les nœuds intermédiaires ont la possibilité de rediffuser en multicast dans la structure.
  - assurer leur transmission fiable au niveau MAC qui offre une transmission fiable de saut-en-saut basée sur l'échange de RTS / CTS en face des collisions.
- **Suppression locale, retransmission locale et réponse rapide:** lorsqu'un nœud intermédiaire reçoit un acquittement négatif (requête de retransmission), il le diffuse en multicast à ses nœuds fils directs (downstream) pour supprimer localement les requêtes similaires et demander la retransmission aux nœuds répondeurs possibles (retransmission locale). Dans le cas échéant, il redirige l'acquittement négatif vers le nœud intermédiaire en amant (upstream) tout en augmentant progressivement sa portée de transmission. En outre, avec la distribution de la charge de retransmission entre les trois entités « source, nœud intermédiaire, récepteur », le protocole peut réduire le délai de la latence de recouvrement.
- **La coordination inter-couches avec la couche MAC (cross-layer design) :** la transmission des paquets de données multicast en diffusion (broadcast) peut générer des collisions pourront détruire les paquets au niveau de la couche MAC réceptrice. Le protocole à la capacité de détecter ce genre des erreurs tout en exploitant les informations partagées fournies par

la couche MAC, afin de réagir de façon rapide en demandant la retransmission de paquet détruit sans besoin d'attendre l'arrivé d'un nouveau paquet bien reçu.

- **Le concept des acquittements passifs "passive acknowledgment" :** en profitant de la capacité naturelle de diffusion de l'interface radio, le protocole adopte le concept des acquittements passifs "passive acknowledgment" qui a été utilisé par le protocole HCP **[81]**. Après la diffusion en multicast du paquet de données multicast, la source sera bientôt mis en écoute de sa rediffusion, qui sert comme un acquittement passif en feedback, par au moins un de ses voisins valide dans la structure de distribution multicast (situés à l'intérieur de sa portée radio). À l'absence de cet acquittement pendant un temps d'attente, la source va retransmettre le paquet. Après un certain nombre de tentatives, elle peut déduire le partitionnement de la structure et en effet se cesse de transmettre les données. le processus de transmission va être redémarré une fois que la liaison à la structure soit rétablie. Ce mécanisme à la tendance d'éviter le problème d'implosion en feedback des NACKs (requêtes de retransmission) si la perte est subie sur les liens sources.
- **La gestion de cache au niveau des nœuds intermédiaires et des récepteurs:** pour remédier au problème de l'espace illimité de stockage, qui est plafonné par la capacité des mémoires dans les nœuds mobiles, les nœuds intermédiaires actifs, similairement au protocole ARMPIS **[79]**, mettent en cache une copie de chaque paquet de données selon la stratégie FIFO probabiliste. Si le nombre aléatoire généré, entre 0 et 1, est plus petit que certaine probabilité 'p', le nœud peut stocker ce paquet en le mettant dans la queue selon le principe premier arrivé premier servi. Autrement, le paquet sera relayé (délivré) sans être stocké. L'idée derrière cette technique est de réduire la duplication des paquets en cache et de stocker autant que possible les paquets multicast entre les nœuds voisins **[79].** Néanmoins, les récepteurs mettent en cache les paquets reçus selon la stratégie FIFO.
- Les valeurs des temporisateurs aléatoires sont inspirées du protocole Internet SRM **[35]**, au contraire de celles basées sur le nombre de saut du protocole ReMHOC, difficile à maintenir.

4.3 Stratégies utilisées dans le protocole WASRM

4.3.1 Stratégie des niveaux

Comme montrer la figure **(4.1(a))**, le réseau ad hoc est divisé en plusieurs niveaux (Levels) virtuels partant des nœuds fils, le niveau '0', de source. Cette division est établie à chaque paquet de données transmit où chaque niveau 'i' désigne la distance entre les nœuds de la structure (récepteurs, nœuds intermédiaires) incorporés dans ce niveau et la source du paquet tout le long du chemin parcouru selon la profondeur de l'arbre (voir la figure **(4.1 (b))**).

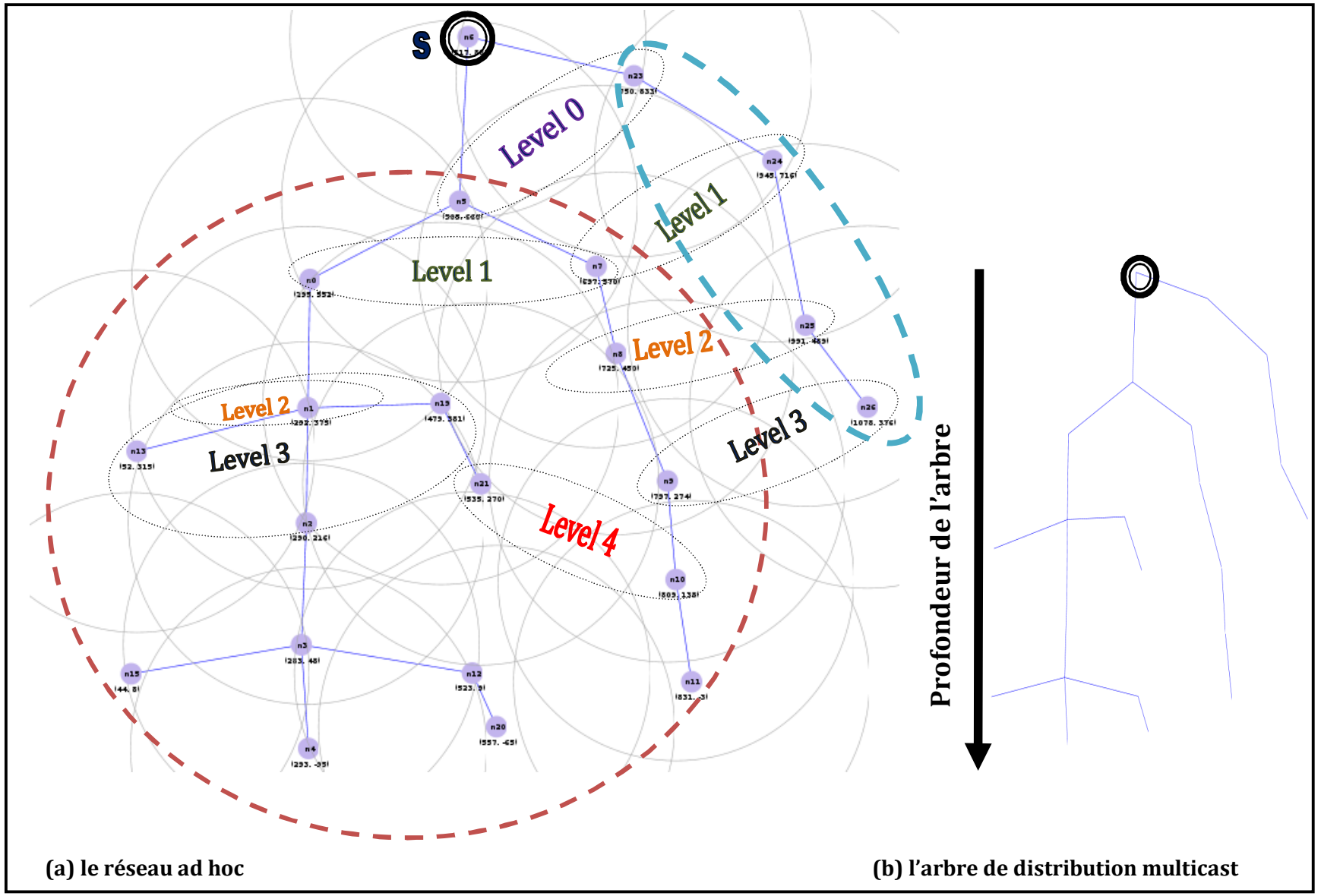

Figure 4.1: Stratégie de niveaux

De même, cette structure est divisée en sous structures, racinées par la source, autant de liens sources (2 liens source / 2 sous structures représentés par cercles rouge et bleu dans la figure **(4.1(a))**). Cette répartition en niveaux virtuels a le but d'identifier le niveau sur lequel la perte est subie, afin de restreindre la portée de propagation des acquittements négatifs demandant la retransmission et des réparations en réponse pour recouvrir les pertes potentielles sur le même niveau ou des niveaux inferieurs (recouvrement local) sans la nécessité de parcourir la structure en entière d'une part, et de minimiser le nombre de nœuds intervenus dans le processus de recouvrement (assurer une utilisation efficace de bande passante et d'énergie) d'une autre part.

4.3.2 Stratégie d'observation de pertes

Dans la structure de distribution multicast, deux types de pertes peuvent être surgis à différents liens de la structure de distribution multicast, à savoir, pertes partagées ou pertes indépendantes. Les pertes partagées se profilent quand un paquet est perdu sur un lien commun en amant dans la structure, tous les récepteurs au dessous de ce lien (en aval) pourront détecter la perte et éventuellement la signaler. Néanmoins, les pertes indépendantes se réfèrent à des pertes hétérogènes surgissant à différents liens fils ayant le même lien commun en amont et à différents niveaux de la structure. Un exemple descriptif est illustré dans la figure **(4.2),** la figure **(4.2(a))** montre que la perte produite au niveau du lien (A, B) soit partagée par les nœuds B, C, D et E qui ont au dessous de ce lien commun. Alors que les pertes produites sur les liens (B, C) et (B, E) dans la figure **(4.2(b))** soient détectées de façon indépendante par les nœuds C, E respectivement.

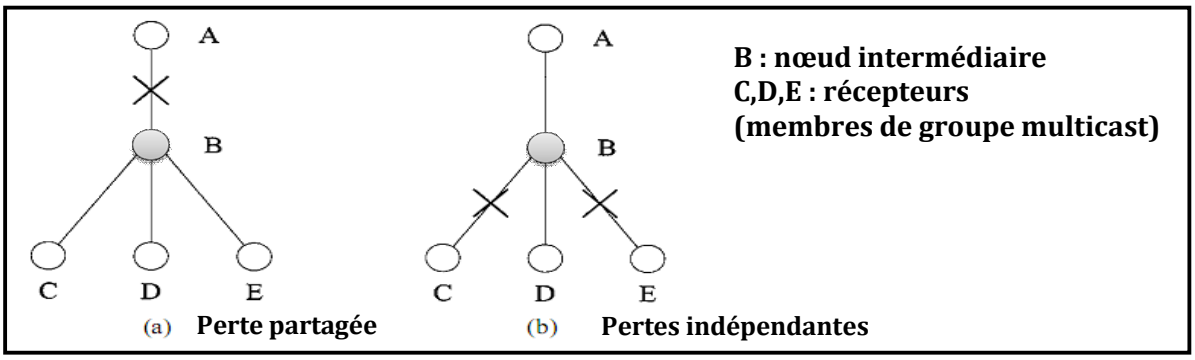

Figure 4.2: Stratégie d'observation de pertes

L'utilisation de cette stratégie à la tendance de permettre à notre protocole de mieux réagir aux pertes détectées, et au contraire du protocole ARMPIS **[79]** où plusieurs retransmissions dupliquées (autant de récepteurs demandeurs) peuvent être situées dans des différents liens de la structure de distribution multicast, de minimiser le nombre des retransmissions

dupliquées sachant qu'une seule retransmission peut atteindre les récepteurs demandeurs situés en aval du niveau de premier demandeur (requestor) le plus proche du lien où la perte est subie.

