République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

Université Abderrahmane Mira

Projet de Fin d'études

Pour l'obtention du diplôme de master académique en Informatique

Spécialité : Administration et sécurité des réseaux

Thème

Impact de la taille de la fenêtre de contention dans les réseaux AD HOC

Réalisé par :

FADMI Melissa

TARZALT Sylia

Encadré par :

MEHAOUED Kamal

Examiné par :

AMROUN kamel

ELBOUHISSI Houda

Année universitaire : **2020/2021**

REMERCIEMENT

En premier lieu, nous remercions le Bon Dieu « ALLAH » de nous avoir donné la force et le courage pour accomplir ce travail.

La réalisation de ce mémoire a été possible grâce au soutien de plusieurs personnes à qui nous voudrions adresser toute notre gratitude.

Nous tenons à exprimer notre gratitude et notre reconnaissance envers notre encadreur Mr MEHAOUED Kamel de nous avoir encadré, suivi et dirigé pendant toute la durée de ce travail et surtout pour sa patience, ses judicieux conseils et sa disponibilité.

Nous remercions tous les professeurs, intervenants et toutes les personnes qui par leurs paroles, leurs écrits, leurs conseils et leurs critiques ont guidés nos réflexions et ont accepté de nous rencontrer et de répondre à nos questions durant nos recherches.

Nous adressons bien évidemment nos remerciements à nos familles, nos parents, nos frères et sœurs qui ont tous su nous soutenir sans insister et s'informer de l'état d'avancement de nos travaux sans être trop curieux.

Un grand merci pour tous les enseignants de l'université Abderrahmane Mira qui nous ont fourni les outils nécessaires à la réussite de nos études universitaires du premier au dernier jour.

Enfin, nous désirons exprimer notre gratitude à nos amis et collègues qui nous ont apporté leur soutien moral tout au long du chemin de la réalisation de ce travail.

DEDICACE

Je dédie ce travail

A ma famille, qui m'a doté d'une éducation digne, m'a soutenu pendant toute la période de mes études et durant ce mémoire et Particulièrement à mes chers parents, pour leurs amours, encouragements et soutien ce qui a fait de moi ce que je suis aujourd'hui.

A mes sœurs et mon seul et petit frère Wassim qui ont partagé avec moi tous les moments d'émotions lors de la réalisation de ce mémoire, ils m'ont chaleureusement supporté et encouragé, que dieu les protège et leurs offre la santé la chance et le bonheur.

A tous les autres étudiants en master2 spécialité ASR et même dans d'autre spécialité, je leurs souhaite un bon courage pour leurs soutenances et bonne chance dans leurs vies.

A toutes mes amies sans particuliers, je commence par Lynda, Sara, kenza……

A monsieur Keddou A. basset qui a toujours été là pour moi

Sans oublier ma binôme Sylia, pour sa compréhension et sa présence morale et physique qui me donne à chaque fois la volonté et le courage de travailler sur ce mémoire.

MELISSA

DEDICACE

Je dédie ce modeste travail :

A mes parents

Grâce à leurs tendres encouragements et leurs grands sacrifices ils ont pu créer le Climat affectueux et propice à la poursuite de mes études. Aucune dédicace ne pourrait exprimer mon respect, ma considération et mon profond sentiment envers eux.Je prie le bon Dieu de les bénir, en espérant qu'ils seront toujours fiers de moi.

A mes très chers frères et sœurs

Je vous dédie ce travail en vous souhaitant un avenir radieux, pleins de bonheur et de Succès. Que dieu, le tout puissant, vous préserve et vous procure santé et longue vie.

A mes ami(e)s et mes collègues

En témoignage de l'amitié qui nous unie et des souvenirs de tous les moments que nous avons passés ensemble, je vous dédie ce travail et je vous souhaite une vie pleine de réussite et de bonheur.

A tous les professeurs qui m'ont enseigné ou aidé.

SYLIA

Sommaire

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABRÉVIATIONS

AODV	Ad hoc On-Demand Distance Vector Routing
CBR	Cluster Based Routing
CW	Contention Window
DCF	Distributed Coordination Function
DIFS	DCF Inter Frame Space
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
IETF	Internet Engineering Task Force
LLC	Logical Link Control
LSR	Link State Routing
MANET	Mobile Ad hoc NETwork
NS2	Network Simulator 2
OSLR	Optimized Link State Routing
PCF	Point Coordination Function
QoS	Quality of service
RREQ	route request
SDCR	Software Defined Cognitive Radio
STAR	Source-Tree Adaptative Routing
WAVE	Wireless Ability in Vehicular Environnements
Wi-Fi	Wireless Fidélité
WRP	Wireless Routing Protocol
ZRP	ZONE Routing Protocol

Introduction générale

Les réseaux sans fil ont connu une forte expansion et sont de plus en plus populaires du fait de leur facilité de déploiement. L'évolution rapide de la technologie dans le domaine de la communication sans fil, a permis aux usagers munis d'unités de calcul portables d'accéder à l'information à n'importe quel moment depuis n'importe quel endroit. Cet endroit permet une libre mobilité tout en assurant sa connexion avec le réseau. La plupart de ces réseaux sont des réseaux centralisés et ont besoin d'administrations centralisées et d'infrastructures coûteuses.

Un réseau Ad hoc mobile (MANET) est un système autonome constitué de nœuds mobiles reliés par des liens sans fils qui ne suppose pas d'infrastructure préexistante. Le réseau ad hoc se forme de manière spontanée et provisoire dès que plusieurs nœuds mobiles se trouve à portée radio les uns des autres. Les nœuds communiquent, selon la distance qui les sépare, par deux modes de communication : soit les nœuds mobiles peuvent directement communiquer (en transmission ad hoc) car ils sont à portées de transmission, soit ils doivent utiliser d'autres nœuds mobiles comme des relais pour acheminer les paquets à destination. Ainsi, chaque nœud est à la fois utilisateur finale est routeur afin de relayer les paquets vers leur destination finale, en raison de la couverture limitée du champ radio disponible pour chaque nœud.

Dans le cas d'un MANET {Mobile Ad hoc NETwork), plusieurs problèmes existent, notamment la sécurité, l'ordonnancement et le routage puisqu'il n'y a pas de point d'accès qui s'occupe de la gestion. Voilà que le mouvement des nœuds ajoute une instabilité des liens entre les paires de nœuds du réseau.

Cette instabilité est une source de variation de la qualité de connexion allant jusqu'à une perte des données et un changement rapide de la topologie du réseau, la mobilité des hôtes, limitation de la bande passante, limitation de source d'énergie, débit du réseau, capacité de traitement de la mémoire.la question actuelle est de chercher une solution optimale pour améliorer les performances des réseaux ad hoc, plusieurs stratégies ont été proposées pour cela mais ces mécanismes développés ne sont pas approprié aux réseaux ad hoc, sont couteux, lents, et consomment beaucoup de ressources.

Dans ce travail, nous nous intéressons au problème de perte de paquets et débit lors de la transmission des données des nœuds nombreux dans un réseau ad hoc avec une taille de fenêtre de contention différente.

Un nœud souhaitant émettre une trame doit vérifier que le canal est resté inoccupé pendant une période au moins égale à un délai appelé DIFS (DCF Inter Frame Space). Si le canal est occupé ou devient occupé, le nœud doit retarder sa transmission jusqu'à ce que le support redevienne libre pendant une durée de DIFS. Le retard est déterminé par le tirage d'une valeur aléatoire appelée délai de backoff. Ce délai est décrémenté tant que le canal est inoccupé et arrêté dès que celui redevient actif. Quand le délai de backoff a atteint la valeur nulle, le nœud peut entamer sa transmission. Le tirage aléatoire du backoff est effectué dans un intervalle appelé fenêtre de contention (CW : Contention Window). La taille de cette fenêtre est fonction du nombre de tentatives de transmission. Sa taille est doublée à chaque tentative infructueuse. La valeur minimale et maximale de cette fenêtre (CW) nous indique son impact sur le débit et la perte des paquets lors de la transmission des données.

Dans le premier chapitre, nous introduisons les réseaux ad hoc, les différents concepts, leurs caractéristiques, ainsi que leurs applications. Nous exposerons par la suite, la couche Mac IEEE802.11 et ses caractéristiques. Le troisième chapitre sera consacré à la présentation de l'outil de simulation NS2 et les éléments qui l'accompagnent pour la simulation, nous faisons une étude comparative des deux paramètres (débit, perte de paquets) effectuant plusieurs retransmissions et en interprétant ensuite les résultats obtenus.

Chapitre I :

INTRODUCTION AUX RESEAUX MOBILES AD HOC

I.1-Introduction :

L'apparition de l'internet et son grand succès dans notre mode de vie ainsi l'évolution des équipements terminaux (ordinateurs, téléphones, etc.) sont autant d'éléments qui ont changés notre manière d'utiliser ces technologies, ainsi notre relation avec les moyens de communication.

Durant ces dernières décennies beaucoup de solutions de communication sans fil ont étés apparues et de plus en plus évolués, ces communications sans fil permettent aux nœuds mobiles de transmettre leurs informations avec une grande flexibilité d'utilisation dans des zones ouvertes. En particulier, ils offrent la mise en réseau des sites dont le câblage serait trop difficile et coûteux à réaliser.

Généralement, les réseaux mobiles sans fil sont divisés en deux catégories (les réseaux avec infrastructure ou cellulaire et sans infrastructure ou AD HOC), les activités de recherche dans ce domaine ont prouvé le développement de ces réseaux sans fil.

Les réseaux ad hoc sont des systèmes autonomes composés par un ensemble d'entités mobiles libres de se déplacer sans contraintes. Une définition de ces réseaux est donnée formellement dans RFC 2501[Corson and Macker, 1999] : "Un réseau Ad-hoc comprend des plates-formes mobiles (par exemple, un routeur interconnectant différents hôtes et équipements sans fil) appelées nœuds qui sont libres de se déplacer sans contrainte. Un réseau Ad-hoc est donc un système autonome de nœuds mobiles.

Ce premier chapitre consiste à définir les réseaux Ad hoc, leurs caractéristiques, et leurs domaines d'applications, par la suite nous présenterons leurs modes de routage et on va finir par citer leurs avantages et inconvénients.

I.2-Historique

A l'origine les réseaux ad-hoc mobiles ont été introduits pour améliorer les communications dans le domaine militaire, vu la nature dynamique de leurs opérations et champs d'action. Le début des années 1970 voit, au sein du projet militaire Américain DARPA (The Defense Advanced Research Projects Agency), la naissance des premiers réseaux utilisant le médium radio. Ces réseaux disposaient déjà d'une architecture distribuée, partageaient le canal de diffusion en répétant des paquets pour élargir la zone de couverture globale.

Par la suite, en 1983, *les Sur vivable Radio Networks* (SU RAN) furent développés par le DARPA. L'objectif était de dépasser les limitations (en particulier permettre le passage à des réseaux comportant énormément des nœuds, gérant la sécurité, l'énergie). Mais les recherches sur ces réseaux restaient exclusivement militaires. Ce n'est qu'avec l'arrivée du protocole 802.11 de l'IEEE (Institute of Electrical and Electronics Engineers) qui permet de bâtir des réseaux sans fil autour de bases fixes, que la recherche civile s'empare à la fin des années 90 des problématiques liées à ces réseaux[1].

I.3-Définition des réseaux mobiles AD HOC

Les réseaux ad hoc sont des réseaux mobiles et sans fil qui peuvent fonctionner sans infrastructure. Ils s'adaptent dynamiquement à leur environnement et à leur topologie. Les réseaux mobiles ad hoc sont généralement multi-sauts, ce qui signifie qu'il s'agit d'un groupe d'entités mobiles et / ou fixes qui forment un réseau dynamique temporaire avec ou sans l'aide d'une gestion centralisée. Ad hoc est une expression latine qui signifie « pour cela », qui signifie « uniquement pour cet objectif ». Nous utilisons souvent le terme « mobile » pour signifier « réseau mobile ad hoc », également connu sous le nom de MANET (mobile ad hoc network). Spécifier divers réseaux sans fil multi-sauts. La communication entre les nœuds du réseau effectue directement cette opération. Par conséquent, les nœuds peuvent se déplacer librement de manière aléatoire et s'organiser de manière arbitraire. Cependant, la route du nœud source au nœud cible peut impliquer plusieurs sauts sans fil, c'est pourquoi on l'appelle un réseau sans fil à sauts multiples. Par conséquent, si le nœud mobile se trouve dans sa portée de transmission, il peut communiquer directement avec un autre nœud, et le nœud intermédiaire agit comme un routeur (répéteur) pour relayer les messages bond par bond.

[1]Daniel MABELE MONDONGA,étude sur les protocole de routage d'un réseau ad hoc et leur impacts,memoire ,Institut supérieur d'informatique, programmation et analyse de Kinshasa - Ingénieur informaticien, 2010.

Figure I.1: Exemple d'un réseau ad hoc

I.4-Caractéristiques

Les réseaux mobiles ad hoc (sans fil) ont des caractéristiques spécifiques, telles qu'une topologie dynamique, des liens asymétriques, une sécurité limitée et des limitations énergétiques, qui doivent être prises en compte dans la conception de chaque protocole.

Topologie dynamique : La topologie des réseaux de capteurs peut changer au cours du temps pour les raisons suivantes :

- Les nœuds capteurs peuvent être déployés dans des environnements hostiles (champ de batail par exemple), la défaillance d'un nœud capteur est, donc très probable.
- Un nœud capteur peut devenir non opérationnel à cause de l'expiration de son énergie.
- Dans certaines applications, les nœuds capteurs et les stations de base sont mobiles.

Une bande passante limitée : une des caractéristiques primordiales des réseaux basés sur la communication sans fil est l'utilisation d'un médium de communication partagé. Ce partage fait que la bande passante réservée à un hôte soit modeste.

Lien symétrique : Les liens sont symétriques car on a un affaiblissement du signal inversement proportionnel à la distance entre l'émetteur et le récepteur.

Sécurité limitée : La plupart des réseaux sans fil ad hoc n'implémente pas de contrôle d'accès réseau, laissant ces réseaux vulnérables à des attaques de consommation de ressources lors desquelles un nœud malicieux injecte des paquets dans le réseau dans le but de vider de leurs ressources les nœuds relayant les paquets.

Contrainte d'énergie : Cette contrainte est beaucoup plus importante dans les réseaux ad hoc, où les terminaux consomment leur propre énergie en routant des données pour d'autres terminaux. Ainsi, la consommation d'énergie devrait être une question cruciale lors de la conception de nouveaux protocoles de communication et plus spécialement les protocoles de routage ad hoc.

I.5-Mode de communication dans les réseaux ad hoc

Avant de parler des protocoles de routage proprement dit, nous allons rappeler quels sont les principaux modes de communication dans les réseaux, et particulièrement dans les réseaux ad hoc.

- **La communication point à point ou unicast** : Dans ce mode de communication le paquet est adressé à un seul nœud mobile.
- **La communication multi point ou multicast** : contrairement à l'unicast, un paquet est adressé à un ensemble des unités mobiles dans le réseau.
- **La diffusion ou broadcast** : un paquet est adressé à toutes les unités composant le réseau.

La figure I.2 présente les trois modes de communications citées précédemment :

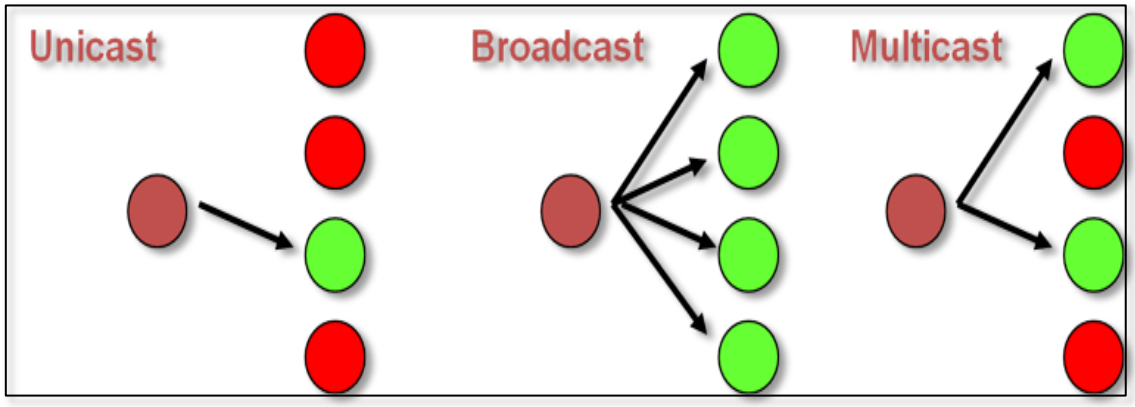

Figure I.2: mode de communication des réseaux ad hoc

I.6-Domaines d'application des réseaux ad hoc

Les applications des réseaux sans fil ad hoc sont nombreuses, nous pouvons citer les applications suivantes :

Jeux vidéo : Cette application permet aux utilisateurs qui souhaitent jouer à des jeux sur le réseau. Il est plus simple et plus fiable de déployer un réseau ad hoc. Le meilleur exemple de ce type d'application est la PSP de Sony.