4.4 Principe de fonctionnement du protocole WASRM

Le protocole WASRM supporte l'existence de plusieurs sources dans le même groupe multicast où le trafic du chacune est identifié par la couple <S, N°seq> qui indique le numéro de séquence du paquet de données multicast généré par la source active 'S'. Une fois qu'un membre de groupe veut devenir une source, il transmit les paquets de données multicast partant de N°seq = '0'. Cette transmission utilise le concept 'Wireless Multicast Advantage' en exploitant la capacité naturelle de diffusion offerte par l'interface radio de sorte que la transmission implique un nombre maximum des nœuds intervenus dans la réception avec une faible énergie consommée.

Durant la propagation du paquet de données tout au long du chemin de distribution, chaque nœud intermédiaire met en cache, avec une certaine probabilité 'p', une copie de ce paquet, définit son niveau virtuel en basant sur le contenue de l'entête du paquet traversé et calcule la distance qui le sépare de la source en utilisant l'estampille du paquet (qui est égale au temps d'arrivé au nœud – le temps de son envoie par la source) puis il va le relayer jusqu'au bout. À l'arrivé du paquet à un récepteur, en plus de la définition du niveau et du calcul de la distance, il garde une copie de ce dernier dans le cache selon la stratégie 'FIFO' puis il met à jour la liste ordonnée des IDs des paquets reçu par la couple <S, N°seq>. Si un récepteur détecte un décalage dans la séquence de numérotation qui sert comme un signal de perte, il va notamment demander sa retransmission via un acquittent négatif généré. En effet, nous explorons le processus de recouvrement via un exemple illustratif représenté par la figure **(4.3)** ci-dessous.

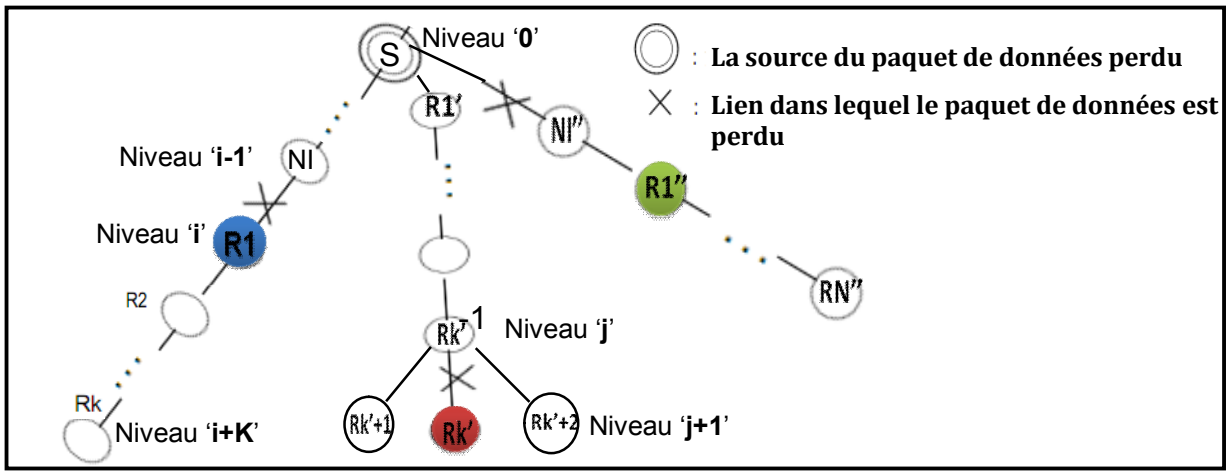

Figure 4.3: Processus de recouvrement

Comme ce protocole est de famille receiver-initiated, les récepteurs détectent la perte de façon autonome. Dans ce cas, plusieurs acquittements négatifs pourront être générés et le problème d'implosion des acquittements négatifs peut être survenu. Cette situation est illustrée dans l'exemple où les récepteurs R1->Rk et R1''->RN'' détectent chacun la perte qui se produite sur le lien (NI, R1) et le lien source (S, NI'') respectivement, tandis que au dessous du lien (RK'-1, RK') la perte soit détectée par le récepteur RK' qu'il subit.

Cependant, avec la technique de suppression des NACKs basée sur les temporisateurs aléatoires, le problème d'implosion peut être allégé. Chacun récepteur détectant la perte, arme un délai d'attente aléatoire relatif à la distance de la source, ceci permet au récepteur de niveau '**i**', le plus proche du lien sur lequel se produit la perte, de déclencher en premier lieu le processus de recouvrement, le cas des récepteur R1, RK' et R1'' les plus prés des liens de pertes (NI, R1), (RK'-1, RK') et (S, NI'') respectivement. Ce dernier transmet un acquittement négatif vers le nœud intermédiaire direct en amant pour demander la retransmission de paquet perdu. À la réception de cet acquittement par ce dernier, on peut distinguer plusieurs cas de figure :

- S'il est possédé le paquet demandé en cache, il le retransmet en multicast immédiatement (aucun délai d'attente ni armé) vers les nœuds directs en aval afin de réparer les pertes surgissent dans ce niveau, et probablement celles aux niveaux inferieurs, et de supprimer les acquittements négatifs similaires en réduisant le délai de la latence de recouvrement. C'est le cas des nœuds intermédiaire NI, au niveau 'i-1', et NI'', au niveau '0', qui peut impliquer le récepteur R1, au niveau '**i**' jusqu'au récepteur Rk, au niveau 'i+K', et R1''->RN'', à partir du niveau '1', respectivement, avec une seule retransmission, alors que le nœud RK'-1, au niveau 'j' implique seulement le récepteur RK', au niveau 'j+1'.
- S'il ne possède pas le paquet mais la perte détectée est indépendante, il redirige en multicast partiel (subcast) l'acquittement vers les nœuds directs en aval, pour demander sa retransmission aux nœuds qui n'ont pas signalés la perte et supprimer les acquittements similaires dans ceux qu'ont détectés la perte. Dans l'exemple le récepteur Rk', au niveau 'j+1', détecte la perte surgit au lien (RK'-1, RK'), tandis que dans le même niveau, les deux récepteurs Rk'+1 et Rk'+2 n'étant pas affectés par cette perte. En effet, le nœud intermédiaire Rk'-1, au niveau 'j', peut récupérer le paquet perdu à partir de ces derniers.
- Le cas échéant où la perte est partagée, il transmet donc l'acquittement en multicast afin de demander la retransmission au nœud intermédiaire direct en amant et éventuellement de supprimer les acquittements similaires dans ses nœuds fils en aval dans la structure. Idem

pour les nœuds R1 et R1''qui demandent la retransmission aux nœuds intermédiaires NI et NI'', et supprime les demandes similaires des récepteurs R2->RK et R2''->RN'' respectivement.

À la réception de l'acquittement négatif par un récepteur, si ce dernier avait le paquet en question dans son cache, il arme un délai d'attente de retransmission lié à la distance calculée entre lui et le nœud intermédiaire demandeur en amant. À l'expiration de délai d'attente sans la réception de retransmission, il retransmit directement le paquet perdu vers le nœud en amant. Ce dernier va le rediffuser en multicast vers les nœuds directs en aval afin de réparer la perte (pour ce qui demandé la retransmission) et pour supprimer les retransmissions en attente (pour les récepteurs qui ont armés le délai d'attente de retransmission). De plus, un récepteur peut avoir un signal de perte durant la réception du paquet de données depuis la couche MAC (due à la collision). Dans ce cas-là, il doit agir conformément au cas d'absence d'une couple <S, N°seq>, mais sans la nécessité d'attendre la réception du prochain paquet.

Quand la source reçoit un acquittement négatif, peut être dû à l'échec de processus de recouvrement local, il retransmit immédiatement (sans armé un délai d'attente) en multicast le paquet en question vers ses voisins directes et supprime l'acquittement pour ne peut être propagé dans la structure en entière. Seulement les nœuds intermédiaires de niveau '**0**', qui ont détecté la perte, sont autorisés de relayer le paquet retransmit vers leurs nœuds directs en aval. dans l'exemple ci-avant, une perte est produite sur le lien source (S, NI''), et en effet, le nœud intermédiaire NI'' va rediriger l'acquittement négatif, de la part du R1'' vers la source S qui va nommant retransmettre le paquet demandé. Seulement le nœud NI'', affecté par cette perte, aura bientôt la permission de relayer le paquet de réparation vers sa sous structure.

5. Description du protocole WASRM

5.1 Structures de données

Pour atteindre son objectif, le protocole **WASRM** utilise les structures de données suivantes:

- **packet-received ID cache:** une liste chainée des IDs (couple <S, N°seq>) de paquets bien reçus.
- **hierarchy :** composée de champs suivants : <Level> : indiqué le niveau virtuel du nœud dans la structure de distribution par rapport à la source, <Upstream> : indiqué l'@IP du nœud direct en amant (upstream) afin de construire le chemin inverse (revers path) vers la source.

- **request cache :** une liste chainée de <S, N°seq> requêtes enregistrées dans le nœud pour la suppression des requêtes dupliquées et la permission du passage de retransmission vers le niveau supérieur dans la structure.
- **repair cache :** une liste chainée de réparations (retransmissions) enregistrées dans le nœud, ayant la structure <S, N°seq>, pour la suppression des réparations dupliquées.

5.2 Structure des paquets

On distingue trois sortes de paquets, les paquets de données, de requête et de réparation.

- **Le paquet de données:** pour assurer un recouvrement local, le protocole introduit des nouveaux champs dans l'entête du paquet de données, comme montre dans la figure **(4.4):**
  - La couple <Source, N°seq>: qui indiquée la source du paquet de données identifié par le numéro de séquence 'N°seq'.
  - Le champ <Level>: incrémenté à chaque nœud traversé pour indiquer le niveau du nœud (intermédiaire ou récepteur) dans la structure de distribution par rapport à la source.
  - Le champ <Upstream> : pour indiquer le saut précédent par le quel le paquet est relayé.

@IP source	@IP multicast	Source	N°seq	Level	Upstream	Timestamp	Données

Figure 4.4 : Structure d'un paquet de données du protocole WASRM

- **Le paquet "repair request":** ou encore paquet de requête qui se sert comme un acquittement négatif pour signaler la perte du paquet de données et demander sa retransmission. Il englobe en plus des informations concernant l'adresse de demandeur et de destination, l'estampille pour calculer la distance et le <Levelrequestor> qui désigne le niveau du nœud demandeur de paquet perdu dans la structure de distribution. La structure de ce paquet est illustrée dans la figure **(4.5).**

@IP requestor	@IP destination	Source	N°seq	Timestamp	Level requestor

Figure 4.5 : Structure d'un paquet de requête du protocole WASRM

- **Le paquet "repair":** il s'agit comme un paquet de réparation, sa structure est montrée dans la figure **(4.6)**. ce dernier est structuré comme suit: < @IP replier, @IP destination, Source, N°seq, données > où le paquet perdu identifié par la couple <Source, N°seq>.

@IP replier	@IP destination	Source	N°seq	données

Figure 4.6 : Structure d'un paquet de réparation du protocole WASRM

5.3 Algorithmes des différentes entités du protocole WASRM

Notre protocole repose sur trois sortes d'entités à savoir: les sources, les récepteurs et les nœuds intermédiaires. Chacune se comporte de la manière suivante :

a. Comportement de la source

- **À l'émission du paquet de données:**
  - Diffusion en multicast du paquet de données, de 'N°seq' partant de '0', à une adresse IP multicast, dans laquelle sont inscrits tous les récepteurs d'un groupe multicast ;
  - Après l'envoie du paquet:
    - Initialisation d'un délai d'attente d'acquittement passif égale au temps de la transmission de paquet aux nœuds voisins immédiats ;
    - À l'expiration du délai d'attente:

      Si nb de tentatives < retransmission_threshold **alors**
        - Retransmission du paquet ;
        - Réinitialisation à nouveau le temporisateur ;

      Sinon
        - Cesse l'émission (l'arrêt de la transmission des paquets) ;

      Fin si

- **À la réception d'un paquet de données:**

  {Elle agit comme étant un récepteur ;}

- **À la réception d'un paquet de requête "repair request":**

  Si la couple <S, N°seq> de la requête identifie un paquet propre à cette source **alors**
    - Envoie immédiatement en multicast un paquet de réparation ;

  Sinon

  {Elle agit comme étant un récepteur;}

  Fin si

- **À la réception d'un paquet de réparation "repair":**

  Si la couple <S, N°seq> du paquet de réparation détermine une source autre que celle-ci **alors**

  {Elle agit comme étant un récepteur ;}

  Fin si

b. Comportement du nœud intermédiaire

- **À la réception d'un paquet de données:**
  - Génération d'un nombre aléatoire de distribution uniforme entre 0 et 1 ;

  Si ce dernier est inferieur à une probabilité 'p' **alors**
    - Stockage d'une copie du paquet de données dans le buffer du cache ;
  - Mise à jour de la liste 'packet-received id cache' par la couple <S, N°seq> récupérée du paquet de données reçu;

- Incrémentation du "Level" de paquet reçu;
- Mise à jour des 'Level' et 'Upstream' de la structure 'hierarchy';
- Mise à jour du 'Upstream' de paquet par l'adresse IP de ce nœud;
- Expédition du paquet de données aux fils directs dans la structure de distribution multicast ;

- **À la réception d'un paquet de requête "repair request":**

Si ∃ une entrée correspondante la couple <S, N°seq> dans la liste 'request cache' **alors**

- Ignorance de la requête reçue. /**suppression locale des requête dupliquées*/*

Sinon /**pas de requête pour la couple < S, N°seq> figure dans la liste 'request cache'* */

Si la couple < S, N°seq > ne figure pas dans la liste 'packet-received id cache' **alors**

/**la détection d'une situation de perte partagée* */

- Inscription d'une requête pour <S, N°seq, > dans la liste 'request cache' ; /* *pour supprimer les requêtes identiques reçues*/*
- Rediffusion en multicast (@IP destination=@IP multicast) de ce paquet ; /**pour supprimer les requête potentiel des nœuds en aval de ce nœud*/*

Sinon /**la couple < S, N°seq > se trouve dans la liste des IDs des paquets de données reçus* */

Si ∃ en cache une copie du paquet de données **alors**

- Insertion d'une réparation < S, N°seq > dans la liste 'repair cache' ;
- Expédition d'un paquet de réparation <S, N°seq, données > selon:

Si le niveau du nœud intermédiaire 'Level' = '0' **alors**

- Diffusion en multicast partiel (subcast) aux nœuds fils en aval ;

Sinon /* *le niveau du nœud intermédiaire > 0* */*

Si le niveau <Level> de ce nœud = <Level requestor> de la requête **alors**

- Expédition en unicast vers le nœud en amant (@IP destination= <Upstream>) ;

Sinon Diffusion en multicast. /**pour recouvrir les pertes au niveau ≥ Level requestor* */*

Fin si

Fin si

Sinon /* *pas de copie du paquet de données se trouve dans le cache*/*

- Inscription d'une requête <S, N°seq, > dans la liste 'request cache' ; /* *pour supprimer les requêtes identiques* */*
- Rediffusion en multicast partiel (subcast) aux nœuds fils directes en aval;
- Initialisation d'un délai d'attente d'arriver de réparation pour la couple <S, N°seq> à la valeur de la distance calculée en mesure du temps d'arriver au nœud – le temps de son envoie du nœud requestor dans la structure de distribution (estampille du paquet);
- À l'expiration de délai d'attente :
  - Réexpédition de la requête en unicast vers le nœud direct en amant (@IP destination= <Upstream>);

Fin si

Fin si

Fin si

- **À la réception d'un paquet de réparation "repair":**

Si ∃ une entrée correspondante la couple <S, N°seq> dans la liste "repair cache" **alors**

- Ignorance de la réparation reçue;

Sinon /**pas de réparation pour la couple < S, N°seq > figure dans la liste 'repair cache'* */

Si le délai d'attente de requête pour la couple <s,n°seq> est armé **alors**

{Il agit identiquement comme un récepteur;} /**le nœud est un membre de groupe*/*

Sinon Si ∃ une entrée correspondante dans la liste "request cache" **alors**

- Retire de la requête de la liste "request cache" ;
- Insertion de la couple <S, N°seq > dans la liste "repair cache"; /* *pour supprimer les réparations identiques**/
- **Si** la couple < S, N°seq > ne figure pas dans la liste 'packet-received id cache' **alors**
  - Mise à jour de la liste 'packet-received id cache' par la couple <S, N°seq> ;
  - Stockage d'une copie du paquet de données dans le buffer du cache ;
  - Rediffusion en multicast partiel (subcast) aux nœuds directes en aval;

Fin si

Fin si

Fin si

c. Comportement du récepteur

- **À la réception d'un paquet de données:**

Si le récepteur est un nœud intermédiaire **alors**

{Il agit identiquement comme un récepteur;}

Sinon

- Stockage en cache d'une copie du paquet de données reçu selon la stratégie FIFO ;
- Mise à jour de la liste 'packet-received id cache' par la couple <S, N°seq> récupérée du paquet de données reçu ;
- Incrémentation du "Level" de paquet reçu;
- Mise à jour des 'Level' et 'Upstream' de la structure 'hierarchy';
- Mise à jour du 'Upstream' de paquet par l'adresse IP de ce nœud;

Fin si

- Ordonnancement de la liste des IDs des paquets de données reçus;

Si ∃ un saut dans la séquence <S, N°seq> des paquets reçus **alors** /**une perte à signaler*/*

- Initialisation d'un délai d'attente de requête de cycle (round) = 0 pour la coupl $d_{S,A}$ N°seq> du paquet perdue avec une valeur aléatoire à distribution uniforme dans l'intervalle $[C_1 d_{S,A}, (C_1 + C_2) d_{S,A}]$ seconds . Où C1 et C2 sont des paramètres de protocole, la distance calculée en fonction de l'estampille du paquet (en mesure du temps d'arriver au récepteur A – le temps de son envoie depuis la source S) ;

Fin si

- À l'expiration de délai d'attente de requête:
  - Expédition d'une requête 'repair request' < S, N°seq> selon deux cas :

Si le récepteur est un nœud intermédiaire **alors**

- diffusion en multicast (@IP destination=@IP multicast); /***pour demander la retransmission de paquet perdu et supprimer les requêtes chez les nœuds en aval* */

Sinon /* *le nœud est un récepteur final (feuille de l'arbre multicast)*/
- Expédition en unicast (@IP destination=<Upstream>) vers le nœud intermédiaire père en amant;

Fin si

- Réinitialisation du délai d'attente de requête pour l'attente d'arriver de réparation;

- **À la réception d'un signal de perte durant la réception (due à la collision au niveau Mac):**
  {Il réagit conformément au cas d'absence d'une couple <S, N°seq>;}

- **À la réception d'un paquet de requête "repair request":**

Si un délai d'attente de requête pour la couple <S, N°seq> est armé **alors**
- Désarmement de délai d'attente ;
- Réarmement du temporisateur avec un algorithme de back off exponentiel où le délai d'attente de requête sera réinitialisé pour le cycle courant +1 avec une valeur aléatoire à distribution uniforme dans l'intervalle $2^i[C_1 d_{S,A}, (C_1 + C_2) d_{S,A}]$ où i = cycle;

Sinon /* *aucun délai d'attente de requête n'est armé* */
Si ∃ une copie du paquet de données dans le cache **alors**
Si le récepteur est un nœud intermédiaire **alors**
{Il réagit de la même façon qu'un nœud intermédiaire;}
Sinon /**le nœud est un récepteur final*/
Si un délai d'attente de réparation pour la couple <S, N°seq> est armé **alors**
- Ignorance de la requête reçue;

Sinon /* *aucun délai d'attente de réparation n'est armé*/
- Armement d'un délai d'attente de réparation pour la couple <S, N°seq> avec une valeur aléatoire à distribution uniforme dans l'intervalle $[D_1 d_{A,B}, (D_1 + D_2) d_{A,B}]$ où D1 et D2 sont des paramètres de protocole, $d_{A,B}$ la distance calculée relativement à l'estampille du paquet en terme du temps d'arriver au niveau du récepteur B – le temps du son envoie depuis le nœud intermédiaire A en amont;

- À l'expiration de délai d'attente de réparation :
  - expédition en unicast un paquet de réparation (repair) <S, N°seq, données > vers le nœud upstream (@IP destination= <Upstream>);