Application de collaboration : une application spécifique utilisée pour la communication entre collaborateurs (utilisateurs professionnels). Cette application permet aux utilisateurs de conférence et de vidéoconférence d'échanger des informations n'importe où sur le réseau.

Urgences : Le réseau sans fil lors de catastrophes naturelles telles que les tremblements de terre, les tsunamis et les incendies permet aux utilisateurs d'établir rapidement un échange d'informations.

Militaires : les réseaux sans fil sont bien adaptés à ce type d'environnement ou les déplacements restent peu rapides et peu soutenus.

Le réseau en mouvement : le véhicule de communication.

La principale raison de l'utilisation de réseaux ad hoc dans différentes zones est de remplacer l'infrastructure câblée par un réseau dynamique à cet endroit.

I.7-Le routage dans les réseaux ad hoc

I.7.1-Définition du routage

Le routage est une méthode qui permet d'acheminer les informations d'un nœud source vers un nœud de destination via un réseau de connexion donné. Convient aux réseaux à adaptation rapide. En effet, dans le cadre du groupe de recherche MANET de l'IETF (Internet Engineering Task Force), un protocole de routage pour les réseaux ad hoc a été développé. Pour évaluer les performances des protocoles de routage, nous devons effectuer des mesures à la fois qualitatives et quantitatives. Diverses règles et réglementations existantes. Les attributs de qualité idéaux comprennent : le traitement distribué, la liberté de boucle, le traitement basé sur la demande, le traitement actif dans certains cas, la sécurité et le traitement de « période de sommeil ». Cependant, les unités quantitatives requises sont : le flux et le retard de données de bout en bout, le temps d'acquisition de l'itinéraire, le pourcentage de pannes de réception, l'efficacité.

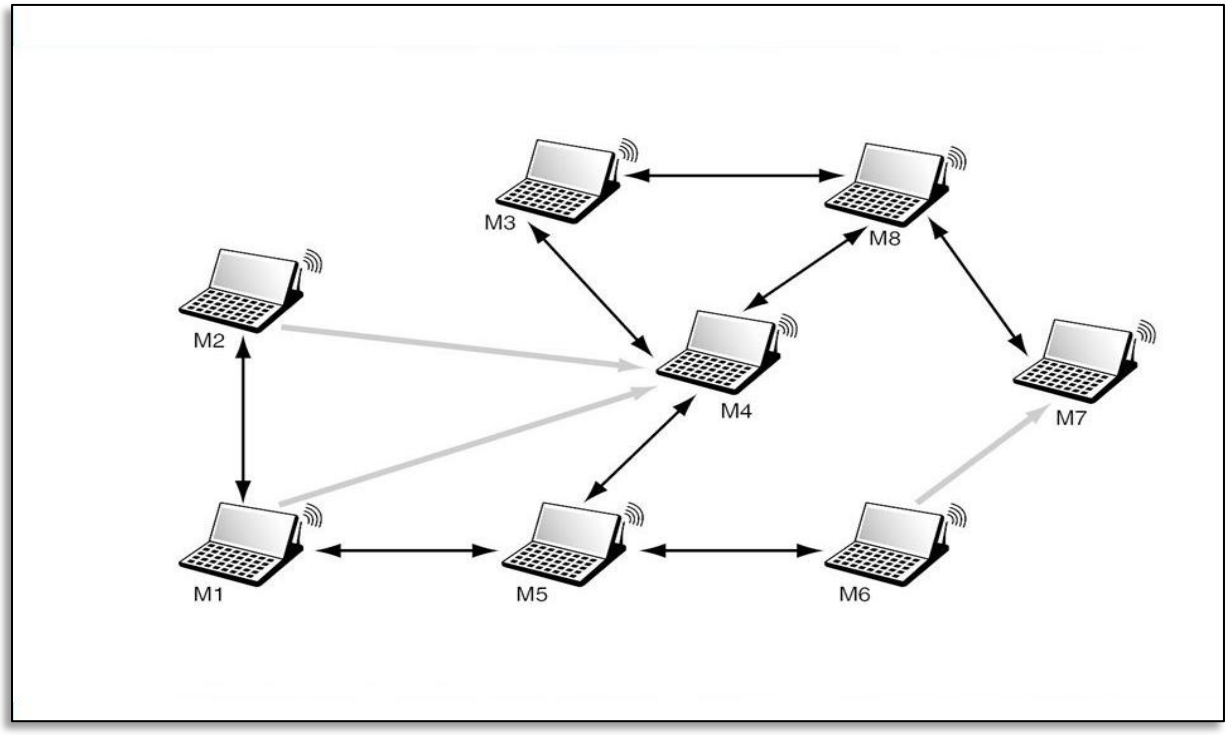

Figure I.3: Le routage dans un réseau Ad hoc

De plus, il faut considérer l'environnement du réseau dans lequel les performances du protocole sont mesurées. Les paramètres de base sont : la taille du réseau, la connectivité du réseau, le taux de changement de topologie, la capacité des liaisons, le taux de liaisons unidirectionnelles, le type de trafic, la mobilité, et le radio et la fréquence des périodes de

sommeil des nœuds. En outre, il semble important que toute conception de protocole de routage prenne en compte les problèmes suivants :

- Minimiser la charge du réseau.
- Offrir un support pour pouvoir effectuer des communications multi-sauts fiables.
- Assurer un routage optimal.
- Offrir une bonne qualité concernant le délai.

Selon la façon de créer et de la maintenir des itinéraires lors de l'acheminement des données, ces protocoles sont divisés en deux catégories :

- Les protocoles proactifs.
- Les protocoles réactifs.

I.7.2-La classification des MANETs

I.7.2.1-Protocoles de routage proactifs

I.7.2.1.1-Le protocole de routage DSDV

Le protocole DSDV (Destination Sequenced Distance Vector) se base sur l'algorithme distribué de Bellman-Ford, qui utilise les vecteurs de distance. Chaque station maintient une table de routage contenant toutes les destinations qu'elle peut atteindre et le cout (en nombre de saut) pour atteindre la destination, ainsi qu'un numéro de séquence lié à chaque destination dont le but est d'éviter la formation de boucle de routage. Cette table est constituée par l'intégration des données de mise à jour émises par chaque station. Ces mises à jour s'effectuent en fonction du temps, ou en fonction d'événements liés à une modification de la topologie du réseau (lien rompu, nouvelle station) Elles se font soit de manière incrémentale (les seules données qui ont changé par rapport à la dernière mise à jour), soit intégralement (la table toute entière), ceci selon l'importance des modifications constatées.

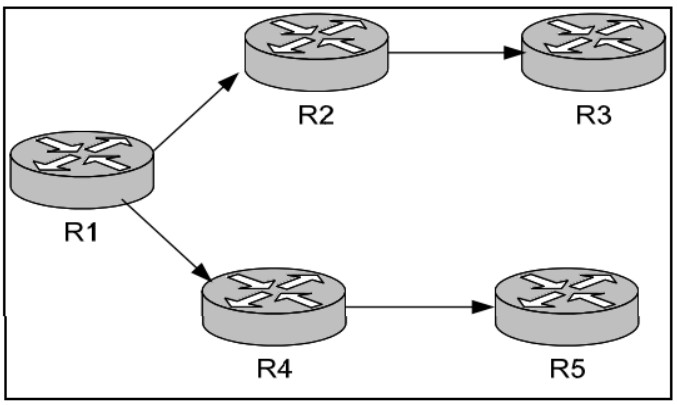

Figure I.4: Exemple de réseau mobile ad hoc.

Destination	Nombre de sauts	Prochain nœud	Numéro de séquence
R1	0	R1	1
R2	1	R2	4
R3	2	R2	5
R4	1	R4	6
R5	1	R5	3

Tableau I.1 : La table de routage du nœud R1

I.7.2.1.2-Le protocole de routage OLSR

Le protocole OSLR (Optimized Link State Routing), développé pour les réseaux MANETs. Il est basé sur la méthode "état de lien "et permet d'échanger des informations sur la topologie du réseau avec les autres nœuds. OSLR utilise le principe du relais multipoints MPR (Multiponts Relays). Tous les nœuds du réseau envoient des messages "HELLO" pour déterminer la nature des liens qui les relient et découvrir l'ensemble de réseau. Ensuite, ces messages « HELLO » transmettent l'état et le type de lien entre l'expéditeur et chaque nœud voisin puis ils spécifient le MPR choisi par l'expéditeur. Ces nœuds particuliers MPR expédient des messages de diffusion pendant le processus d'inondation et produisent les messages d'état de lien[2].

I.7.2.1.3-Le protocole LSR

Dans le protocole LSR (Link State Routing), toutes les stations envois constamment à son voisinage l'état de ses liens. Celles-ci acheminent à leur tour, et de proche en proche, les informations qu'elles reçoivent, jusqu'au moment qu'elles soient connues de toutes les stations. De cette façon, chaque station va pouvoir former ainsi sa propre table de routage, qui va être utilisée lorsque la station souhaitera joindre un destinataire : une simple recherche dans la table va suffire pour trouver le récepteur. Ce protocole illustre parfaitement le concept de routage proactif, et cumule les défauts inhérents à cette technologie (une diffusion parfois excessive des données de routage, et un gaspillage de la bande passante). En faible mobilité, ce protocole fournit de bons résultats, mais qui s'affaiblissent progressivement quand la mobilité des stations augmente[3].

[2] Younes Nadim, Qualité de service des services multimédia sur les réseaux ad hoc sans fil à multi-saut, école supérieure de technologie univ Quebec,2009

[3] Tahar Abbes Mounir, proposition d'un protocole à économie d'énergie dans un réseau hybride GSM et ad hoc, univ Oran,2011/2012

I.7.2.1.4-Le protocole WRP

Le protocole WRP (Wireless Routing Protocol), est un protocole de routage à vecteur de distance. Les vecteurs de distance sont, uniquement, émis lorsque des changements sur la topologie du réseau surviennent. Ces mises à jour doivent être acquittées par la totalité des nœuds voisins (détectant ainsi une perte éventuelle). Pour détecter ces changements, les nœuds transmettent périodiquement des paquets pour se faire connaitre dans leur voisinage[4].

I.7.2.1.5-Le protocole STAR

Le protocole STAR (Source-Tree Adaptative Routing) est basé sur le principe des protocoles à état de liens. Chaque nœud met à jour un arbre qui contient l'ensemble des routes favorites pour joindre les destinations. Ce protocole réduit les messages de contrôles échangés en éliminant les mises à jour périodiques du protocole à état de liens. L'envoie de son arbre n'est pas fait périodiquement, il est réalisé uniquement lors de changements majeurs sur le réseau (détection d'une nouvelle destination, rupture d'un lien…). Cette approche évite les mises à jour périodiques. Ce protocole est performant lors du passage à de vastes réseaux car il maitrise le nombre de messages de contrôles transmis[5].

I.7.2.2-Protocoles de routage réactifs

Les protocoles de routage réactifs créent et maintiennent les routes selon les besoins. Lorsqu'une route est demandée, une procédure de découverte globale est lancée par la source afin de trouver le meilleur chemin. Exemples des protocoles réactifs : DSR (Dynamic Source Routing), AODV (Ad hoc On-Demand Distance Victor Routing), etc.

I.7.2.2.1-Le protocole de routage DSR

Le protocole DSR (Dynamic Source Routing) est basé sur la technique de routage par la source. La source des données détermine la séquence complète des nœuds intermédiaires par lesquels les informations vont transiter. Quand un nœud veut envoyer des données, il diffuse un paquet requête « route request » qui contient un champ permettant d'enregistrer tous les nœuds qu'il va visiter jusqu'à l'atteinte de la destination. En cas de découverte d'une route, la source reçoit un paquet réponse de la route « route reply » qui contient la séquence des nœuds traversés. Ensuite, la source insère la séquence des nœuds de la route reconnue

[4] Tahar Abbes Mounir,op.cit,p10
[5] Tahar Abbes Mounir,op.cit,10

dans l'entête de tous les paquets qu'il désire transmettre. Dans ce cas, les nœuds intermédiaires jouent un rôle de simple relayeur d'information. À la réception d'un paquet, chaque nœud supprime son adresse de la séquence des nœuds contenue dans l'entête, puis l'achemine au nœud suivant dans la séquence.

Le protocole DSR exécute une procédure de maintenance de routes afin d'assurer la validité des chemins utilisés. Un message erreur de route « route error » est envoyé à l'émetteur original du paquet, lors de la détection d'un problème majeur. Ce message contient l'adresse du nœud qui a détecté l'erreur et celle du nœud suivant dans le chemin. Lorsque le nœud source reçoit ce message d'erreur, le nœud concerné par l'erreur est supprimé du chemin sauvegardé, et tous les chemins contenant ce nœud sont coupés à ce point-là. Ensuite, l'émetteur initie une nouvelle opération de découverte de routes vers la destination.

Les paquets de données contiennent toutes les décisions de routage ce qui résulte que les nœuds intermédiaires n'aient pas besoin de maintenir les informations de mise à jour pour envoyer les paquets de données. Dans ce protocole il n'y a pas de boucle de routage, parce que la route entre la source et la destination est une partie des paquets de données envoyés.

I.7.2.2.2-Le protocole de routage AODV

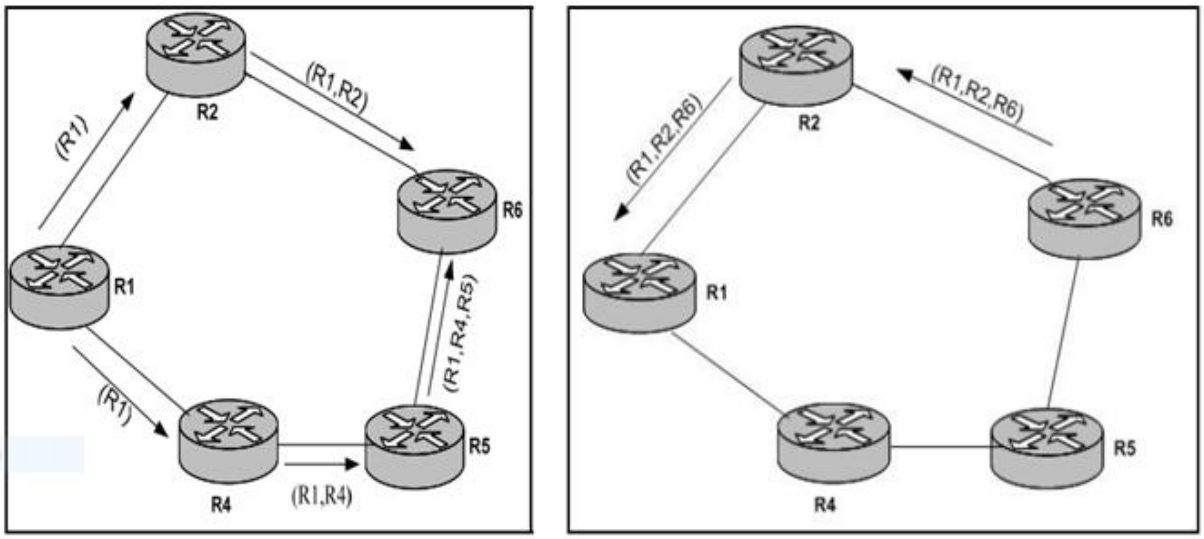

Figure I.5: La détermination d'une route selon DSR. (Figure à gauche)

Le renvoi du chemin calculé (figure à droite).