Fin si
Fin si
Fin si
Fin si

- **À la réception d'un paquet de réparation "repair":**

Si un délai d'attente de réparation pour la couple <S, N°seq> est armé **alors**
- Désarmement du délai d'attente;

Sinon /**pas de délai d'attente de réparation n'est armé*/
Si un délai d'attente de requête pour la couple <S, N°seq> est armé **alors**
- Désarmement du délai d'attente; /**suppression de la requête*/
- Mise en cache une copie de paquet reçu;
- Inscription de la couple <S, N°seq> dans la liste 'packet-received id cache' ;

Si le récepteur est un nœud intermédiaire **alors**
- Rediffusion en multicast partiel (subcast) aux nœuds directes en aval;

Fin si
Fin si

5.4 Informations partagées inter-couches (cross-layer)

Un réseau, comme nous avons vu dans le premier chapitre, est représenté abstraitement par une architecture structurée en couches. Cette structuration a l'avantage de simplifier la compréhension de l'architecture et de savoir les différents niveaux fonctionnels. Cependant, les architectures de réseaux sans fil impliquent une forte interdépendance entre les couches **[1]**. Cette interdépendance, qui viole l'architecture traditionnelle en couche, fait l'objet du concept de conception cross-layer où des informations se partagent entre les différentes couches de la pile protocolaires à des fins d'adaptation et d'augmenter les interactions entre elles. Cette partage des informations permet à chaque couche d'avoir une image globale des contraintes et des caractéristiques du réseau, conduit à une meilleure coordination pour prendre des décisions susceptibles d'optimiser conjointement la performance du réseau **[11]**.

Afin de contourner la destruction des paquets de données en réception à cause de la collision, nous avons conçu notre protocole suivant le concept inter-couche, comme illustré la figure **(4.7)**. En effet, notre protocole (implanté au niveau transport) sera bientôt informé de cette situation, via les informations partagées fournies par la couche MAC, pour qu'il puisse se réagir de façon rapide et idéale (l'invocation de procédure de recouvrement après perte).

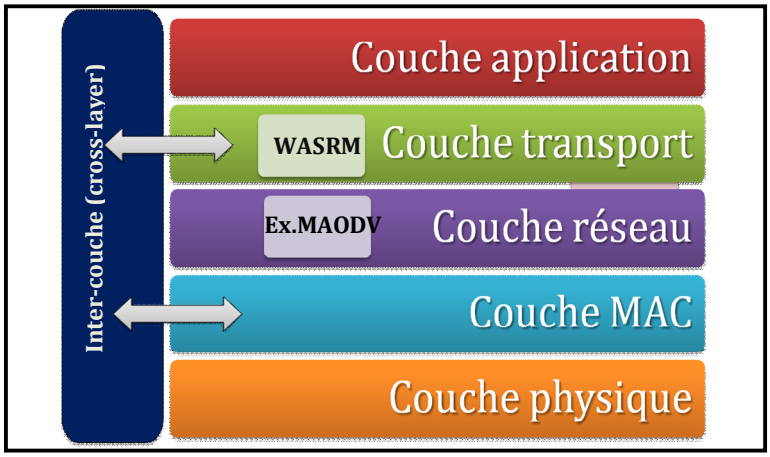

Figure 4.7 : Conception inter-couche (cross-layer)

6. Conclusion

Dans ce chapitre, nous avons proposé un nouveau protocole de transport multicast fiable pour les réseaux ad hoc en adoptant une approche basée sur les temporisateurs aléatoires avec la contribution de support des routeurs actifs.

Théoriquement, cette combinaison a le potentiel de remédier aux problèmes surgissant à grandes échelles, notamment la localité de perte et l'implosion des acquittements en feedback qui se servent comme des défis en face du facteur de scalabilité. En d'autres termes, il répartie la charge de recouvrement, en basant sur le type de perte (partagée ou indépendante) sur plusieurs niveaux logiques de la structure de distribution. Cependant, pour valider pratiquement notre protocole, nous allons évaluer ses performances par la simulation dans des conditions variées (scénarios) de réseau. Pour cela, nous choisissons d'utiliser l'outil de simulation (simulateur) de réseau, parmi d'autres, NS2.

Evaluation des performances

1. Introduction

La simulation permet de couvrir certains aspects de validation des performances de notre protocole proposé, que nous avons vu dans le chapitre précédent. L'objectif principal de ce chapitre est d'évaluer les performances de notre protocole en utilisant le simulateur de réseaux NS2 **[86]**. Nous commençons d'abord par une présentation des outils de simulation, ensuite nous discutons de l'environnement utilisé pour la simulation, enfin, nous analysons la performance de notre protocole avec les différentes simulations.

2. Outil de simulation "NS2"

La simulation est une technique utilisée pour valider et évaluer les performances des protocoles pour les réseaux filaires / sans fil via des outils de simulation où elle simule le comportement dynamique d'un modèle de réseau. Les simulateurs de réseaux , tels que : NS2, OMNET++, NCTUns, GlomoSim, JiST/SWANS et OPNET, sont des outils de simulation pour développer, tester et diagnostiquer les protocoles de réseaux. NS2 (Network Simulator) est le plus utilisé dans le domaine de la recherche pour ces raisons : (1) l'utilisateur peut concevoir et configurer le modèle de réseau à la fois à travers un générateur de scénarios ou par un code écrit à l'aide de langage (OTcl); (2) il offre la possibilité d'émulation et de simulation rapide (3) de nombreux protocole déjà mis en œuvre; (4) le comportement dynamique peut être visualisé à l'aide d'un animateur; (5) un logiciel Open source (code source libre) et extensible **[87,88]**.

NS2 est un simulateur à événement discret né du projet VINT (Virtual Inter-Network Testbed), qui fournit un support pour la simulation de TCP, le routage et les protocoles de multicast (routage et transport) et multicast fiable. Le simulateur est basé sur le langage de commande Tcl /Otcl (Tool Command Language / Object Oriented Tcl) comme une interface de configuration et le langage (C + +). La simulation dans NS2 est exécutée sur le modèle de réseau décrit et défini dans les fichiers (.tcl). Les fichiers de trace de simulation (.tr) et d'animation (.nam) sont crées au cours de la simulation. Une fois crées, les utilisateurs peuvent utiliser le fichier (.nam) pour vérifier le comportement à plusieurs reprises via un animateur de réseau **[88]**. Pour qu'un trafic multidestinataire (avec une adresse multicast de destination) soit délivré aux membres du groupe multicast (récepteurs), l'agent de routage (ragent) du nœud sans fil membre du groupe va d'abord créer une copie de paquet de données reçu avec l'adresse IP du nœud comme adresse de destination, ensuite il va la délivrer à l'agent de transport multicast.

```
ih->daddr() = @IP unicast du noeud;
ch->direction() = hdr_cmn::UP;
ih->dport() = UPPER_LEVEL_PORT;
Scheduler::instance().schedule(target_, p, 0);
```

3. Analyse de performance du WASRM

3.1 Métriques de performance

Afin d'analyser la performance de notre protocole, nous avons utilisé les métriques suivantes:

- **Taux de paquets livrés avec succès (Packet delivery ratio) :** le ratio de nombre de paquets de données reçus par les récepteurs par rapport aux paquets émis par le réseau. Ce paramètre donne le pourcentage des paquets livrés de façon fiable à leurs destinations afin de mesurer la fiabilité de protocole multicast fiable.

$$PDR = \frac{\sum \text{paquet reçus}}{\sum \text{paquets émis} \times \text{nombre de récepteur}} \times 100$$

- **Délai moyen de bout en bout (Average End to End Delay) :** Ce paramètre représente le délai passé entre l'instant où un paquet de données quitte l'émetteur et l'instant où il est reçu par le destinataire concerné, tout en incluant le délai résulté par la retransmission.

Ainsi, nous avons conduit multiples simulations où nous soumettons notre protocole à certaines caractéristiques des réseaux ad hoc, notamment:

- La mobilité des nœuds du réseau sans fil ad hoc.
- La taille du groupe multicast (G) dans le réseau sans fil ad hoc.
- Le nombre des sources de trafic(S) dans le réseau sans fil ad hoc.

Ceci pour le but d'étudier leur effet sur les performances de notre solution.

3.2 Environnement de simulation

Notre simulation est établie sur un environnement constitué par la version ns-allinone-2.35 du simulateur de réseau NS2 installée sous le système d'exploitation LINUX Ubuntu 9.10 (Karmic Koala). L'environnement de simulation NS2 que nous avons utilisé modélise une architecture réseau de quatre couches. Les scénarios de simulation utilisent des sources de trafic à débit constant CBR (Constant Bit Rate), qui modélisent la couche application. Ces sources sont attachées à des agents de protocole de multicast fiable WASRM implémenté dans la couche transport. Dans les couches réseau et MAC, nous avons utilisé le protocole de routage multicast MAODV **[63]** et le protocole IEEE.802.11 respectivement.

L'outil de simulation NS2 n'inclut pas une implémentation standard du protocole MAODV. Pour l'implémenter nous avons utilisé les détails expliqués dans **[89]** tout en apportant les modifications nécessaires sur la version **ns-2.35**

En se basant sur l'environnement de simulation NS2, nous avons développé des scénarios de simulation et exécuté des simulations pendant un temps de 450 secondes. Chaque scénario définit un réseau ad hoc de 50 nœuds. Certains d'eux sont choisis en tant que participants d'un seul groupe multicast dans le réseau. Par défaut, tous les membres sont les récepteurs de ce groupe. Les nœuds du réseau défini peuvent se déplacer dans un espace plat de 1000 mètres 1000 mètres où la mobilité est régie par un modèle pseudo aléatoire appelé « Random Point Model ». Dans ce modèle, chaque nœud est placé dans un emplacement aléatoire au début de la simulation (X0, Y0), ensuite, à des instants choisis aléatoirement, certains nœuds, eux choisis aléatoirement, vont se déplacer selon le principe suivant :

- choisir un nouvel emplacement (Xt, Yt) ;
- choisir une vitesse de mouvement entre 0 et Vmax m/s ;
- se déplacer vers le nouvel emplacement ;
- rester en repos pendant une durée entre 0 et un temps de pause maximal en ms.

Ainsi, deux paramètres pourront affecter la mobilité des nœuds dans le réseau : la vitesse Vmax, le temps de pause maximal : nous avons choisi de varier le temps de pause de 0,70 et 130 (s) et de fixer la vitesse à 1 m/s.