Le protocole AODV (Ad-hoc On-Demand Vector Distance) représente une amélioration de l'algorithme DSDV et il peut être aussi vu comme un hybride des protocoles DSDV et DSR. Il est prévu pour être utilisé par les réseaux Ad-hoc mobiles. L'amélioration

par rapport au DSDV réside dans le fait que, le protocole AODV permet de mettre à jour la table de routage d'un nœud sans que celui-ci ait à communiquer avec tous ses voisins ce qui diminue considérablement le nombre de paquets diffusés dans le réseau. L'AODV utilise le principe des numéros de séquence pour maintenir la consistance des informations de routage. Comme dans le DSR, l'AODV utilise le principe d'inondation pour trouver une route vers une certaine destination en envoyant un paquet RREQ « route request ».

Cependant, contrairement au DSDV, chaque nœud recevant ce paquet prépare une entrée dans sa table de routage afin de pouvoir rédiger plus tard les paquets qu'ils recevront. Le paquet RREQ contient dans le champ « numéro de séquence destination » le dernier numéro de séquence associé à la destination. Ce numéro est recopié de la table de routage. Si ce numéro n'est pas connu, la valeur nulle ne sera prise par défaut. Afin de maintenir des routes consistantes, une transmission périodique du message "HELLO" est effectuée. Un lien est considéré défaillant, si trois messages "HELLO" ne sont pas reçus consécutivement à partir d'un nœud voisin.

Le protocole AODV ne présente pas de boucle de routage et évite le problème "counting to infinity" de Bellman-Ford, ce qui offre une convergence rapide quand la topologie du réseau Ad hoc varie.

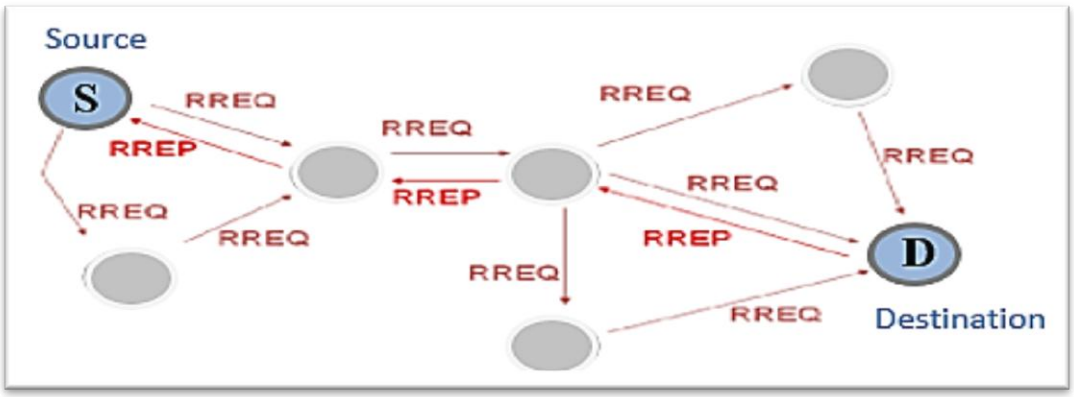

Figure I.6 : Exemple de protocole AODV.

I.7.2.3-Les protocoles hybrides

Dans cette catégorie on combine entre les deux premiers types de protocoles de routage pour acquérir un temps de réponse plus court en impliquant les avantages des protocoles proactifs et réactifs. Dans le protocole hybride, le réseau est décomposé en petites zones ou le routage à l'intérieur de chaque zone est assuré par le protocole proactif, alors que

le routage entre les différentes zones est à base du protocole réactif. Les protocoles ZRP et ZHLS sont parmi les protocoles hybrides les plus connus[6].

I.7.2.3.1-Le protocole ZRP

ZRP (ZONE Routing Protocol) est un protocole de routage hybride ou le réseau est décomposé en plusieurs zones de routages chevauchées. La zone de routage d'un nœud est définie comme l'ensemble des nœuds qui se trouvent à une distance inférieure ou égale au rayon de la zone. Les nœuds qui se trouvent exactement à une distance égale au rayon de la zone sont appelés "nœuds périphériques". Le routage interzone peut être assuré par n'importe quel protocole de routage proactif, à condition qu'il soit modifié pour que la portée des mises à jour soit restreinte au rayon de la zone de routage. Le routage interzone est assuré par un cycle RREQs-RREPs. Quand un nœud reçoit un paquet RREQ s'il n'est pas destination et si encore la destination ne se situe pas dans sa zone, il renvoie le RREQ uniquement vers les nœuds périphériques. Cela limite considérablement le nombre des RREQs propagés au réseau. Les performances de ZRP dépendent de la valeur choisie pour le rayon des zones. Pour des grandes valeurs, le ZRP se comporte comme un protocole de routage purement proactif tandis que pour des petites valeurs, il se comporte comme un protocole de routage purement réactif[7].

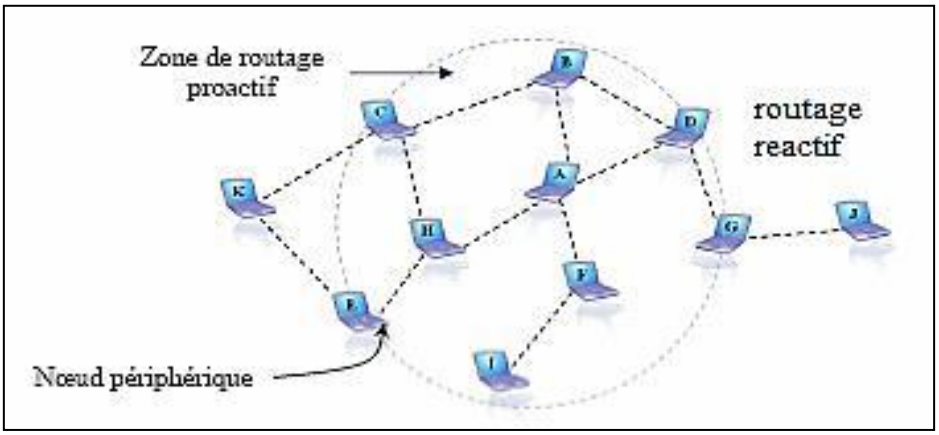

Figure I.7: Exemple de protocole ZRP.

I.7.3-La puissance

La distance maximale de communication entre deux nœuds de WLAN est une fonction de trois paramètres : la puissance de transmission de l'émetteur, le modèle de propagation de

[6] Mirar Youcef, Djettou Brahim Khalil, étude des réseaux ad hoc par la théorie des jeux, univ akliMouhand Oulhadj-Bouira, 2018/2019
[7] idem

perte de route "path-loss", et le seuil de la puissance de réception (sensibilité du récepteur) du nœud de réception. La norme IEEE 802.11 limite la distance entre les nœuds de WLAN à 300 mètres.

Par conséquent, les réseaux de WLAN qui se prolongent au-delà de 300 mètres pourraient encourir une dégradation de performance dans l'algorithme de MAC de WLAN (OPNET documentation).

Afin de créer des problèmes dans le réseau de simulation, nous avons la destination de la source et nous avons diminué la puissance des stations pour affaiblir le signal entre la source et la destination et produire des situations d'erreurs dans le réseau pour bien montrer l'effet de FEC[8].

I.8-Comparaison entre les différentes catégories de protocoles de routage

Protocole	Les avantages	Les inconvénients
Proactif Recherche périodique des routes	-Pas de temps de réaction, rapidité d'établissement des routes. -Adaptés aux réseaux denses de taille moyenne. -Adaptés aux réseaux à forte mobilité	-Trafic de contrôle important -Capacité d'échange du réseau limitée - Consommation énergétique importante.
Réactif Routes obtenues à la demande	- Trafic de contrôle faible -Adaptés aux grands réseaux. -Consommation énergétique réduite -Optimisation de la bande passante.	-Temps long de réaction, - Délai nécessaire pour trouver une route -Pas optimisé pour la forte mobilité des nœuds.
Hybride Combinaison (proactif -réactif)	-Adaptables aux réseaux -Consommation énergétique réduite.	-Recherche des routes complexes -Temps de réaction long -Ressources CPU et mémoire.

Tableau I.2: Comparaison entre les différentes catégories du protocole de routage.

[8] Younes Nadim, Qualité de service des services multimédia sur les réseaux ad hoc sans fil à multi-saut, école supérieure de technologie univ Quebec,2009

I.9-Les avantages des réseaux Ad hoc

- La mobilité des nœuds : la mobilité continue des nœuds crée un changement dynamique de topologie. Par exemple, un nœud peut joindre un réseau, changer de position ou quitter le réseau. Ce déplacement a naturellement un impact sur la morphologie du réseau et peut modifier le comportement du canal de communication.
- Un cout fiable : aucune infrastructure n'est à mettre en place initialement et surtout aucun entretien n'est à prévoir.
- L'indépendance technique et commerciale, vis-à-vis de point d'accès.
- La rapidité de mise en place.
- La robustesse : un réseau évolutif et dynamique.
- Les réseaux ad hoc peuvent être déployés dans un environnement quelconque.
- La tolérance aux pannes : la rupture d'un lien dans le réseau Ad hoc est réparée par les autres nœuds en cherchant des nouvelles routes pour atteindre la destination.
- La taille des réseaux ad hoc : elle est souvent de petite ou moyenne taille ; le réseau est utilisé pour étendre temporairement un réseau filaire, comme pour une conférence ou des situations où le déploiement du réseau fixe n'est pas approprié (ex : catastrophes naturelles). Cependant, quelques applications des réseaux ad hoc nécessitent une utilisation d'un plus grand nombre de nœuds, comme dans les réseaux de capteurs [9]. Des problèmes liés au passage à l'échelle tels que : l'adressage, le routage, la gestion de la localisation des capteurs et la configuration du réseau, la sécurité, etc, doivent être résolus pour une meilleure gestion du réseau.

I.10- Les inconvénients des réseaux Ad hoc

Il existe beaucoup de problèmes techniques dans les réseaux Ad hoc

I.10.1-Problèmes de transmission radio

- Augmentation de nombre d'erreurs sur la transmission.
- Diminution de débit de la liaison.
- La redondance.
- Amoindrissement des performances du lien radio.

I.10.2-La mobilité des nœuds :

Modification de la topologie de réseau dû à la densité des nœuds.

Transformation du tracé des routes lors des échanges des paquets.

I.10.3-Consommation d'énergie :

La durée de vie d'un équipement dépend de la durée de vie, la batterie, pour cela la consommation d'énergie doit obligatoirement diminuée.

I.10.4-Les problèmes liés au routage :

Le problème de routage est l'un des problèmes majeurs dans les réseaux Ad hoc, il se pose sur l'adaptation de la méthode d'acheminement utilisée avec le grand nombre de calcul, de sauvegarde et changements rapides de topologies.

I.10.5-Problème de sécurité :

La sécurité dans les réseaux Ad hoc constitue l'une des préoccupations durant la planification, la mise en place ainsi la gestion du réseau.

Cette dernière dépend de plusieurs paramètres tel que : authentification, confidentialité, intégrité et disponibilité. Elle concerne deux points, la sécurité des données transitant sur le réseau est limitée étant donné que le média de transmission est partagé par tous les nœuds de réseau et aussi la sécurité de routage. Ces deux aspects comportent quelques vulnérabilités et sont exposés à plusieurs attaques.

I.11-Conclusion

Dans ce chapitre, nous avons présenté le réseau mobile Ad hoc qui occupe d'un jour à l'autre, une place plus importante en termes de recherche, revenus. Ces réseaux mobiles Ad-hoc (ou MANET pour Mobile Ad hoc Networks) sont des réseaux sans fil mobiles indépendants de toute infrastructure fixe. Vu la nature du média de transport, ces réseaux héritent des avantages et des inconvénients de leur homologue qui se rattache à des infrastructures filaires, auxquels se rajoutent des nouveaux avantages et inconvénients.

Chapitre II :

La couche MAC IEEE 802.11

II.1-Introduction :

De manière générale, un équipement réseau comporte sept couches, qui vont de la couche physique à la couche application. Dans notre cas, plusieurs couches ne sont pas prises en compte comme par exemple la couche réseau (3eme couche) qui sert au routage entre les réseaux car nous situons toujours dans un seul réseau de communication. Le modèle sera donc réduit en une seule couche : couche Mac.

Couche Mac : cette couche fournit les moyens fonctionnels et procéduraux pour le transfert de données entre les nœuds adjacents d'un réseau. Pour Wifi, deux technologies majeurs existent dans cette couche : IEEE 802.11 et IEEE 802.11e.

La couche Mac est réalisée par un circuit électronique spécifique. Ce circuit porte plusieurs noms, par exemple : coupleur de communication, interface réseau, carte E/S réseau ou carte réseau sans fil. En conclusion, dans un SDCR (Software Defined Cognitive Radio) sans fil, chaque équipement qui envoie des informations à travers le réseau doit être équipé de ce type de carte. Nous allons à travers ce chapitre détailler la couche MAC IEEE 802.11 et ces caractéristiques, les différents modes d'accès, par la suite on présente la qualité du service, la problématique et la solution proposé et enfin le protocole de sécurité dans ces réseaux.

II.2-Définition du Wifi :

Le nom Wi-Fi ou Wireless Fidélité correspond initialement au nom donné à la certification délivrée par WECA qui est l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11.

Le principe consiste à établir des liaisons radio rapides entre des terminaux et des bornes reliées aux réseaux Haut Débit. Grâce à ces bornes Wi-Fi, l'utilisateur se connecte à Internet ou au système d'informations de son entreprise et accède à de nombreuses applications reposant sur le transfert de données[9].

II.3-Définition du standard IEEE 802.11 :

La norme IEEE 802.11 appelée aussi WI-FI, réfère à une famille de spécifications développée pour les réseaux locaux sans fil. Le protocole IEEE 802.11 peut opérer selon deux configurations du réseau sans fil local : réseau avec ou sans infrastructure. Dans la première

[9] Ratsimbazafimanana Manoela, étude des performances des réseaux wifi avec des simulations sur Opnet, univ d'Antananarivo école supérieure polytechnique,2015/2016

configuration, au niveau de chaque cellule, un contrôleur centralisé est utilisé. Il s'agit également d'un point d'accès (AP). Ce dernier est connecté au réseau filaire et peut ainsi fournir aux stations mobiles l'accès au réseau internet entre autres. Les stations mobiles peuvent en l'occurrence changer de point d'accès lors de leurs déplacements, ceci s'appelle le « handover ». Dans la seconde configuration, il s'agit d'un réseau, pair à pair, constitué de stations qui s'écoutent directement et s'auto configurent pour un réseau temporaire.

Aujourd'hui le standard IEEE 802.11 est principalement utilisé dans les réseaux ad hoc pour le support de communications sans fil. Les améliorations apportées au premier standard depuis sa normalisation forment l'ensemble des normes IEEE802.11.

- **IEEE 802.11a** : Ce standard a été normalisé en 1999. Il applique une technique de multiplexage en fréquence appelé OFDM pour transférer les données avec un taux de transfert maximal 54 Mbit/s sur une bande de fréquence de 5.25 à 5.35 GHz (bande U-NII). Les dispositifs 802.11a ne sont pas compatibles avec les autres technologies 802.11 puisqu'ils opèrent dans une partie différente du spectre radioélectrique et utilisent des techniques de modulation différentes[10].
- **IEEE 802.11b** : C'est la version la plus connue et la plus utilisée des standards IEEE 802.11. Elle opère sur la bande de fréquence 2.4 GHz (bande ISM) avec un débit de 11 Mbit/s. Elle utilise CSMA/CA comme méthode d'accès au canal pour éviter les collisions et la technique d'étalement de spectre par séquence directe DSSS au niveau de la couche physique. Les produits conforment à ce standard sont nommés "WiFi" (Wireless Fidelity). L'application du protocole de sécurité WEP (Wired equivalent Privacy) a commencé avec ce standard afin d'apporter un niveau de sécurité équivalent au réseau filaire[11].
- **IEEE 802.11g** : Paru en 2003, ce standard est une amélioration du standard IEEE 802.11a en le transposant de la bande U-NII à la bande ISM. Il est donc compatible à la norme IEEE 802.11b avec un débit maximal de 54 Mbit/s. Le protocole WEP est appliqué aussi pour sécuriser les données[12].
- **IEEE 802.11i** : Il implique de nombreux changements, y compris l'ajout de l'algorithme AES pour chiffrer l'information. Il introduit le protocole WPA (Wi-Fi

[10] Ghada zaibi, sécurisation par dynamiques chaotiques des réseaux locaux sans fil au niveau de la couche mac, école nationale d'ingénieurs de Sfax-Tunisie, 6/12/2012
[11] Ghada zaibi, op.cit, p07
[12] Idem

Protected Access) puis WPA2 pour remplacer WEP qui est devenu obsolète en raison de ses faiblesses[13].