Les sources de trafic du groupe multicast (CBR) envoient des paquets de données de taille 512 octets avec un débit de 4 paquets par seconde au groupe à partir de 31.0 secondes et vont arrêter leurs transmissions à la 350^{iéme} secondes, le reste du temps permettra que le protocole fiable de multicast finisse ses retransmissions.

Le tableau **(5.1)** ci-dessous résume les paramètres de la configuration réseau qui vont constituer le contexte de toutes les simulations.

Paramètre	Valeur
Temps de la simulation	450 secondes
L'agent de transport et Protocole de routage	WASRM ; MAODV
Temps de pause des nœuds	0, 70, 130 secondes
Taille du paquet de données	512 octets
L'intervalle entre les paquets	0.25 milliseconde
Nombre maximale de paquets envoyés par source CBR	1276 paquets
Type d'accès au media (MAC)	802.11
Type d'interface de la file d'attente	File d'attente avec priorité
Nombre maximum de paquets dans la queue d'interface	50

Tableau 5. 1: Paramétrage du contexte de simulation

Pour configurer et exécuter les différentes simulations, nous avons développé un script TCL. Les résultats de chaque simulation sont enregistrés dans un fichier trace (.tr) spécifié dans le script TCL. Voici une illustration de ce script

```
$WASRM($i) set dst_addr_ IP_MULTICAST
$WASRM($i) set dst_port_ UPPER_LEVEL_PORT
$cbr_(0) attach-agent $WASRM_($i)
$ns_ at 30.0 "$WASRM_($i) start"
$ns_ at 30.1 "$cbr_(0) start"
$ns_ at 0.0100000000 "$node_($i) aodv-join-group IP_MULTICAST "
```

Pour exploiter et filtrer les résultats voulus nous avons écrit des scripts AWK. Par la suite nous avons présenté les résultats sous forme des courbes par le programme **Gnuplot**.

3.3 Paramètres des protocoles de simulation

Le tableau **(5.2)** suivant montre les valeurs de paramètres que nous avons utilisés dans les simulations:

protocole	paramètre	valeur
protocole MAODV	UPPER_LEVEL_PORT	100
	IP_MULTICAST	0xE000000
Protocole WASRM	La probabilité du cache (p)	0.3
	C1, C2	2
	D1, D2	1
	Taille du buffer (cache) des nœuds	50 paquets

Tableau 5. 2: Paramétrage des protocoles de simulation

3.4 Evaluation des performances

Afin d'analyse les deux aspects de la performance à savoir: l'impact de la taille du groupe multicast et de la charge de réseau, nous avons évalué les performances en faisant varier trois paramètres: le temps de pause (P), la taille du groupe multicast (G) et le nombre de sources (s).

3.4.1 Impact de la taille du groupe multicast

Nous fixons le nombre de source (S) à une source et nous varions la taille du groupe multicast (G) de 5 à 25 membres, où le nombre de récepteurs vaut la taille du groupe -1, et le temps de pause (P) de 0, 130 et 70 sec. Les figures **(5.1), (5.2)** et **(5.3)** schématisent chacune deux courbes dans un environnement ad hoc fixe, à faible mobilité et à forte mobilité respectivement. La courbe de gauche illustre le taux de paquets livrés avec succès et la deuxième représente le délai moyen de bout en bout des protocoles WASRM et MAODV.

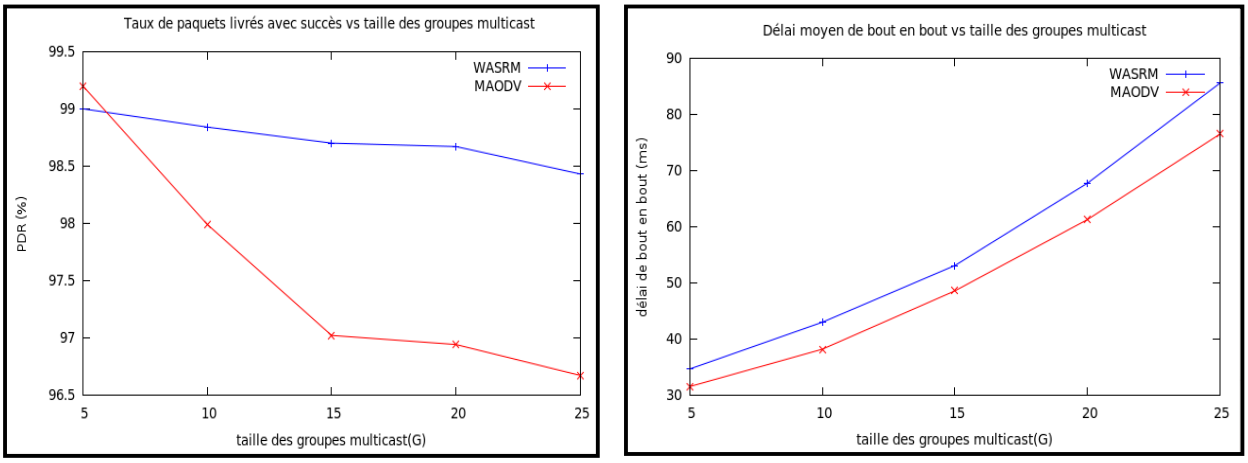

Figure 5. 1: Taux de paquets livrés et délai moyen de bout en bout en fonction de la taille du groupe multicast (G) dans un réseau ad hoc fixe P=0(s); S=1

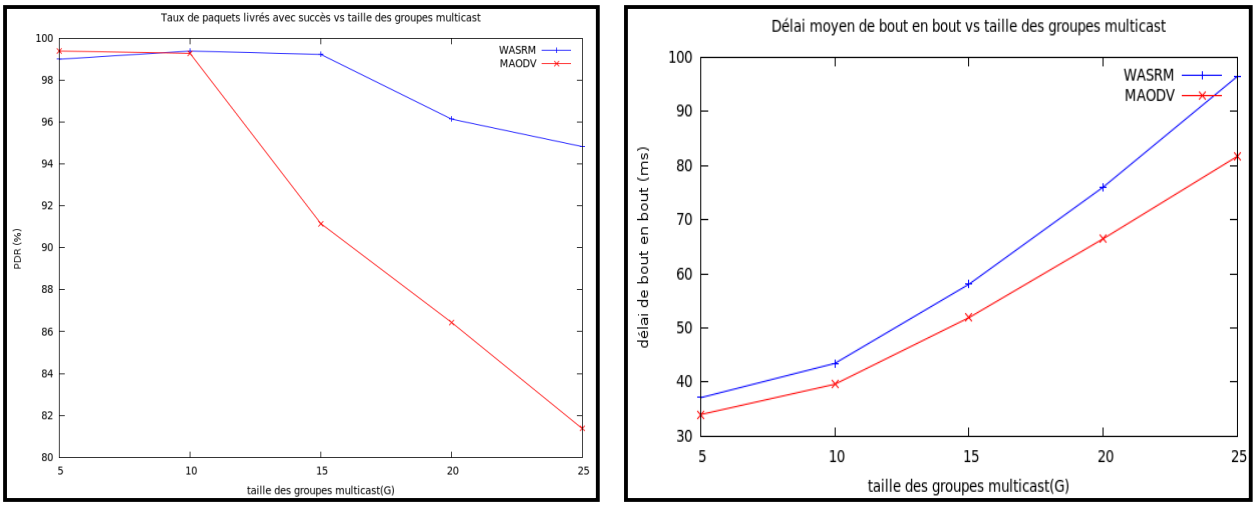

Figure 5. 2: Taux de paquets livrés et délai moyen de bout en bout en fonction de la taille du groupe multicast (G) dans un réseau ad hoc à faible mobilité P=130 (s); S=1

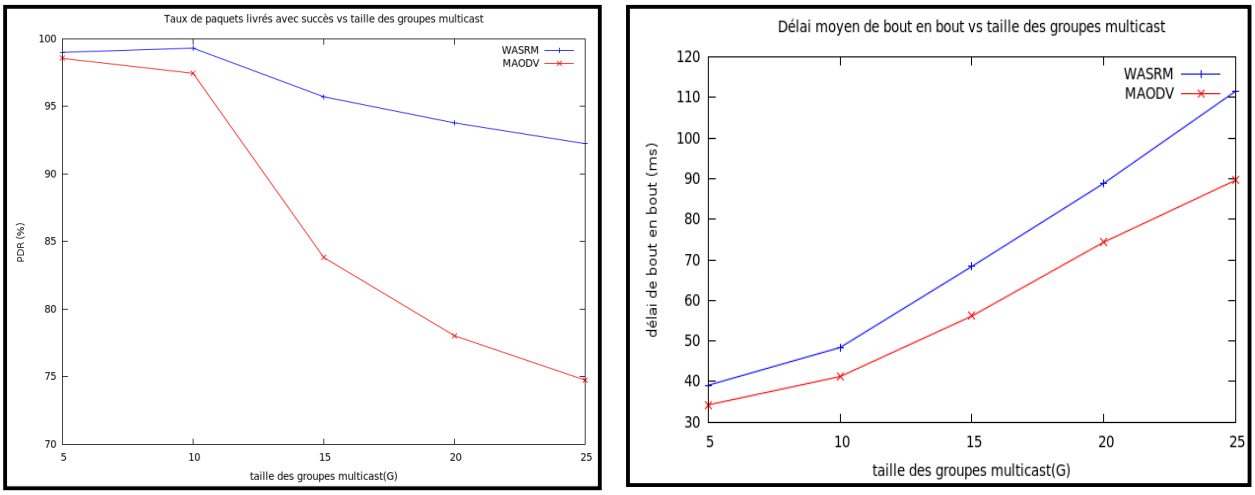

Figure 5. 3: Taux de paquets livrés et délai moyen de bout en bout en fonction de la taille du groupe multicast (G) dans un réseau ad hoc à forte mobilité P=70 (s); S=1

La figure **(5.1)** nous montre d'abord que le taux de livraison de paquets de données du protocole WASRM diminue légèrement si la taille du groupe multicast augmente (presque 98.5%). Cependant, les figures **(5.2)** et **(5.3)** nous montrent que cette diminution soit

augmentée avec l'augmentation du niveau de mobilité, à partir de G=15, sans dépasser le seuil de 90%. Ainsi, nous remarquons que ce taux, pour le protocole de routage multicast MAODV, diminue de façon appréciable (presque 75%) dans tous les scénarios de simulation (fixe, faiblement mobile et fortement mobile) avec l'augmentation du nombre de récepteurs. Ceci est justifié par le fait que si le niveau de mobilité des nœuds augmente, il devient plus difficile de maintenir les liens d'arbre multicast (fragile) au niveau du réseau et donc le nombre de paquets perdus augmente.