- **IEEE 802.11e** cherche à améliorer 802.11 de façon à pouvoir donner des garanties de qualité de service. Cette extension de la norme n'est pas encore finalisée. Ainsi, cette norme a pour but de définir les besoins des différents paquets en termes de bande passante et de délais de transmission de telle manière à permettre notamment une meilleure transmission de la voix et vidéo[14].
- **IEEE 802.11h** cherche à mieux gérer la puissance d'émission et la sélection des canaux dans la bande des 5 GHz suivant si l'on est à l'intérieur ou à l'extérieur de bâtiments. L'objectif est d'être, à terme, mieux en accord avec les diverses l´législations (notamment européennes).
- **IEEE 802.11p :** en 2003, le groupe de travail IEEE a défini un nouveau standard dédié aux communications inter-véhicules, nommé WAVE (Wireless Ability in Vehicular Environnements) et aussi connu sous le nom 21 de IEEE 802.11p. Cette norme utilise le concept de multicanaux afin d'assurer les communications pour les applications de sécurité et les autres services du transport intelligent. Elle est capable d'offrir un débit entre 6 et 27 Mbps, de plus sa couche MAC reprend le principe de CSMA/CA pour gérer la qualité de service et le support du protocole de marquage de priorité.

II.4-Caractéristiques :

Le débit : dans le Wifi, le débit maximal fourni peut atteindre 54 Mbit/s selon la couche physique utilisée (les différentes possibilités 802.11a, b, g seront présentées au paragraphe 1.5). Le débit important (par rapport aux technologies précédentes) du Wifi est un atout pour transmettre les données des applications multimédia ou temps réel, qui demandent un haut niveau de qualité de service même si cela n'est pas suffisant, en particulier en cas de gigue ou de latence.

La portée : Dans le milieu industriel, les machines peuvent être éloignées l'une de l'autre. Donc la transmission des données depuis l'émetteur vers le récepteur peut passer une distance considérable. Pour cela, la portée peut être une contrainte essentielle de la technologie choisie. Les portées des technologies sans fil dépendent de la puissance d'émission. Plus la puissance

[13] Idem
[14]Ratsimbazafimanana Manoela, op.cit, p11

est grande, plus la distance entre la source et le destinataire est potentiellement grande. Or dans le Wifi, la puissance maximale autorisée est plus grande que dans d'autres types de technologie, ce qui favorise une portée plus importante. Pour le Wifi, la transmission peut atteindre une distance de 500 mètres. Les autres technologies ont une portée de 100m mais avec une consommation d'énergie plus conséquente, c'est le cas du Bluetooth.

Populaire : Wifi est devenu une technologie publique par rapport à d'autres technologies sans fil. Les Hotspot sont populaires dans tous les cafés, hôtels, Presque tous les PC portables sont équipés de cartes Wifi. La demande pour cette technologie motive les chercheurs à développer des travaux autour de ce standard. De plus, Cette demande les encourage à améliorer cette technologie pour qu'elle s'adapte à tous les milieux où elle se trouve et aux types de données transmises. Plusieurs améliorations sont standardisées : exemple le 802.11e, qui est le 802.11 avec priorité entre les flux.

Coût : l'augmentation de la demande, pousse la fabrication des équipements qui implémentent cette technologie. Cette augmentation diminue donc le coût de fabrication de ces équipements.

Disponibilité : basse disponibilité de largeur de bande avec un débit de transmission très bas typiquement une vitesse très lente que celle des réseaux filaires, causant la dégradation de qualité de service.

II.5-Etude de la norme 802.11 :

L'évolution au niveau de la couche physique en termes de débit montre clairement les grandes avancées qui ont été faites afin de répondre aux besoins des applications multimédia.

802.11 est une norme établie par l'IEEE. Elle décrit les couches physiques et MAC d'interfaces réseau radio et infra-rouge.

Couche Physique : c'est la première couche dans le modèle OSI. Elle est chargée de la transmission effective des signaux. Son service est typiquement limité à l'émission et la réception d'un bit ou d'un train de bits continu. Cette couche est chargée donc de la conversion entre bits et signaux électriques ou optiques.

Couche MAC : Cette couche fournit les moyens fonctionnels et procéduraux pour le transfert de données entre les nœuds adjacents d'un réseau. Pour Wifi, deux technologies majeures existent dans cette couche : IEEE 802.11 et 802.11e.

II.6-IEEE 802.11: Couche MAC

La couche liaison, dans la norme IEEE 802.11, est constituée de deux sous-couches : LLC (Logical Link Control) et MAC (Medium Access Control).

La première sous-couche consiste à délimiter les trames et à corriger d'éventuelles erreurs survenues lors de la transmission physique.

Le rôle de la deuxième sous-couche est de gérer le partage du support physique entre plusieurs stations en mettant en œuvre des mécanismes d'accès au canal. Pour atteindre cet objectif, le standard IEEE 802.11 définit un protocole d'échange des trames. La séquence minimale d'échange contient deux trames : une trame de données envoyée de la source à la destination et une trame d'acquittement (ACKnowledgment ou ACK) envoyée de la destination à la source une fois que la trame de données est reçue avec succès. Chaque trame émise contient une Frame Check Sequence (FCS : 32bit CRC) qui est vérifiée par le destinataire lors de sa réception. Si la FCS correspond au contenu attendu, le destinataire envoie un ACK, le cas échéant cet ACK n'est pas envoyé. Si la source n'a pas reçu l'ACK attendu, la trame est retransmise de nouveau. Ce mécanisme permet de pallier les problèmes d'erreurs causées par des interférences sur le canal radio. Cela garantit l'intégrité des données au niveau de la couche liaison.

II.6.1-Mode d'accès d'IEEE 802.11 :

IEEE 802.11 propose deux modes d'accès au canal : Distributed Coordination Function (DCF) et Point Coordination Function (PCF).

II.6.1.1-Distributed Coordination Fonction (DCF) :

Cette transmission s'effectue en mode asynchrone c'est-à-dire les stations tentent d'envoyer des données sans être gérées par un contrôleur, Elle est conçue pour permettre aux utilisateurs d'avoir chance égale d'accéder au support. Elle permet de réduire les collisions sans pouvoir les éliminer totalement. Cette méthode s'appuie sur le protocole CSMA/CA combiné à l'algorithme de back-off. Lorsqu'une station souhaite émettre une trame de données, elle écoute le canal durant un intervalle de temps appelé DIFS. Si celui-ci est inactif durant cette période, la station transmet immédiatement sa trame. Dans le cas contraire, le canal est occupé, la station doit attendre jusqu'à ce que le canal soit inactif durant une période

SIFS.À la fin de cette période, la station entre dans la procédure du Back-off qui l'oblige à calculer un Back-off Time durant lequel elle s'abstient de transmettre.

La station réceptrice vérifie le CRC de la trame reçue et envoie une trame d'acquittement à l'émetteur après un SIFS. Ce dernier est utilisé pour séparer les trames d'un dialogue. La réception de l'acquittement informe l'émetteur du succès de la transmission. Lorsque le PCF est utilisé, le coordinateur central a la priorité d'accéder au canal. Pour cela, il utilise l'intervalle PIFS qui est plus court que le DIFS. Une fois que le canal saisit, le coordinateur central instaure le PCF.

II.6.2-Point Coordination Function (PCF) :

Cette méthode sans contention ne permet pas de gérer les collisions. Au début de la période sans contention, le point coordinateur PC transmet des balises Beacons qui contiennent la durée maximale CFPMaxDuration de la période d'accès sans contention. Ensuite, il commence à interroger les stations associées en envoyant des trames CF-Poll afin de savoir si elles possèdent des données à transmettre. Le CF-Poll peut être accompagné d'une trame de données si le PC a des données à transmettre pour une station. La station qui est destinataire du CF-Poll envoie sa trame en intégrant un acquittement CF-ACK qui acquitte le CF-Poll après un temps d'attente SIFS.

Enfin, le PC acquitte la trame envoyée par la station après un intervalle SIFS. Cet acquittement est généralement accompagné par un CF-Poll pour interroger une autre station. Dans le cas où une station interrogée ne répond pas au bout d'un temps PIFS (elle n'a pas de données à transmettre), le PC reprend l'interrogation des stations qui restent.

II.7-Le protocole CSMA/CA :

L'objectif du CSMA est d'éviter les collisions. Il part du principe que les nœuds transmettent seulement lorsque le canal est libre, fait l'écoute du canal pour la détection des porteuses, le fonctionnement du CSMA peut être expliqué de la manière suivante [12] : Un nœud qui veut transmettre dans un canal, écoute d'abord le canal.

- Si le canal est libre, il transmet.
- Sinon, il attend pendant un temps spécifique**.**

– Si le transmetteur n'a pas reçu l'information après un moment donné, il suppose qu'il y a une collision.

Après la collision, le nœud attend pendant une période aléatoire, puis il retransmet.

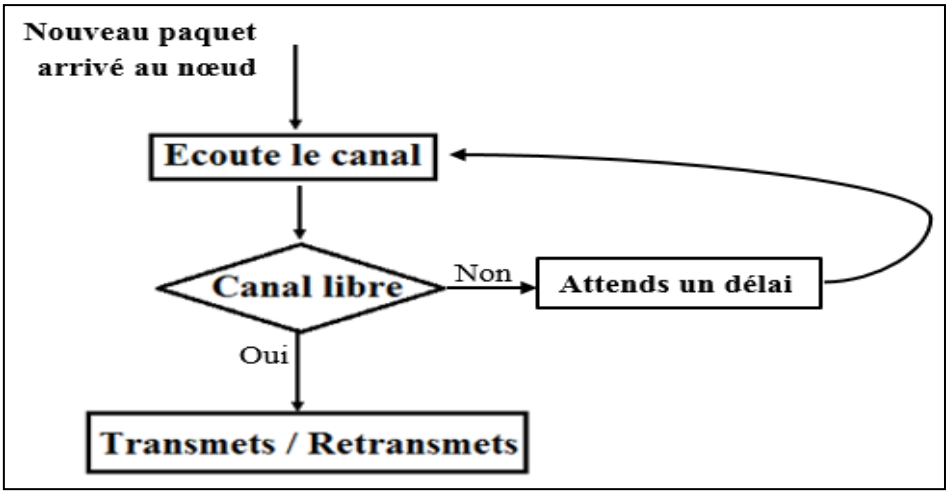

Figure II 1: La méthode CSMA/CA

Le principe général de la méthode CSMA/CA est : chaque station, après que le médium devient libre, attend une durée fixe DIFS suivie de processus de Backoff qui permet de gérer les collisions et garantir la même probabilité d'accès pour chaque station au support.

Le processus de Backoff (Backoff process) consiste, dans un premier temps, à calculer un nombre aléatoire (ce qui empêche les stations multiples de saisir le médium en même temps) compris entre zéro et CW (Contention Windows, fenêtre de contention). Ce nombre est ensuite multiplié avec une durée appelée slot time. Le résultat de la multiplication permet à la station d'initier un Backoff dont la valeur est donnée par la formule :

Backoff time= Random (0, CW) x SlotTime

Ou Random (0,CW) est une valeur aléatoire entière uniformément distribué sur [0,CW] avec CW (Contention Windows) la fenêtre de contention vérifiant CWmin CW CWmax =1023.

Initialement on a : CW=CWmin=15 dans 802.11. SlotTime est une durée fixe (9us dans 802.11a).

Les stations par la suite décrémentent leurs backoff time. Dès que le backoff time de l'une d'elles atteint zéro (Source 1 dans notre exemple), elle émet. Les autres stations, dés quelles

détectent le regain d'activité sur le canal stoppent la décrémentation de leurs Backoff time et entrent en période de defering.

Un paquet de donnée est séparé de son acquittement par un SIFS qui est plus court que le DIFS. Les stations en période de defering ne pourront reprendre la décrémentation de leurs backoff time que si le canal est à nouveau libre pendant DIFS. Le fait que SIFS soit plus court empêche que la décrémentation ne reprenne de manière inopportune entre les données et leur acquittement.

Lorsque les données de la Station 1 ont été acquittées et que DIFS s'est écoulé sans activité sur le canal, les autres stations peuvent reprendre la décrémentation de leur Backoff time.

La figure ci-dessous montre le principe de backoff et de defering, l'envoi et l'acquittement d'une trame :

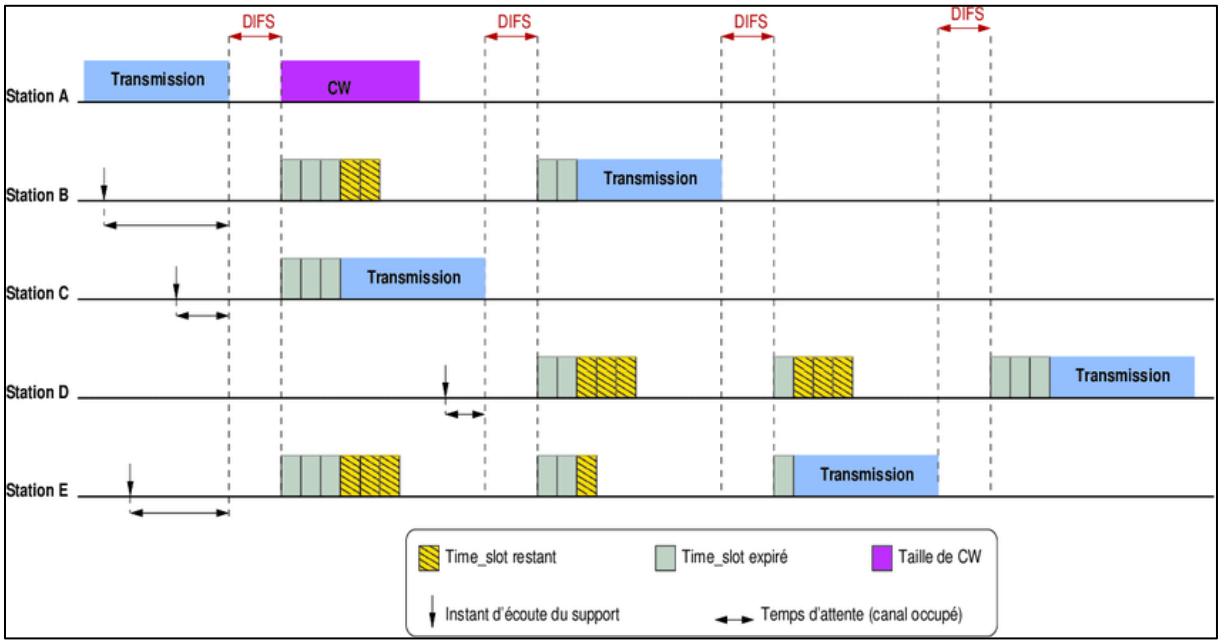

Figure II 2: Algorithme de Backoff

Chaque trame doit être acquittée par la station de destination. Lorsqu'une trame n'est pas acquittée, la station retransmet la trame après avoir attendu DIFS et un processus de Backoff.

La probabilité d'avoir des collisions sur le canal dépend de la dimension de la fenêtre de contention CW. Plus la fenêtre est grande, plus la probabilité que les temps d'attente de deux stations soient identiques est faible. Cependant une fenêtre de contention trop importante nuit aux performances car les temps d'attente sont plus longs. La solution consiste à contrôler

dynamiquement la dimension de la fenêtre de contention. CW est donc recalculé en fonction du nombre de collisions détectées sur le canal. A chaque collision détectée, la formule est la suivante :

CW i=2CWi-1+1 (15,31,63,127,255,511,1023)

II.7.1-L'algorithme de Backoff

La procédure de Backoff est un mécanisme simple, basé sur le calcul d'un temporisateur gérant les transmissions et les retransmissions. Il permet de réduire la probabilité de collision sur le canal en essayant de minimiser les chances d'avoir plusieurs stations qui accèdent au support en même temps.

II.7.1.1-Déroulement :

Une station S désirant envoyer des données attend pendant une période DIFS. Si après cette durée le canal est libre, la station accède directement au canal. Dans le cas contraire, la station déclenche le mécanisme de Backoff qui se déroule en 3 étapes :

La station calcule son temporisateur Backoff_Timer :

Avec Backoff_Timer _Random () x TS

Random () : nombre pseudo-aléatoire choisi ente 0 et CW-1 ; où CW est la taille de la fenêtre de contention qui sera détaillée plus loin. TS : durée d'un time-slot définie comme étant l'intervalle de temps nécessaire pour une station pour savoir si une autre a accédé au canal au début du time-slot précédant.

- Quand le canal devient libre, et après un DIFS, la station commence à décrémenter son temporisateur time-slot par time-slot.
- Lorsque la valeur de Backoff_Timer est égale à 0, la station peut alors envoyer. Si par contre au cours de la phase de décrémentation, une autre station S'termine de décrémenter son temporisateur, la station S bloque son temporisateur. Elle pourra continuer de le décrémenter une fois la transmission de la station S finie.

II.7.2-Problème de stations exposés/stations cachés

Un réseau Ad hoc commence par au moins deux nœuds annonçant leur présence avec leur information d'adresses respectives, une communication est établie entre les deux nœuds

par l'échange de messages de commandes appropriées suivant les mises à jour de leur table de routage.

La connexion entre ces nœuds peut être encore changée pour plusieurs raisons. Par exemple, un nœud peut trainer trop loin hors de la portée de transmission, sa batterie peut être épuisée, ou il peut être susceptible au mal fonctionnement de logiciel ou bien de matériel.

II.7.3- Problème des stations cachés

Ce problème est dû lorsque deux nœuds cachés l'un de l'autre (hors de la portée de la transmission) essaient de transmettre de l'information au même nœud de réception, par conséquent une collision de données se produit à la réception.

L'état d'un nœud est défini par la transmission en cours. Classiquement, l'émetteur est dans un état d'émission. Le récepteur se trouve dans un état de réception. Un nœud est récepteur qu'il soit le destinataire de la communication ou non. Cela signifie qu'il reçoit une transmission et que donc, le canal est occupé. Autrement, le nœud est dans un état inoccupé et aucune communication n'existe.

Pour éviter la collision, tous les nœuds voisins au récepteur doivent être informés que le canal est occupé.

II.7.4-Problème des stations exposées

La transmission des données des nœuds voisins peut empêcher un nœud de transmettre aux autres nœuds. Il s'agit donc du problème des nœuds exposés. Un nœud exposé est un nœud dans la portée de transmission de l'émetteur mais hors de la portée du récepteur.

Par exemple, on a quatre stations A, B, C, D C transmet un message à D, et B peut entendre C et B n'as aucun moyen de savoir que la transmission qu'elle veut faire avec la station A ne vas pas causer une collision, alors B ne vas pas transmettre à A par crainte de causer une collision à C, donc B est exposée à C.

La solution du problème de nœud exposé est l'utilisation des canaux de contrôle et de données de façon séparée ou l'utilisation des antennes directionnels.

II.8-Fenêtre de contention :

La taille de la fenêtre de contention CW a pour valeur initiale CWmin. Deux cas de figures peuvent se présenter :

- **Transmission réussie :** dans ce cas, CW est réinitialisée à CWmin.
- **Transmission échouée :** c'est-à-dire que la station émettrice ne reçoit pas d'acquittement au bout d'un certain temps. CW est alors incrémenté de la façon suivante :

CWnew _ 2*CWold +1

La station suppose dans ce cas qu'il y a eu collision lors de la transmission, et incrémente la taille de sa fenêtre de contention afin de diminuer les chances de collisions lors des prochaines retransmissions. Une valeur limite CWmax est cependant définie. Si pour CW = CWmax la transmission échoue toujours, la valeur n'est plus incrémentée et est maintenue à CWmax.

II.9-Qualité de service IEEE 802.11

II.9.1-Notion de qualité de service

II.9.1.1-Définition de la QoS

Plusieurs définitions ont été proposées pour le terme de la qualité de service dont les plus importantes sont :

La Qualité de Service (QoS) est la capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de disponibilité, débit, délais de transmission, taux de perte de paquets[15]…

Appliquée aux réseaux à communication de paquets (réseaux basés sur l'utilisation de routeurs) la Qos désigne l'aptitude à pouvoir garantir un niveau acceptable de perte de paquets, défini contractuellement, pour un usage donné (voix sur IP, vidéo-conférences, etc.).

En effet, contrairement aux réseaux à communication de circuits, tels que le réseau téléphonique commuté, ou un circuit de communication est dédié pendant toute la durée de la communication, elle est impossible sur internet de prédire le chemin emprunté par les différents paquets.

Ainsi, rien ne garantit qu'une communication nécessitant une régularité de débit puisse avoir lieu sans encombre. C'est pourquoi il existe des mécanismes, dits mécanismes de Qos, permettant de différencier les différents flux réseau et réserver une partie de la bonde passante pour ceux nécessitant un service continu, sans coupures, on parle ici sur la garantie.

[15]Males D., Pujolle G., « Wi-Fi par la pratique », Eyrolles, 2004.

II.9.1.1.1-Niveaux de service :

Définit le niveau d'exigence pour la capacité d'un réseau à fournir un service point à point ou de bout en bout avec un trafic donné. On définit généralement trois niveaux de Qos :

- Meilleur effort (best effort), ne fournissant aucune différenciation entre plusieurs flux réseaux et ne permettant aucune garantie. Ce niveau de service est ainsi parfois appelé « lack of Qos ».
- Service différencié (differentiated service of soft Qos), permettant de définir des niveaux de priorité aux différent flux réseaux sont toutes fois fournir une garantie stricte.
- Service garantie (guaranteed service ou hard Qos), consistant à réserver les ressources réseau pour certains types de flux.
- Le principal mécanisme pour obtenir un tel niveau de service est RSVP (Ressources reSerVation Protocol, traduisez ¨Protocol de réservation de ressources).

II.9.1.1.2-Critères ou paramètres de qualité de service

Les principaux critères permettant d'apprécier la qualité de service sont les suivants :

Débit (en anglais bandwidth) : parfois appelé bande passante, il définit le volume maximal d'information (bits) par unité de temps (b/s).

Perte de paquet (en anglais packet loss) : elle correspond à la non-délivrance d'un paquet de données, la plupart du temps due à un encombrement du réseau.

Gigue (en anglais jitter) : C'est un paramètre important pour les applications communicantes de type voix ou vidéo où la gigue doit être la plus faible possible. La gigue est due principalement aux délais de transferts variables dans les nœuds du réseau (switches et routeurs). Un exemple de la gigue lors de la transmission de trois paquets d'un appel téléphonique où nous remarquons qu'à la transmission le délai entre les deux premiers paquets transmis est de 20 msec alors qu'il varie à la réception[16].

Latence (en anglais delay) : elle caractérise le retard entre l'émission et la réception d'un paquet.

[16]Younes Nadine, op.cit, p40

II.10-Conclusion

Dans ce chapitre nous avons défini le standard IEEE802.11, les améliorations apportées à la technologie IEEE802.11 et ces caractéristiques.

Ensuite on a défini la couche Mac, afin de gérer la priorité d'accès au support et garantir la qualité de service pour les trafics multimédias, le groupe IEEE802.11 a développer de nouveaux mécanisme dans le but de garantir une certaine qualité de service. Ce standard repose sur deux mécanismes d'accès : DCF qui combine les deux algorithmes CSMA et Back-off et PCF qui contrôle l'accès à un média dans les réseaux sans fil à une station centrale. Enfin on a présenté la Qos et ces paramètres.

Chapitre III :

Impact de la taille de la fenêtre de contention et simulation

III.1-Introduction

Les réseaux Ad Hoc multi-sauts suscitent beaucoup d'intérêt grâce à leur déploiement rapide et économique et à leur nature décentralisée.

Dans le troisième chapitre nous allons présenter l'outil de simulation de réseau NS2 et analysé et discuté les résultats des simulations de ces protocoles.

III.2-Présentation du Network Simulator 2

NS2 (Network Simulator 2) est un simulateur de réseau développé pour faire des recherches, il est basé sur les évènements discrets. C'est un environnement riche et populaire, permet de réaliser des simulations des déférents protocoles d'IP dans des environnements filaires et sans fil. Le simulateur utilise le langage orienté objet OTCL dérivé de TCL pour la description des topologies de simulation sous forme d'un script.

Comme il fournit un environnement assez détaillé permettant entre autres de réaliser des simulations d'IP, TCP, du routage et des protocoles multicast aussi bien sur des liens filaires que sans fil[17].

III.3-Simulation

Simuler c'est modéliser un système complexe, afin de prévoir son comportement dans le monde réel. Il s'agit d'une approche permettant de représenter le fonctionnement d'un système réel constitué de plusieurs entités, de modéliser les différentes interactions entre elles, et enfin d'évaluer le comportement global du système et son évolution dans le temps.

Le recours à la simulation permet de contourner les limites de la complexité des modèles analytiques. Toutefois, il est nécessaire de bien identifier les caractéristiques du système afin de la représenter, le plus finement possible, par des modèles abstraits.

[17]A.Berrabah, H.Saidi, Balancement de charges dans lesRéseaux Ad hoc, mémoire de fin d'études, Faculté des Sciences, université Abou BakrBelkaid- Tlemcen, 2012-2013.

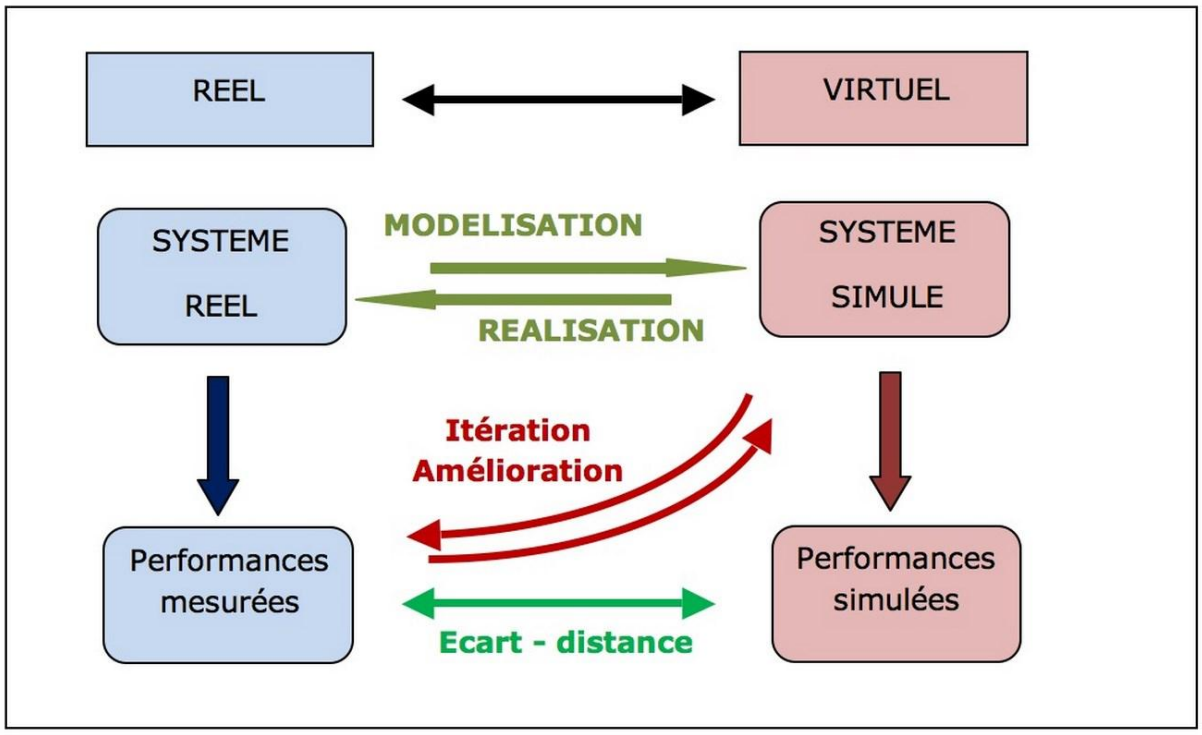

Figure. III 1 : modèle de comportement et simulation.

III.4-Choix du simulateur

Les simulateurs réseaux sont utilisés par des personnes de différents domaines tels que les chercheurs universitaires, industriels et, d'assurance de qualité (AQ) pour concevoir, simuler, vérifier et analyser les performances des protocoles de différents réseaux. Ils peuvent également être utilisés pour évaluer l'effet des différents paramètres des protocoles étudiés

Il existe plusieurs simulateurs réseaux tel que les simulateurs NS-2 et NS-3, OPNET. Le simulateur NS-2 fournit un ensemble d'objets TCL spécialement adapté à la simulation de réseaux. Avec les objets proposés par ce moteur de simulation, on peut représenter des réseaux avec lien filaires ou sans fils, des machines et routeurs (Node), des flux TCP et UDP, et sélectionner des politiques et règles régissantes les files d'attentes mises en œuvre dans chacun des nœuds.

NS2 ne permet pas de visualiser le résultat des expérimentations. Il permet uniquement de stocker une trace de la simulation, de sorte qu'elle puisse être exploitée par un autre logiciel, comme NAM.

III.5-Outil de visualisation NAM

NAM est un outil de visualisation qui présente deux intérêts principaux :

Représenter la topologie d'un réseau décrit avec NS2, et afficher temporellement les résultats d'une trace d'exécution NS2. Par exemple, il est capable représenter des paquets UDP ou TCP, la rupture d'un lien entre nœuds, ou encore de représenter les paquets rejetés d'une file d'attente pleine.

Ce logiciel est souvent appelé directement depuis les scriptes TCL pour NS2, de sorte à visualiser directement le résultat de la simulation.

III.6-Langage de scripte TCL

Le langage TCL est un langage de scripte puissant qui permet d'utiliser éventuellement une approche de programmation orienté objet.

III.7-Logiciel Gnuplot

Est un logiciel scientifique sous linux, libre il permet de produire des représentations graphiques de courbes en 2 dimension (2D) et 3 dimension (3D) de fonctions numériques ou de données[19].

III.8-Simulations et analyses des résultats

Pour observer le fonctionnement de NS2 et de son outil de simulation NAM. Nous avons simulé un montage réseau simple correspondant aux sept nœuds NS2 (Node).

✓ **Contexte de simulation** :

Le tableau suivant représente les paramètres de simulation :

Critère	Valeurs
Antenne	OmniAntenna
Nombre de nœuds	5
Type de la couche mac	IEEE802.11
Modèle de propagation radio	TwoRayGround
Taille du réseau	1000x1000y
Temps de simulation	180 s
Taille du paquet	512 octet
L'intervalle de transmission	0.01 ms
Les paramètres simulés	Débit, perte de paquets
Protocole de routage	AODV
Trafic	CBR

Tableau I.3 : Paramètres de simulation

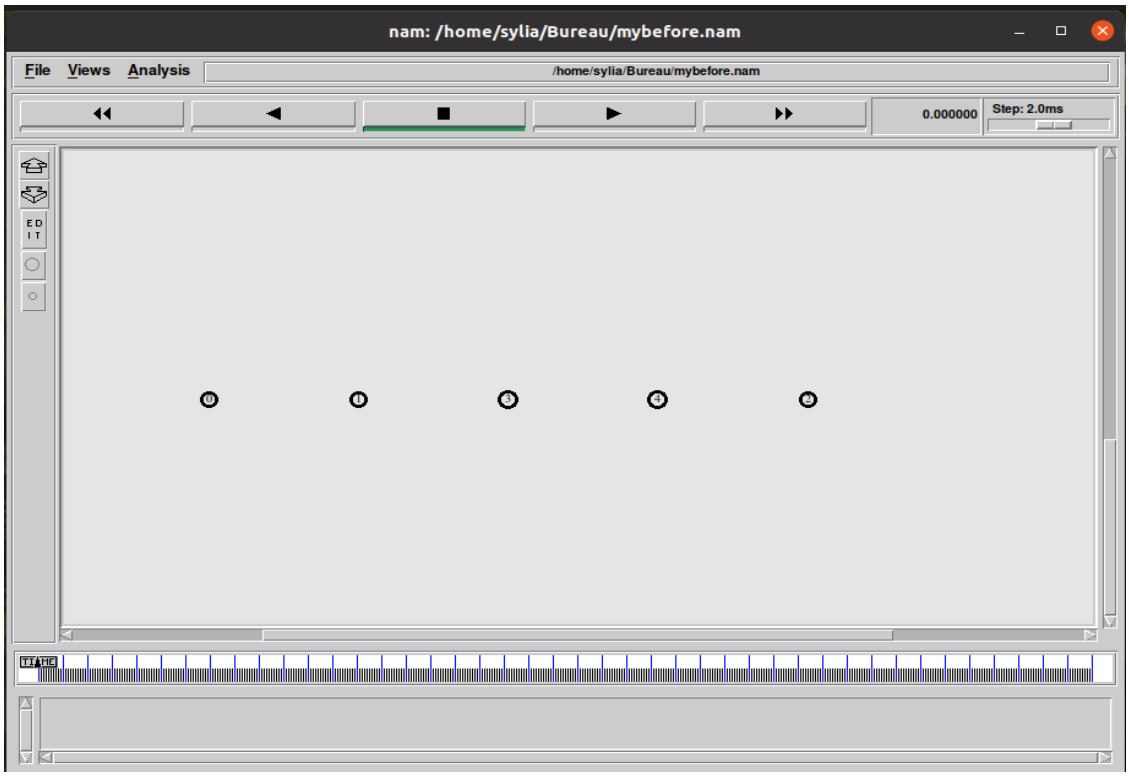

Figure. III 2 : Simulation avec 5 nœuds

Cette figure représente le scénario de simulation avec 5 nœuds avec le protocole AODV dont la topologie est en bus où le nœud n0 transmet des paquets vers le nœud n2.