D'après ces observations, nous constatons que le protocole WASRM soit fiable avec un nombre important des membres de groupe multicast (récepteurs) en donnant un taux supérieur à 90% de livraison réussite dans certains niveaux de mobilité des nœuds de réseau, et que la fiabilité du protocole de routage multicast non fiable (MAODV) augmente avec le processus de recouvrement local du protocole de transport multicast fiable sus-jacent (WASRM).

Dans les figures précédentes, les courbes à droite nous montrent aussi que le délai de bout en bout devient plus important dans un environnement ad hoc mobile avec l'augmentation de la vitesse de déplacement des nœuds. En effet, ce comportement peut être justifié par le fait que pour une mobilité rapide, la topologie du réseau change rapidement et par conséquent, un nombre important des liens d'arbre multicast risquent d'être cassé en fonction du nombre de récepteurs (taille de groupe). En plus, les nœuds mobiles composant le groupe multicast ont la tendance de s'éloigner. Ce qui donne des chemins plus longs (en nombre de sauts) entre la source et l'un des membres du groupe.

Sur ces mêmes figures, nous remarquons que le délai de bout en bout du protocole WASRM dépend fortement du délai de bout en bout du protocole MAODV qui est augmenté aussi dans tous les scénarios. A partir de ces remarques, nous constatons que malgré la différence du délai entre le protocole MAODV et le protocole WASRM qui a une relation de dépendance, nous gagnons presque 20 ms sur le délai pour la livraison fiable du trafic multicast.

3.4.2 Impact de la charge de réseau

Nous fixons la taille du groupe multicast (G) à 20 membres et nous varions le nombre de sources (S) de 1 à 5 sources, et le temps de pause (P) de 0, 130 et 70 sec. Les figures **(5.4)**, **(5.5)** et **(5.6)** schématisent chacune deux courbes dans un environnement ad hoc fixe, à faible mobilité et à forte mobilité respectivement. La courbe de gauche illustre le taux de paquets livrés avec succès et la deuxième représente le délai moyen de bout en bout des protocoles WASRM et MAODV.

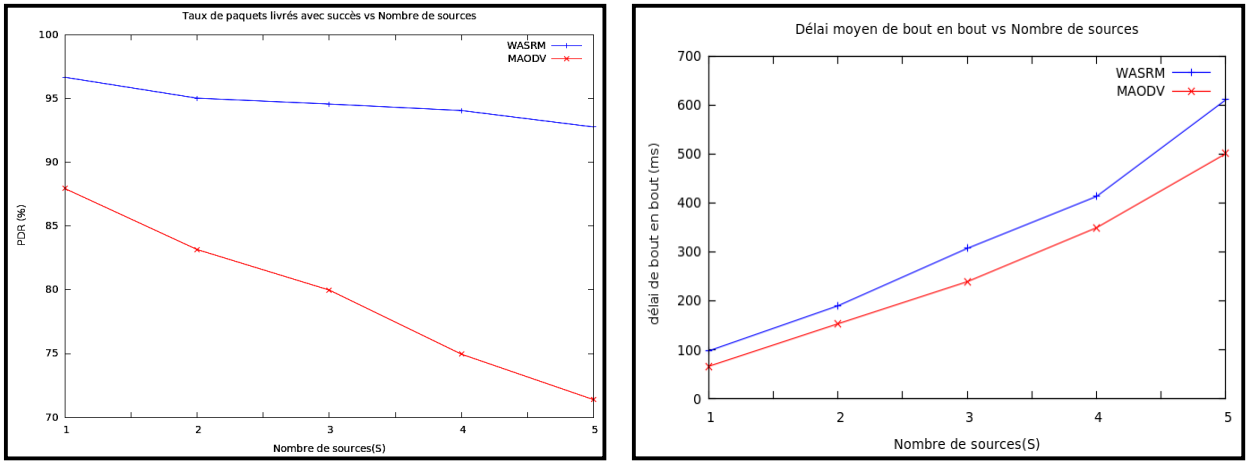

Figure 5. 4: Taux de paquets livrés et délai moyen de bout en bout en fonction du nombre de sources(S) dans un réseau ad hoc fixe P=0(s); G=20

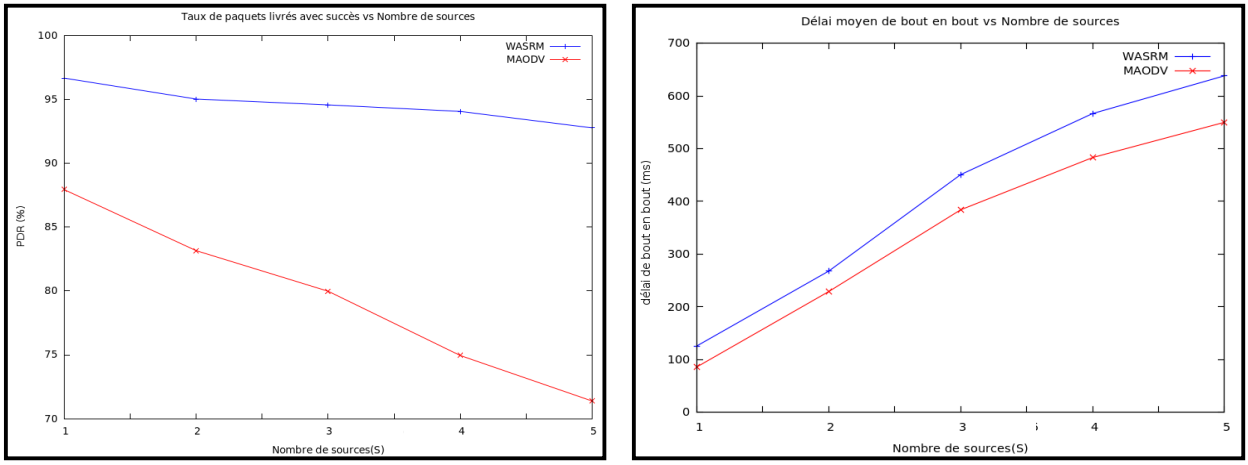

Figure 5. 5: Taux de paquets livrés et délai moyen de bout en bout en fonction du nombre de sources(S) dans un réseau ad hoc à faible mobilité P=130(s); G=20

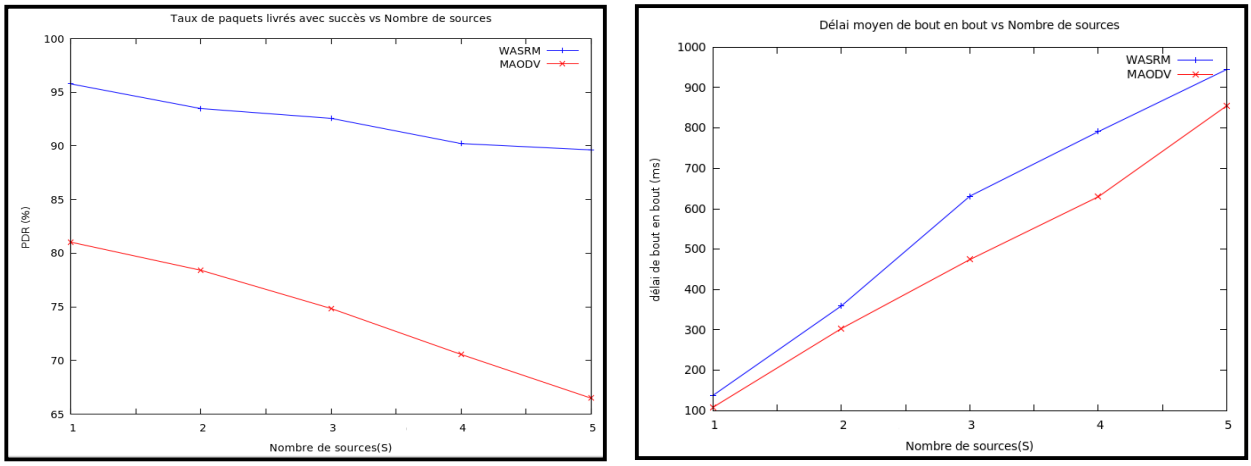

Figure 5. 6: Taux de paquets livrés et délai moyen de bout en bout en fonction du nombre de sources(S) dans un réseau ad hoc à forte mobilité P=70(s); G=20

Dans les figures **(5.4)**, **(5.5)** et **(5.6)** les courbes à gauche présentent le taux de la livraison fiable de paquets des protocoles WASRM et MAODV. Nous remarquons que le protocole WASRM est fiable avec presque 90% de taux de réussite de livraison même dans un réseau à forte charge. Cependant dans le même contexte, le taux de perte du protocole MAODV

est augmenté davantage (taux de réussite diminue). Ceci est du à la collision au niveau MAC avec un nombre important d'émissions simultanées d'une part, et du changement fréquentiel de topologie au niveau réseau d'une autre part. A partir de ces figures, nous constatons que le protocole WASRM puisse maintenir son taux de réussite de livraison proche de 90% dans les scenarios où celui du MAODV se dégrade au-dessous de 70%.

Dans les mêmes figures, les courbes à droite nous donnent le délai moyen de bout en bout des protocoles WASRM et MAODV. On remarque qu'avec un groupe multicast de taille G=20, le délai du protocole MAODV soit augmenté au delà de 900 ms, à partir de presque 100 ms, dans un réseau à forte mobilité et charge. Nous expliquons cette augmentation par le fait qu'avec un nombre important des membres de groupe, leur déplacement peut motiver le changement fréquentiel de routes en engendrant un nombre important des paquets de contrôle pour l'établissement des nouvelles routes et toutefois un overhead additionnel au niveau réseau qui peut retarder la livraison des paquets de données. Sur ces mêmes courbes, nous remarquons aussi que le délai de bout en bout du protocole MAODV peut ainsi affecter celui du protocole WASRM. Cependant, il garde une différence presque stable au regard de cette affectation.

D'après les remarques au-dessus, nous constatons que le nombre de sources et la mobilité des nœuds de réseau puissent influencer négativement sur le délai de livraison de bout en bout du protocole MAODV par rapport au celui du protocole WASRM.

En conclusion, les résultats de simulations ont montré que le protocole de transport multicast fiable WASRM permet le passage à l'échelle d'un grand nombre de récepteurs (scalabilité) dans les réseaux à forte mobilité et forte charge, du fait qu'il ait gardé ses performances (un taux supérieur de livraison fiable et un délai moyen de bout en bout stable) avec un nombre important des membres du groupe multicast (taille de groupe).

6. Conclusion

Dans ce chapitre on a validé notre protocole proposé WASRM par la simulation. Pour cela nous avons évalué ses performances avec le simulateur de réseaux NS2. Pour modéliser un environnement ad hoc réel et pour mesurer la fiabilité du protocole WASRM et sa capacité de satisfaire la propriété de scalabilité, nous avons développé plusieurs scénarios de simulation qui ciblent certaines caractéristiques des réseaux ad hoc (tel que la mobilité, la taille du groupe multicast et le nombre de sources). Enfin, nous avons présenté les résultats des différentes simulations sous forme des courbes. Dans la majorité des cas, les résultats obtenus montrent que la solution proposée offre de meilleures performances par rapport au protocole de routage multicast sous-jacent MAODV.

Conclusion générale

Conclusion générale

Dû à la simplicité de déploiement des réseaux ad hoc dans des situations où l'installation des infrastructures est difficile, ainsi qu'à leurs caractéristiques d'auto-organisation orientés-groupes, plusieurs applications requièrent un service de communication multicast ont été déployées au sein de ces réseaux. Cependant, dû à leurs caractéristiques et aux contraintes des ressources fournies limitées (bande passante, mémoire, énergie) imposées par les réseaux ad hoc, le support du service multicast est devenu un problème complexe à traiter.

L'objectif de ce mémoire était de proposer un protocole afin de traiter l'un des problèmes du support du multicast dans les réseaux sans fil ad hoc, la fiabilité multicast au niveau transport qui est exigée par les applications déployées dans ces réseaux.

Notre étude des travaux actuels dans le cadre de ce mémoire, nous a permis d'extraire certains problèmes liés au passage à l'échelle des solutions proposées. Afin de les résoudre, nous avons proposé un nouveau protocole appelé « WASRM ».

Le protocole WASRM s'articule sur la combinaison des temporisateurs aléatoires avec le support des routeurs (nœuds intermédiaires) actifs. Cette combinaison a la tendance d'alléger les problèmes d'implosion des acquittements en feedback et de localité de pertes afin d'assurer la scalabilité de retransmissions d'une part, et d'assurer un recouvrement local afin d'améliorer la fiabilité du protocole d'une autre part. Notre solution utilise aussi le concept d'acquittement passif et l'interaction avec la couche MAC pour minimiser le taux d'erreurs de transmission.

Notre protocole proposé a été validé par simulation en évaluant ses performances via le simulateur de réseaux NS2. Les résultats de simulation nous montrent que WASRM permet le passage à l'échelle d'un grand nombre de récepteurs du fait qu'il garantisse un niveau supérieur de fiabilité dans certaines conditions des réseaux ad hoc.

Finalement nous envisageons poursuivre ce travail de recherche en limitant le nombre des nœuds intermédiaires actifs par une fonction de choix multicritères afin d'exploiter l'hétérogénéité des nœuds de réseau (taille du mémoire, énergie, mobilité…), et en utilisant d'autres métriques de performance (l'overhead de retransmission). Aussi, nous voulons proposer un protocole de routage multicast sous-jacent plus robuste et efficace afin d'améliorer les performances du protocole de transport multicast fiable sus-jacent.

Bibliographie

[1] G. Pujolle, **''Les Réseaux ''**, Éditions Eyrolles, France, 2007, pp. 14, 21, 40,507.

[2] A. Tanenbaum, D. J. Wetherall, **'' Réseaux 5e édition '',** Pearson Education, France, 2011, pp. 6-43.

[3] L. L. Peterson, B. S. Davie, **'' RESEAUX D'ORDINATEURS, une approche orientée système'',** Morgan Kaufmann Publishers, traduit chez Vuibert (1998), France, 1996, pp. 9-29.

[4] D. Dromard, D. Seret, **'' Architecture des réseaux'',** Collection Synthex, Pearson Education, France, 2009, pp. 90-97.

[5] F. Lemainque, **'' Tout sur les Réseaux sans fil''**, Collection CommentCaMarche.net, Dunod, France, 2009, pp. 5-57.

[6] S. Pierre, **'' Réseaux et systèmes informatiques mobiles : fondements, architectures et applications ''**, Presses internationales Polytechnique, Canada, 2011, pp. 3-29.

[7] K. Al Agha, G. Pujolle, G. Vivier,**''Réseaux de mobiles et réseaux sans fil'',** Éditions Eyrolles, France, 2001, pp. 23,341.

[8] C. Perkins, **'' IP Mobility Support for IPv4'',** Internet standard RFC 3220, January 2002.

[9] C. K. Toh, "**Ad Hoc Mobile Wireless Networks: Protocols and Systems",** Prentice Hall, États-Unis, 2001.

[10] P. Mohapatr, A. V. Krishnamurthy, "**AD HOC NETWORKS Technologies and Protcols",** Springer Science + Business Media, États-Unis, 2005, pp. 1-22.

[11] S. K. Sarkar, T. G. Basavaraju, C. Puttamadappa, "**Ad hoc mobile wireless networks: principles, protocols, and applications"**, Auerbach Publications,Taylor & Francis Group, États-Unis, 2008 , pp. 21-36, 115-139.

[12] D. P. Agrawal, Q. A. Zeng, "**Introduction to Wireless and Mobile Systems Third Edition"**, Cengage Learning, États-Unis, 2011, pp. 220-236, 317-520.

[13] S. E. Deering**, "Host Extensions for IP Multicasting",** Internet standard RFC 1112, August 1989.

[14] R. Wittmann,M. Zitterbart , "**Multicast Communication: Protocols, Programming, & Applications** ", Morgan Kaufmann**,** États-Unis, 2000, pp. 135-144.

[15] S. Loye, "**Le multicast IP: principes et protocoles**", Revue des Techniques de l'ingénieur. Télécoms, Publication de Techniques de l'ingénieur, Paris, France, vol. TEA2, n°. TE7527, 2005, ISSN 1632-3823.

[16]R. Rümmler, A. Gluhak, A. H. Aghvami, "**Multicast in Third-Generation Mobile Networks: Services, Mechanisms and Performance"**, John Wiley & Sons Ltd, West Sussex United Kingdom, 2009, pp. 12-85.

[17] D. G. Petitt,**" SOLUTIONS FOR RELIABLE MULTICASTING,"** Master's Thesis, NAVAL POSTGRADUATE SCHOOL, Monterey, California, 1996.

[18] A. Popescu, D. Constantinescu, D. Erman, D. Ilie, **"A Survey of Reliable Multicast Communication",** 3rd EuroNGI Conference on Next Generation Internet Networks, vol., n°., pp.111-118, 2007.

[19] A. Benslimane, "**Multimedia Multicast on the Internet**", British Library Cataloguing-in-Publication Data, 2006, pp. 1-49,135-217.

[20] H.Gossain, C.d.M Cordeiro, D.P Agrawal, "**Multicast: wired to wireless**," Communications Magazine, IEEE , vol.40, n°.6, pp.116,123, Jun 2002.

[21] S. Deering, W. Fenner, B. Haberman, **"Multicast Listener Discovery for IPv6",** RFC 2710, October 1999.

[22] S. Deering, D. Cheriton, "**Multicast Routing in Datagram Internetwork and Extended LANs**", ACM Transactions on Computer Systems, vol. 8, n°. 2, pp. 85-110,1990.

[23] J. Moy, "**Multicast Routing Extensions for OSPF**", Commun. ACM, vol. 37, pp. 61-66, 1994.

[24] A. Ballardie, "**Core Based Trees (CBT version 2) Multicast Routing; Protocol Specification**", RFC 2189, 1997.

[25] D.Waitzman, S. Deering, C.Partridge, "**Distance-Vector Multicast Routing Protocol**", RFC 1075, experimental, 1988.

[26] L. Derdouri, **''Une Approche Hybride pour le Transport Multicast Fiable dans un Environnement Actif**'', thèse de doctorat, Université Mentouri Constantine, Algérie, 2009.

[27] A. Mankin, A. Romanow, S. Bradner, V. Paxson, "**IETF Criteria for Evaluating Reliable Multicast Transport and Application Protocols**", Internet standard RFC 2357, June 1998.

[28] V.O.-K. Li, Z. Zhang, "**Internet multicast routing and transport control protocols**", Proceedings of the IEEE, vol.90, n°.3, pp.360-391, Mar 2002.

[29] M. Handley, S. Floyd, B. Whetten, R. Kermode, L. Vicisano, M. Luby,"**The Reliable Multicast Design Space for Bulk Data Transfer**", RFC 2887, August 2000.

[30] F. d. Belleville,"**Transport multipoint fiable à très grande échelle : Intégration de critères de coût en environnement Internet hybride satellite / terrestre**", thèse de doctorat, Institut National Polytechnique de Toulouse, France, 2004.

[31] J. Nonnenmacher, **" RELIABLE MULTICAST TRANSPORT TO LARGE GROUPS''** , thèse de doctorat, Ecole polytechnique fédérale de Lausanne**,** Sophia Antipolis, Eurecom, 1998.

[32] J.W. Atwood, "**A classification of reliable multicast protocols**," Network, IEEE, vol.18, n°.3, pp.24-34, May-June 2004.

[33] S. Ramakrishnan, B.N. Jain**,"A negative acknowledgement with periodic polling protocol for multicast over LANs**", In IEEE Infocom, pp. 502-511, march 1987.

[34] B. N. Levine, J.J. Garcia-Luna-Aceves, **" A comparison of reliable multicast protocols"**, Multimedia Systems 6, Springer-Verlag, pp. 334–348, 1998.

[35] S. Floyd, V. Jacobson, C.-G. Liu, S. McCanne, L. Zhang, **"A Reliable Multicast Framework for Light-Weight Sessions and Application Level Framing,"** IEEE/ACM Transactions on Networking, vol. 5, n°. 6, pp. 784-803, Dec. 1997.

[36] H. Holbrook, S. Singhal, D. Cheriton, "**Log-based receiver reliable multicast for distributed interactive simulation**", In: ACM SIG-COMM'95, pp 328–341, Cambridge, MA, USA, 28 August–1 September 1995.

[37] R. Yavatkar, J. Griffioen, M. Sudan, "**A Reliable Dissemination Protocol for Interactive Collaborative Applications**", Proc. ACM Multimedia '95, 1995.

[38] J.M. Chang, N. F. Maxemchuk, "**Reliable broadcast protocols**", Journal of ACM Transactions on Computer Systems (TOCS), vol. 2(3), pp. 251 – 273, August 1984.

[39] B. Whetten, T. Montgomery, S. Kaplan, "**A High Performance Totally Ordered Multicast Protocol**", Theory and Practice in Distributed Systems, Springer Verlag, pp. 33–57, 1995.

[40] C. Papadopoulos, G. Parulkar, G. Varghese, "**An error control scheme for large-scale multicast applications**", Proceedings of IEEE INFOCOM '98 Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies., vol.3, n°., pp.1188-1196, 29 Mar-2 Apr 1998.