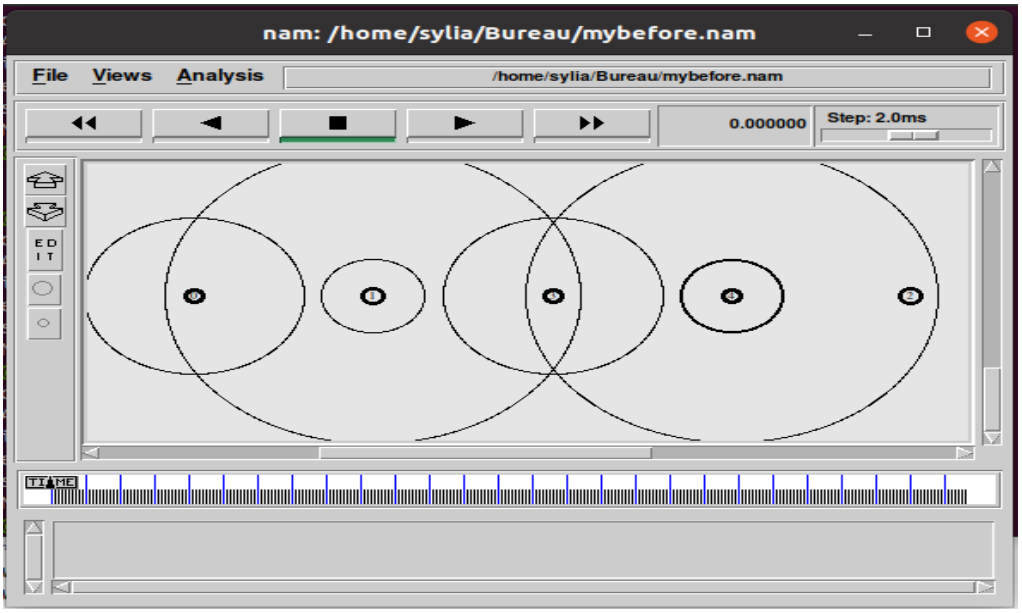

Figure III.3 : Résultat de simulation de transmission de paquet du nœud n0 vers le nœud n2.

Les deux nœuds commencent l'émission de leurs données en CBR en même temps, et nous avons observé le comportement du nœud de commutation à ce moment, avec la valeur minimale et maximale de la taille de la fenêtre de contention [3_15], une saturation du lien reliant les nœuds se produit à partir du moment où la quantité de paquets à transmettre est trop importante pour la taille du lien, et que la file d'attente du lien est saturé.

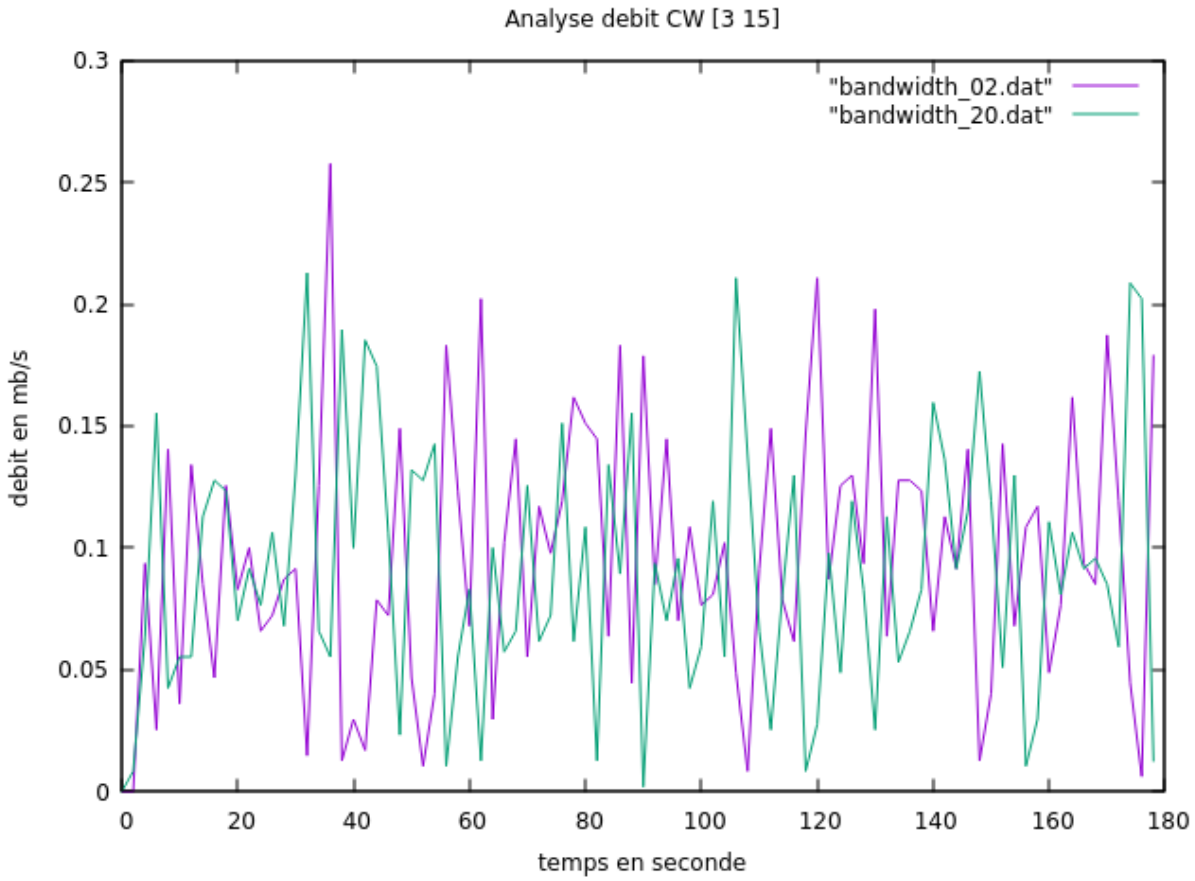

Figure. III 4 : Analyse du débit Fenêtre de contention [3_15]

Dans le cas de transmission de paquets en utilisant une fenêtre de contention de taille [3_15] du nœud n0 vers le nœud n2, on remarque d'après Figure. III 4 que la quantité du débit est approximative pour les deux cas.

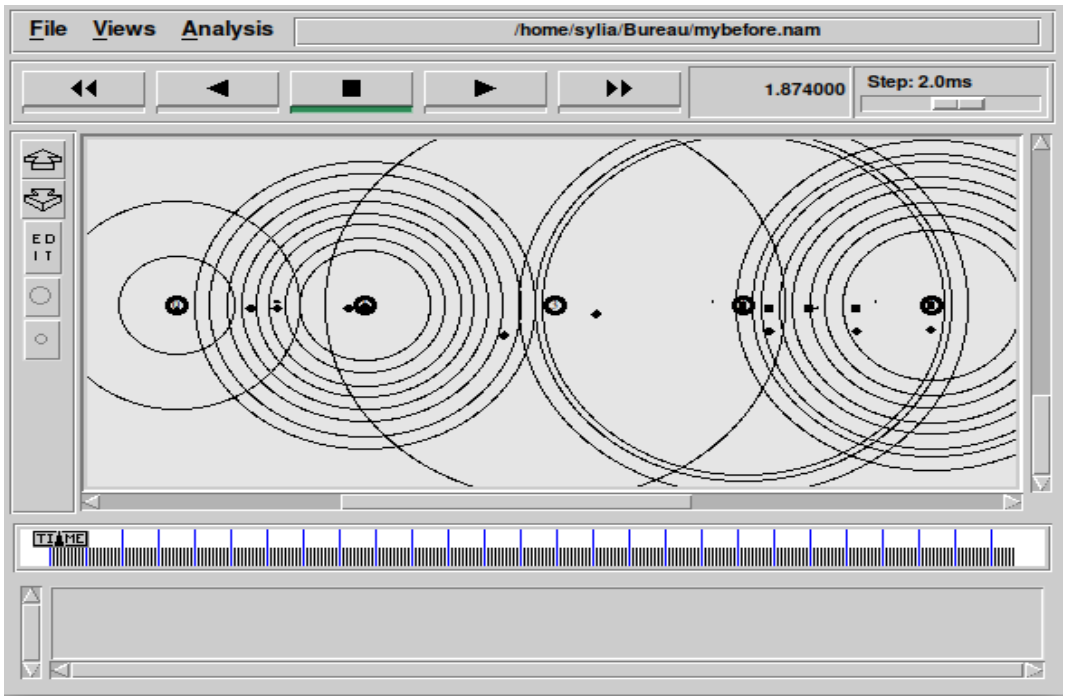

Figure. III 5 : perte de paquets sur Nam CW [3_15]

Cette figure nous montre la quantité de la perte des paquets représentés par des points noirs lors de la transmission en utilisant une fenêtre de contention de taille [3_15].

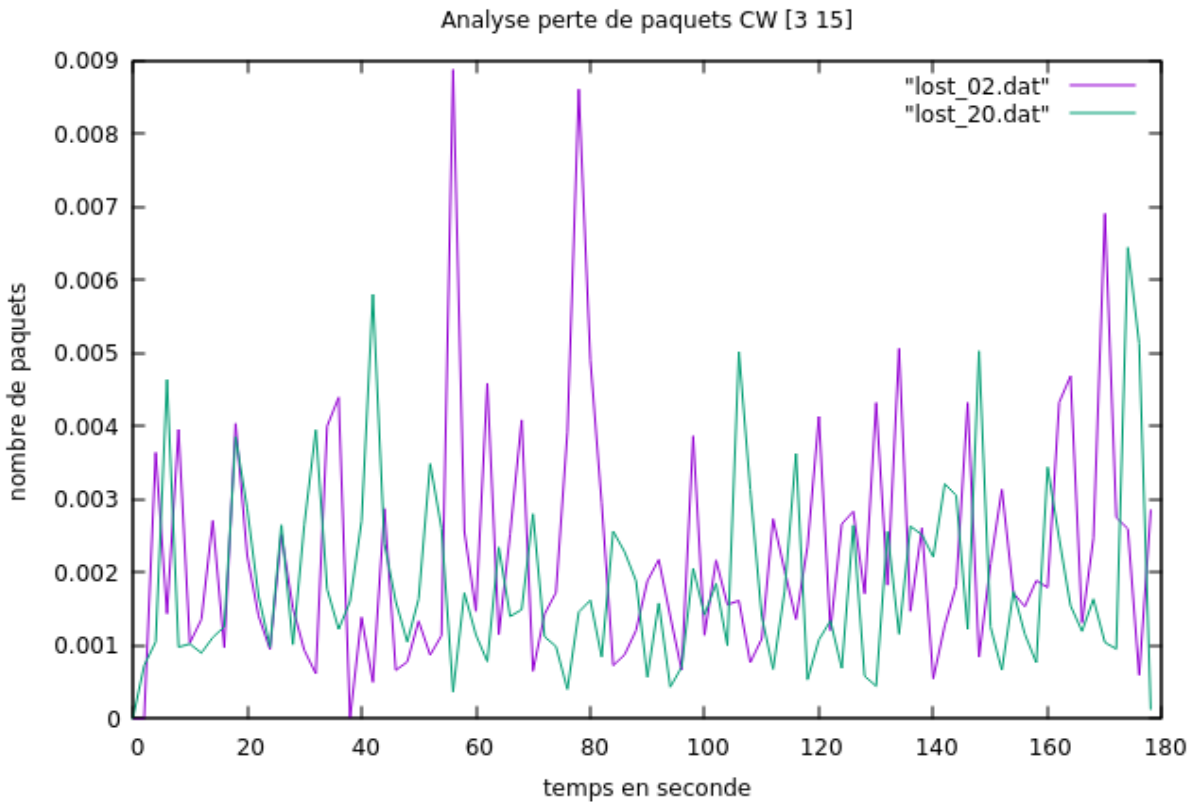

Figure. III 6 : Résultat de la perte de paquets sur gnuplot CW [3_15]

D'après ces résultats on remarque une quantité de perte des paquets intéréssante pour la transmission des paquets.

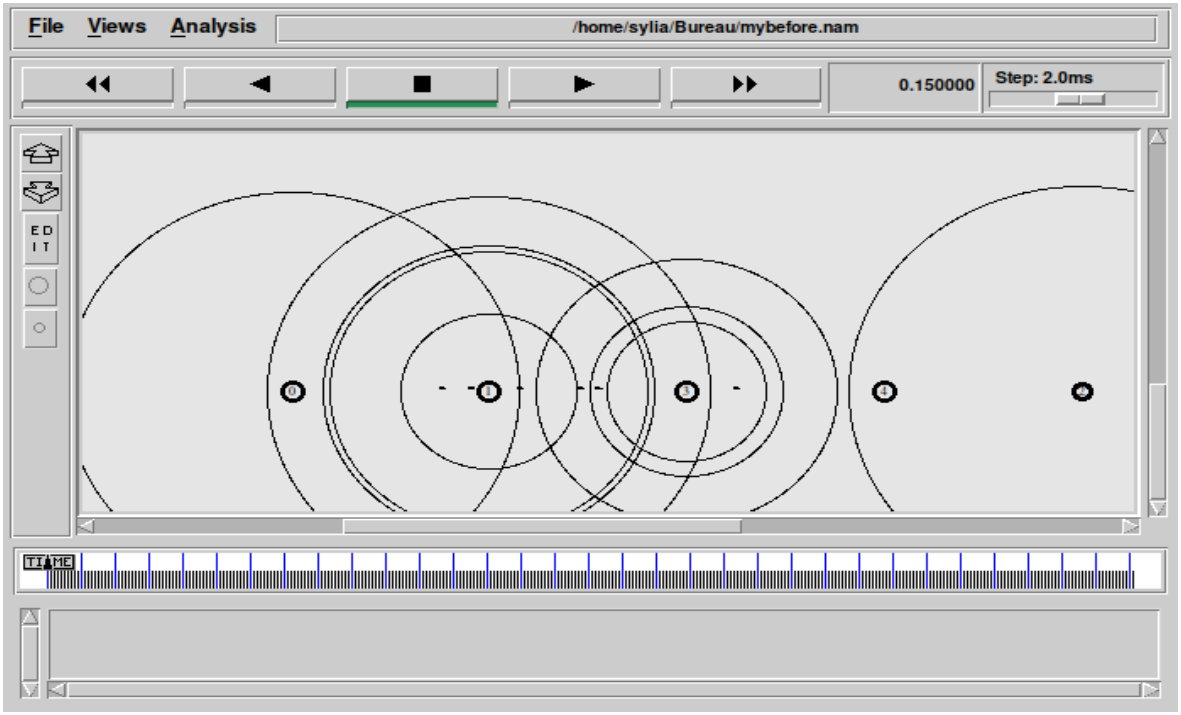

Figure. III 7 : Résultat de simulation CW [7_15]

Cette figure nous montre le résultat de simulation entre les deux nœuds n0 et n2 avec CW[7_15].

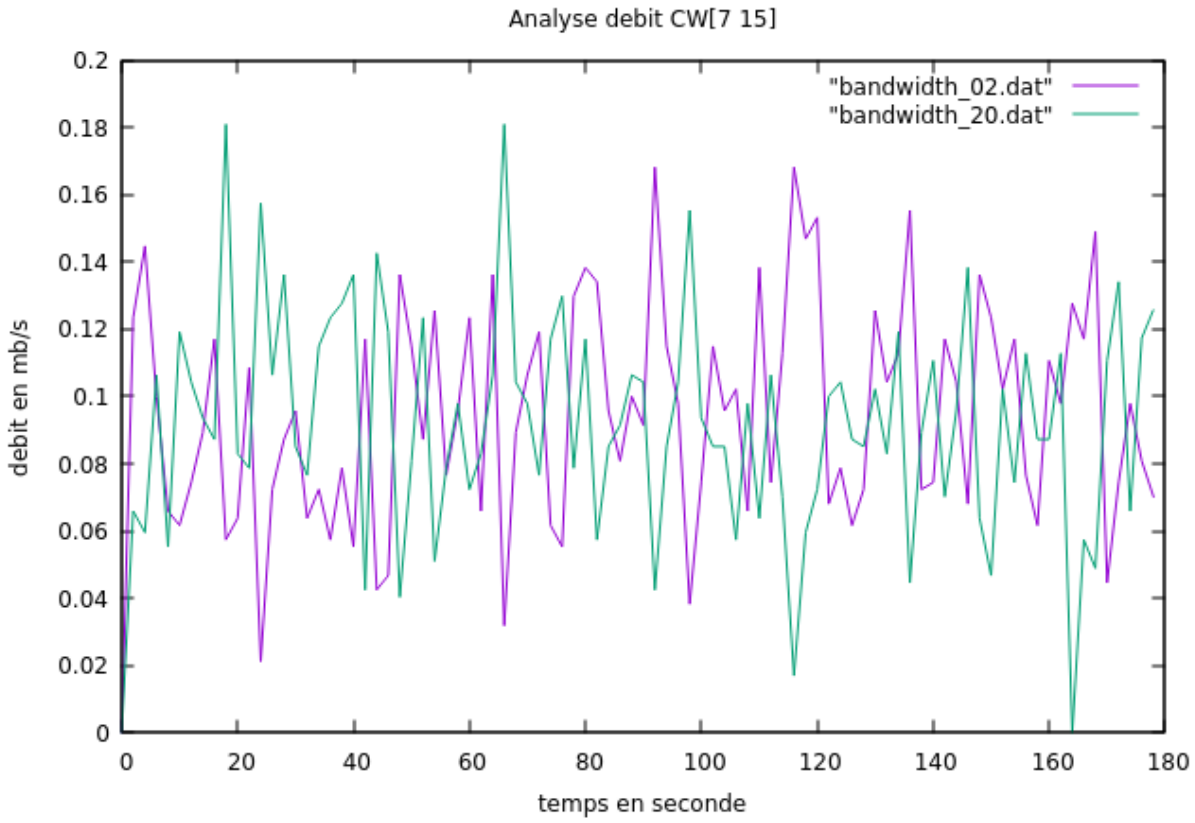

Figure. III 8 : Résultat du débit de transmission CW [7_15]

Dans le cas de la taille de fenêtre de contention CW[7_15], on remarque que le débit est déséquilibré lors de la transmission des données et il d'une quantité inférieure en le comparant avec CW [3_15].

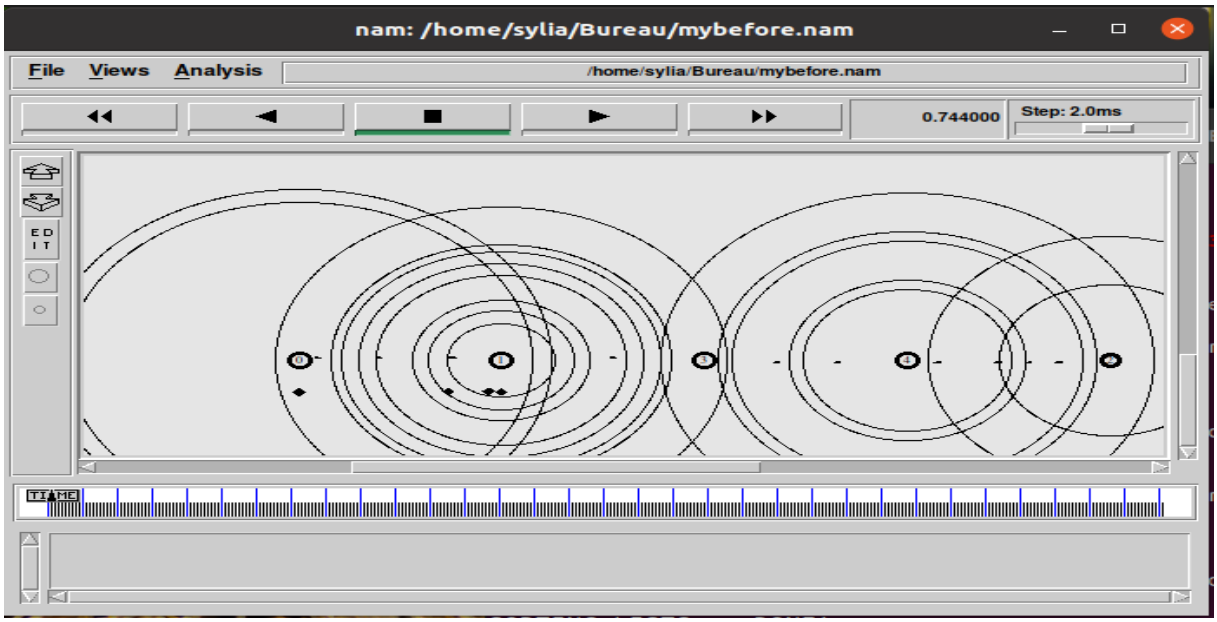

Figure. III 9 : Résultat de la perte de paquets CW [7_15]

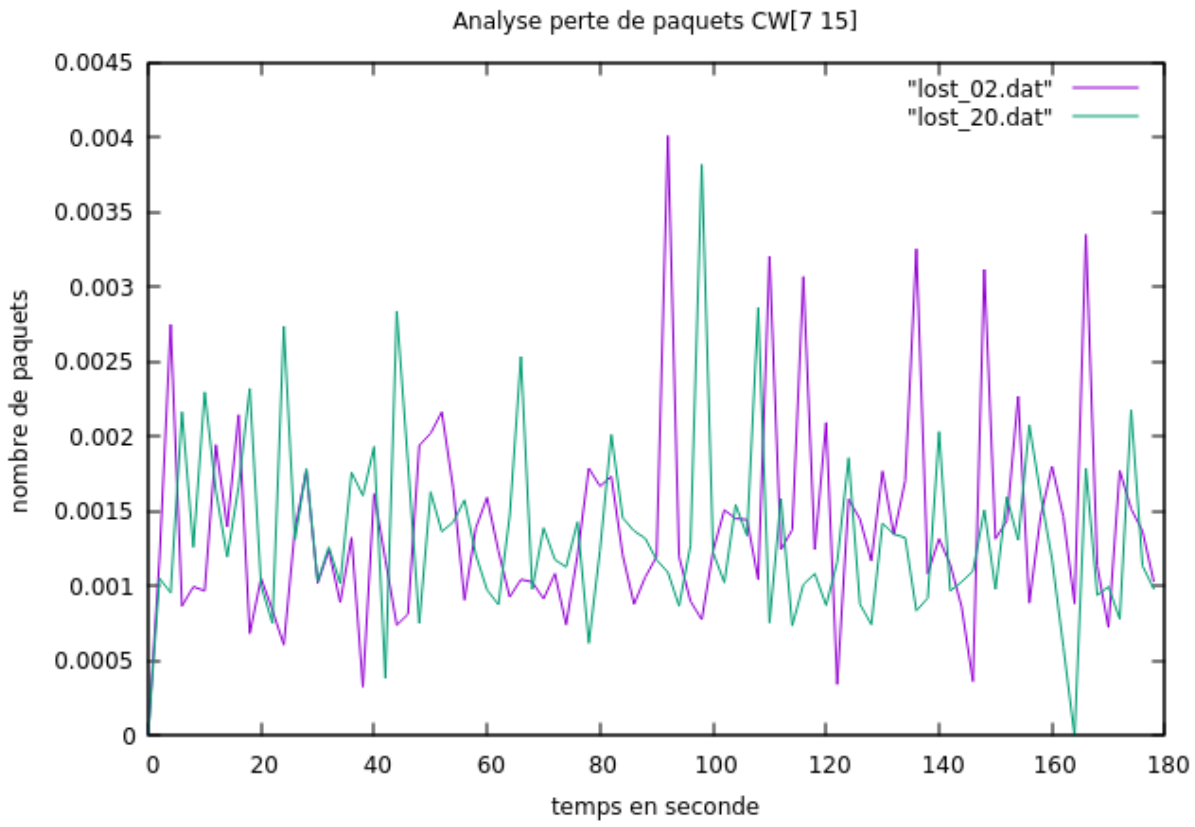

Figure. III 10 : Résultat de la perte de paquets CW [7_15]

La figure III.10 montre que la perte de paquets est faible dans la transmission de données en utilisant une fenêtre de contention de taille [7_15] par rapport à la transmission avec CW [3_15].

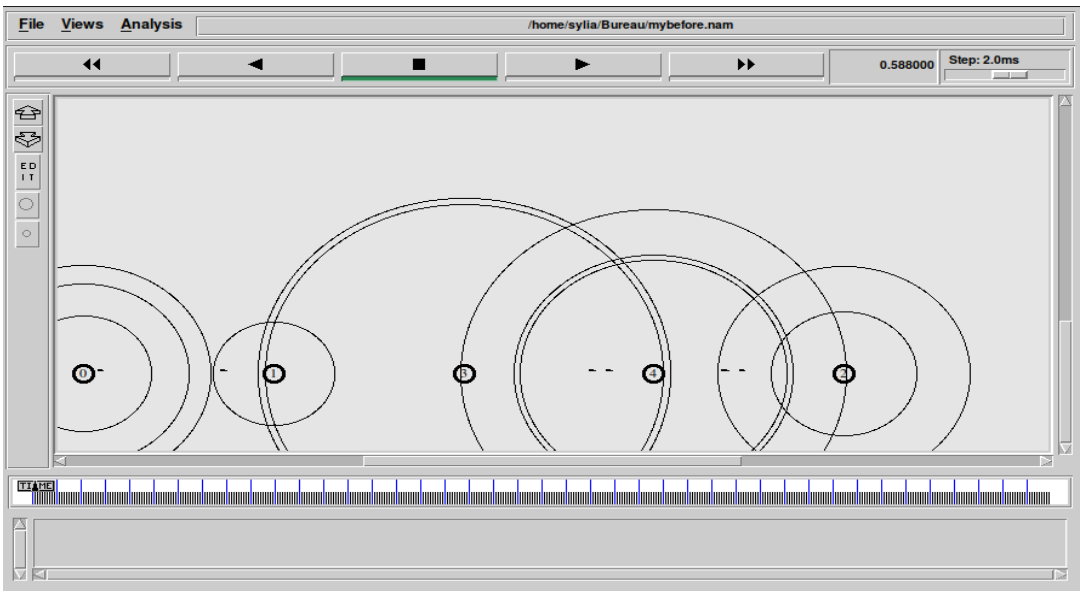

Figure. III 11 : Résultat de simulation CW[15_63]

Nous avons utilisé une fenêtre de contention de taille [15_63] le résultat de simulation est illustré dans la Figure. III 11.

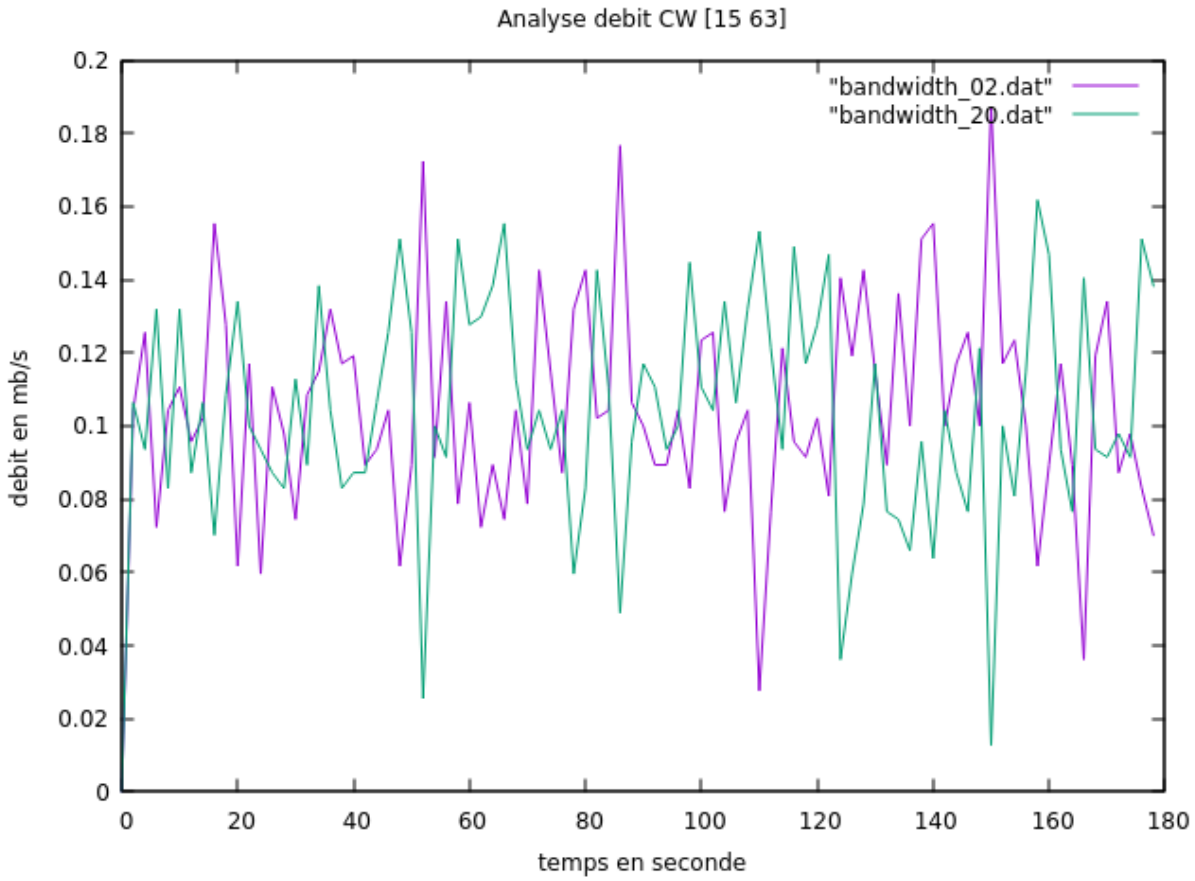

Figure. III 12 : Résultat du débit de transmission avec CW [15_63]

Cette figure nous donne le résultat de débit de simulation avec une fenêtre de contention de taille [15_63] ou on a obtenu les mémes résultats lors de la transmission des données avec CW[7_15].