[41] Y. Gao, Y. Ge, J. C. Hou, "**RMCM: Reliable multicast for core-based multicast trees**", in Proceedings of International Conference on Network Protocols, vol., n°., pp.83-94, Osaka, Japan, 14 Nov -17 Nov 2000.

[42] S. K. Kasera et al, "**Scalable fair reliable multicast using active services**", Network, IEEE, vol. 14, n°.1, pp. 48–57, Jan/Feb 2000.

[43] L.H. Lehman, S. J.Garland, D. L. Tennenhouse, "**Active reliable multicast**", Proceedings of IEEE INFOCOM '98. Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies, vol.2, n°., pp.581-589, San Francisco, CA, 29 Mar-2 Apr 1998.

[44] M. Maimour, C. Pham, "**DyRAM: an Active Reliable Multicast framework for Data Distribution"**, Journal of Cluster Computing, vol. 7(2), pp. 163-176, April 2004.

[45] L. Derdouri, D. E. Saidouni, M. Benmohammed," **Reliable Multicast Transport in Active Environment**", in Proceeding CSIT'06 Conference Computer Science and Information Technologie, Amman, Jordan, Mars 2006.

[46] I. Romdhani, M. Kellil, H. Y. Lach, A. Bouabdallah, H. Bettahar, "**IP Mobile Multicast: Challenges and *s*olutions"**, Communications Surveys & Tutorials, IEEE, vol.6, n°.1, pp. 18-41, First Quarter 2004.

[47] V. Leggieri, P. Nobili, C. Triki, "**Minimum power multicasting problem in wireless networks**", Mathematical Methods of Operations Research, Springer-Verlag, vol. 68(2) , pp. 295-311, 2008.

[48] P. Chaporkar, S. Sarkar, "**Wireless multicast: theory and approaches**", IEEE Transactions on Information Theory, vol.51, n°.6, pp.1954-1972, June 2005.

[49] U. Varshney, "**Multicast Over Wireless Networks",** Communications of the ACM, vol. 45, n°. 12, pp. 31–37, 2002.

[50] G. Xylomenos, G. Polyzos, "**IP Multicast for Mobile Hosts**", IEEE Communications Magazine, vol.35 (1), pp. 54–58, January 1997.

[51] U. Varshney, S. Chatterjee, "**Architectural issues to support multicasting over wireless and mobile networks**", IEEE WCNC Wireless Communications and Networking Conference, vol.1, n°., pp.41-45, 1999.

[52] N. Nikaein, C. Bonnet, "**Wireless Multicasting in an IP Environment**", In Proceedings of the 5th International Workshop on Mobile Multimedia Communication MoMuc'98,Berlin Germany, Oct 12–14 1998.

[53] L.H. Sahasrabuddhe, B. Mukherjee, **"Multicast routing algorithms and protocols: a tutorial"**, Network, IEEE, vol. 14, n°.1, pp.90-102, Jan/Feb 2000, ISSN 0890-8044.

[54] C. Perkins, **"IP Mobility Support"**, IETF RFC 2002, October 1996.

[55] K.Obraczka, G. Tsuduk, "**Multicast routing issues in ad hoc networks**», IEEE ICUPC '98 International Conference on Universal Personal Communications, vol.1, n°., pp.751-756, 5-9 Oct 1998.

[56] O. S. Badarneh, M. Kadoch,"**Multicast routing protocols in mobile ad hoc networks: a comparative survey and taxonomy**", EURASIP Journal on Wireless Communications and Networking, vol.2009, n°.26, pp.1-42, January 2009.

[57] L. Junhai, X. Liu, Y. Danxia, "**Research on multicast routing protocols for mobile ad-hoc networks**", Computer Networks : The International Journal of Computer and Telecommunications Networking, vol. 52,n°. 5, pp. 988-997, 10 April 2008.

[58] J. Xie, R. R. Talpade, A. McAuley, M. Liu, "**AMRoute: ad hoc multicast routing protocol**", Mobile Networks and Applications, vol. 7, n°. 6, pp. 429–439, 2002.

[59] C. Gui, P. Mohapatra, "**Efficient overlay multicast for mobile ad hoc networks**", in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '03), vol.2, pp. 1118–1123, 2003.

[60] K. Tang, M. Gerla, "**MAC reliable broadcast in ad hoc networks**", in Proceedings of the IEEE Military Communications Conference (MILCOM '01), vol. 2, pp. 1008–1013, 2001.

[61] W. Si and C. Li, "**RMAC: a reliablemulticastMAC protocol for wireless ad hoc networks**", in Proceedings of the International Conference on Parallel Processing (ICPP '04), pp. 494–501, 2004.

[62] J. G. Jetcheva, D. B. Johnson, "**Adaptive demand-driven multicast routing in multi-hop wireless ad hoc networks**" , in Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '01),pp.33–44, 2001

[63] E. M. Royer, C. E. Perkins, "**Multicast ad hoc on demand distance vector (MAODV) routing**" , Internet-Draft, draft-ietf-draft-maodv-00.txt, 2000.

[64] S.-J. Lee, W. Su, M. Gerla, "**On-demand multicast routing protocol in multihop wireless mobile networks**", Mobile Networks and Applications, vol. 7, n°. 6, pp. 441–453, 2002.

[65] J. J. Garcia-Luna-Aceves, E. L. Madruga, "**The core-assisted mesh protocol**" , IEEE Journal on Selected Areas in Communications, vol. 17, n°. 8, pp. 1380–1394, 1999.

[66] R. S. Prasun Sinha, V. Bharghavan, "**MCEDAR: multicast core-extraction distributed ad hoc routing**", in Proceedings of the Wireless Communications and Networking Conference, vol.3, pp. 1313–1317, 1999.

[67] L. Ji, M.S. Corson, "**Differential destination multicast-a MANET multicast routing protocol for small groups**", in Proceedings of the 20th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'01), vol.2, pp. 1192–1201, 2001.

[68] K. Chen, K. Nahrstedt,"**Effective location-guided tree construction algorithms for small group multicast in MANET**", Proceedings of the INFOCOM, pp.1180–1189, 2002.

[69] T. Kunz,"**Reliable Multicasting in MANETs**", Contract Report, DRDC-Ottawa, July 2003.

[70] S. Tanaraksiritavorn, S. Mishra, "**Evaluation of gossip to build scalable and reliable multicast protocols**," Proceedings of MASCOTS 2002, 10th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunications Systems, vol., n°., pp.463-470, 2002.

[71] L. Rizzo, L. Vicisano, "**RMDP: A FEC-Based Reliable Multicast Protocol for Wireless Environments**", Mobile Computing and Communications Review, vol. 2, n°. 2, pp. 23–32, April 1998.

[72] D. H. Sadok, C. M. Cordeiro, J. Kelner, "**A Reliable Subcasting Protocol for Wireless Environments**", The 2nd International Conference on Mobile and Wireless Communication Networks, Paris, France, May 2000.

[73] O. O. Sonmez, "**A Survey on Reliable Multicast Approaches for Mobile Ad Hoc",** Networks Software Technologies, Delft University of Technology, the Netherlands, March 1st 2007.

[74] B. Ouyang, X. Hong, Y. Yi, "**A comparison of reliable multicast protocols for mobile ad hoc networks**," Proceedings IEEE SoutheastCon 2005, vol., n°., pp.339-344, 8-10 April 2005.

[75] T. Gopalsamy, M. Singhal, D.Panda, P. Sadayappan, "**A reliable multicast algorithm for mobile ad hoc networks**", In Proceedings of ICDCS, 2002.

[76] V. Rajendran, Y. Yi, K. Obraczka, S.J.Lee, K.Tang, M.Gerla, "**Reliable, Adaptive, Congestion-Controlled Adhoc Multicast Transport Protocol: Combining Source-based and Local Recovery**", UCSC Technical Report, 2003.

[77] Tang, K., Obraczka, K., Lee, S.J., Gerla, M, "**A reliable, congestion-controlled multicast transport protocol in multimedia multi-hop networks**", Proceedings of IEEE WPMC 2002, Honolulu, USA, pp. 252-256, October 2002.

[78] A. Sobeih, H. Baraka, A. Fahmy, "**Remhoc: A reliable multicast protocol for wireless mobile multihop ad hoc networks",** in Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC), 2004.

[79] S. Wu, C. Bonnet,**"ARMPIS: an active reliable multicasting protocol for ad hoc networks",** WMSCI 2004, 8th World Multi-Conference on Systemics, Cybernetics and Informatics, Orlando, USA, July 18-21 2004.

[80] T. Al-Ahdal, S. Subramaniam, M. Othman, Z. Zukarnain, "**A Source Tree Reliable Multicast Protocol for Ad-Hoc Networks,**" The International Arab Journal of Information Technology, vol. 5, pp. 273-280, 2008.

[81] M. Pandey, D. Zappala, **"Hop-by-hop multicast transport for mobile ad hoc wireless networks,"** MASS 2008, 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, vol., n°., pp.45-455, Sept 29 -Oct 2 2008.

[82] R. Chandra, V. Ramasubramanian, K. Birman, "**Anonymous gossip: improving multicast reliability in mobile ad-hoc networks**", International Conference on Distributed Computing Systems, pp. 275-283,2001.

[83] . Luo, P. T. Eugster, J.-P. Hubaux, "**Route driven gossip: Probabilistic reliable multicast in ad hoc networks**", INFOCOM'03, San Francisco, CA, , pp.2229-2239, March 2003.

[84] Z. Genc, O.Ozkasap, "**EraMobile: Epidemic-Based Reliable and Adaptive Multicast for MANETs**," IEEE WCNC 2007, Wireless Communications and Networking Conference, vol., n°., pp.4395-4400, 11-15 March 2007.

[85] H.Hassanein, L.Huang, **"Reliable multicast in wireless ad hoc and sensor networks,"** IPCCC 2005, 24th IEEE International Performance, Computing, and Communications Conference, vol., n°., pp.459-464, 7-9 April 2005.

[86] http://www.isi.edu/nsnam/ns/

[87] S.V. Mallapur, Siddarama . R. Patil **"Survey on Simulation Tools for Mobile Ad-Hoc Networks",** IRACST, International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.2, n°.2, April 2012.

[88] M.A.Rahman,A.Pakštas,F.Z.Wang, **"Network modelling and simulation tools"**, Simulation Modelling Practice and Theory, Vol.17,n°.6, pp. 1011-1031,July 2009, ISSN 1569-190X.

[89] Y. Zhu, T. Kunz, **"MAODV Implementation for NS-2.26"**, Systems and computer Engineering, Carlton University, Technical Report SCE-04-01,January 2004.