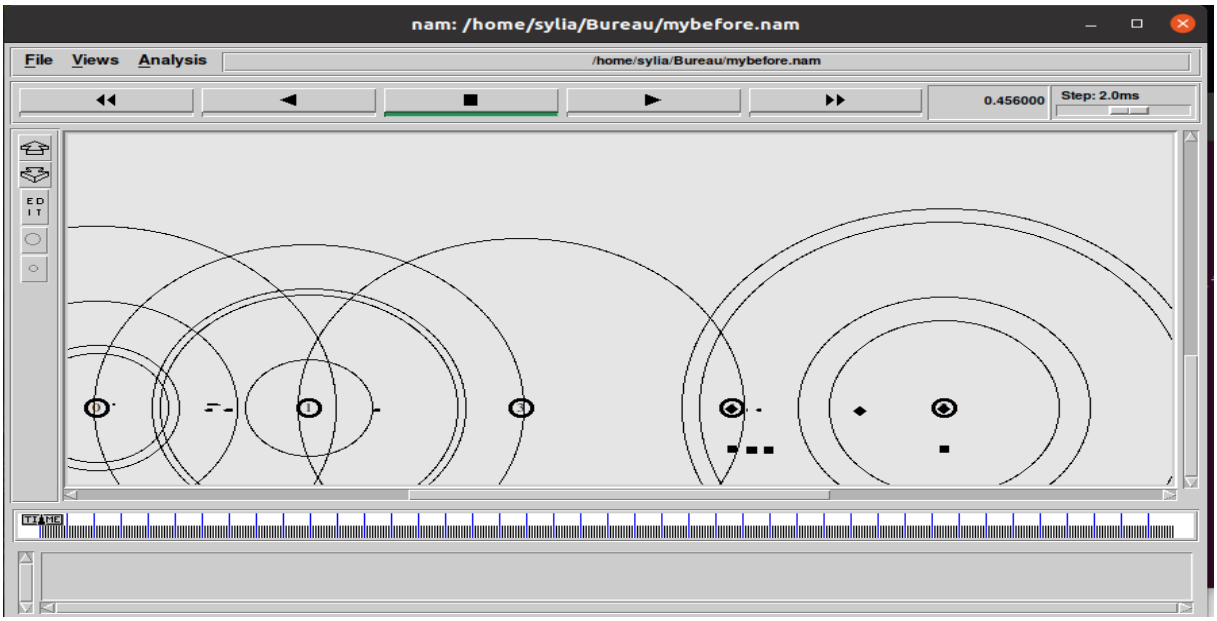

Figure. III 13 : Résultat de la perte de paquets avec CW[15_63] Cette figure nous montre la perte des paquets au niveau des nœuds lors de la transmission des données.

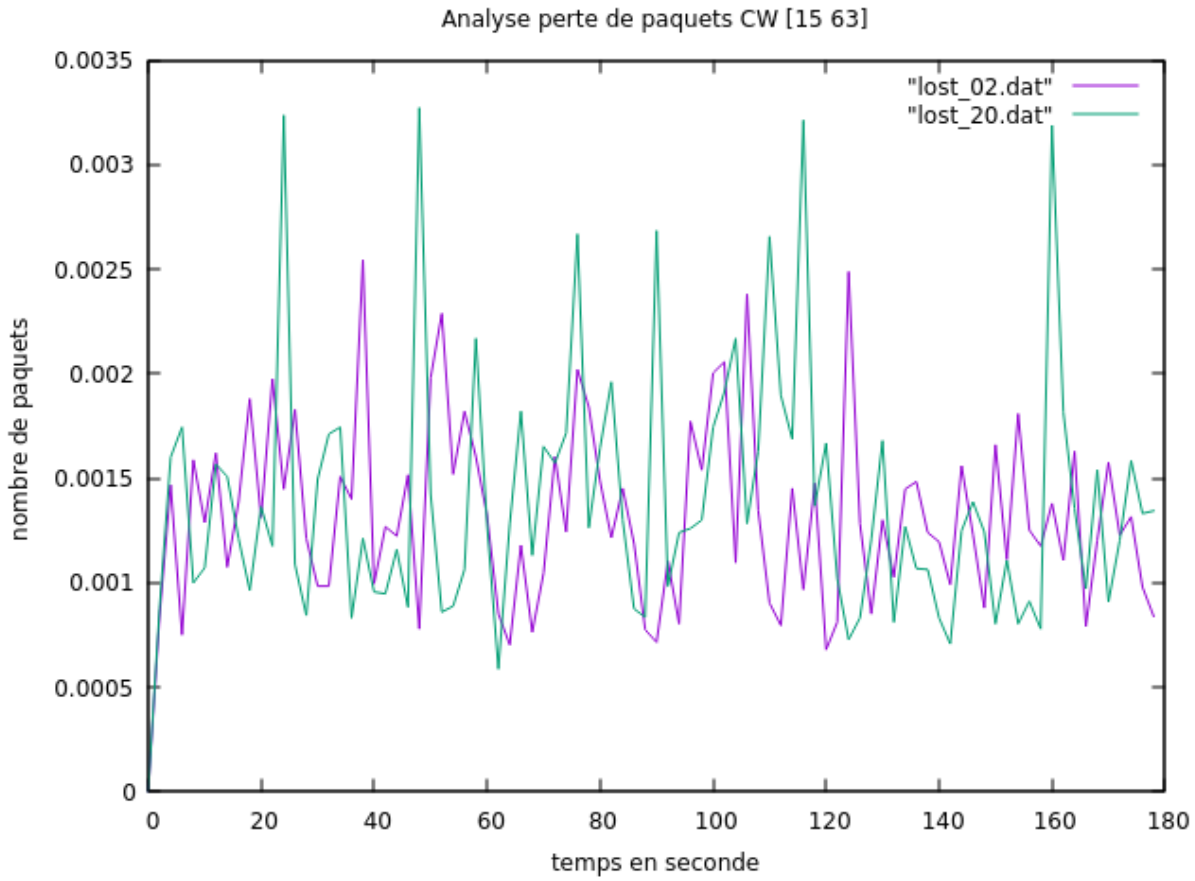

Figure. III 14 : Résultat de la perte de paquets avec CW[15_63]

En analysant la Figure. III 14, nous remarquons que les deux variantes envoient une

quantité de perte de paquets approximative à la transmission de paquets avec CW[7_15] dans le réseau.

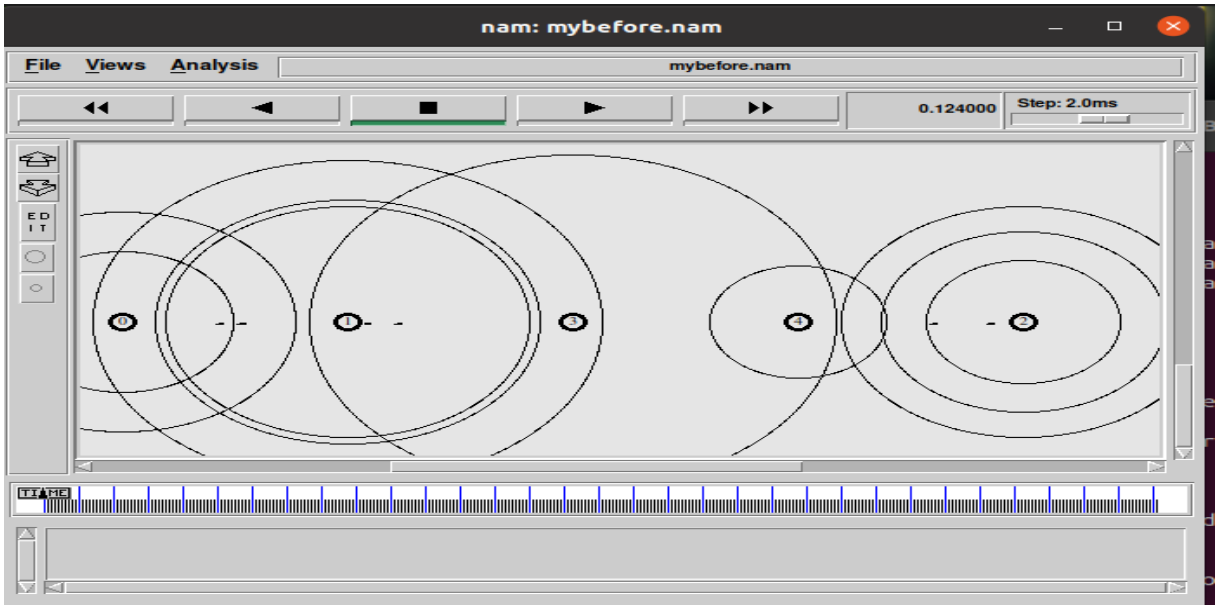

Figure. III 15 : Résultat de simultation avec CW[31_1023]

Cette figure représente le résultat de simulaion en utilisant cette fois une fenêtre de contention de taille CW[31_1023] pour la transmission de données entre les deux nœuds n0 et n2 dans un réseau ad hoc.

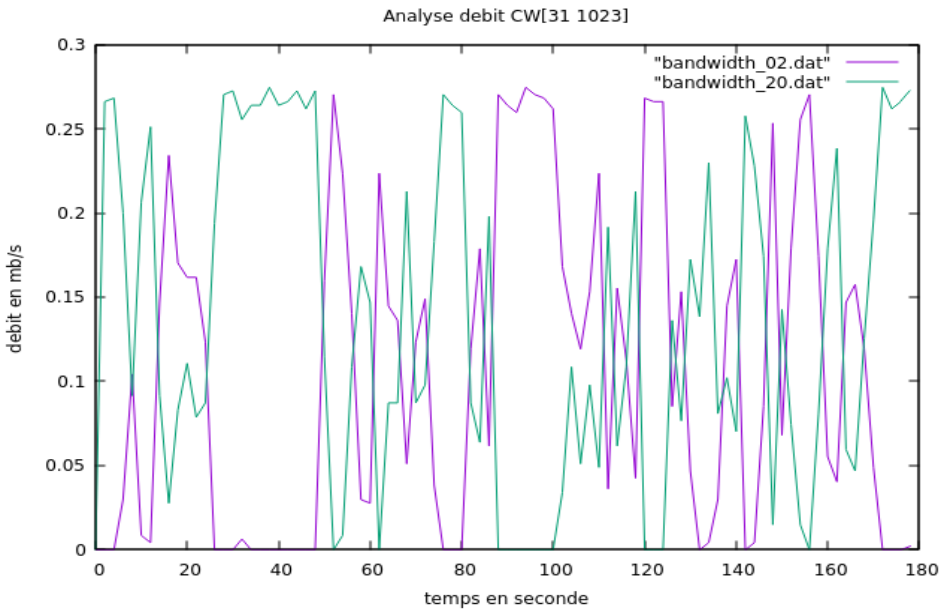

Figure. III 16 : Résultat de débit de transmission avec CW[31_1023]

D'après la Figure. III 16 le résultat de transmission des données nous donne un débit plus élevé jusqu'à 0.27MB/s en comparaison avec les cas de taille de fenêtre de contention CW[7_15], CW[3_15] et CW[15_63].

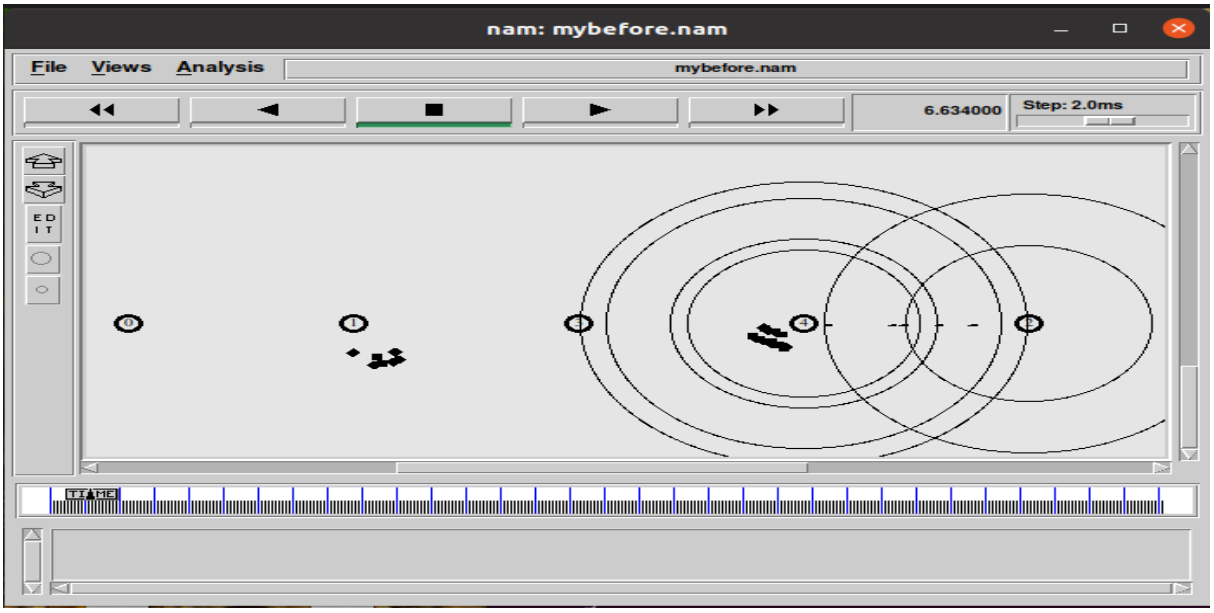

Figure. III 17 : Résultat de la perte de paquets avec CW[31_1023]

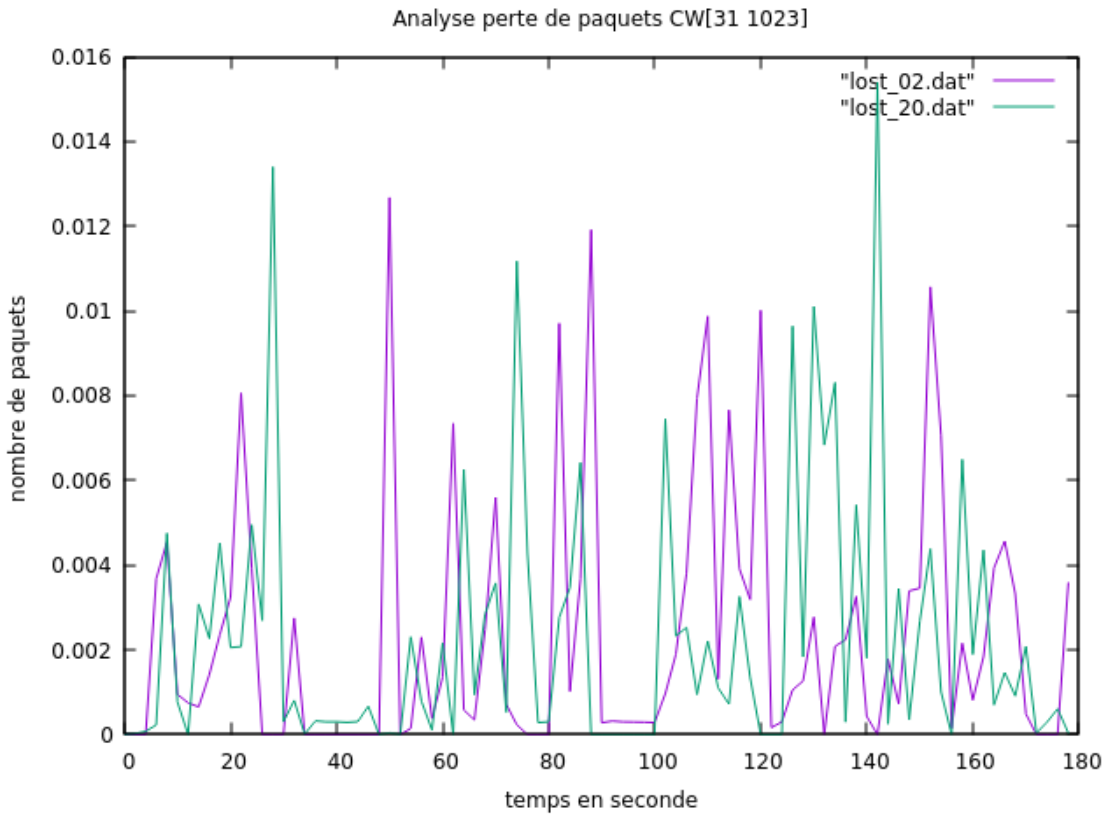

Figure. III 18 : Résultat de la perte de paquets avec CW[31_1023]

Cette figure illustre que la perte de paquets dans cette transmission est considérable quand la taille de la fenêtre de contention est plus grande par rapport aux autres tailles de fenêtre de contention CW[3_15], CW[7_15] et CW[31_1023].

Nous pouvons donc constater que la perte des paquets croit proportionnellement avec la taille de la fenêtre de contention ; ceci peut etre interprété par la présence des nœuds intermédiaires qui coopèrent à la transmission des paquets et encombre le réseau, la non-disponibilité d'une route ou simple perte au niveau de la file d'attente.

Pour une grande taille de fenêtre de contention et en tenant compte des résultats obtenus dans les graphes on constate que le dédit est fort, faible avec une taille minimale de cette fenetre.

III.9-Conclusion

Dans ce chapitre nous avons effectué une simulation sous NS-2 qui nous a permis de voir l'impact de la taille de la fenêtre de contention, la perte des paquets et le débit pour le protocole de routage AODV.

Dans ce travail, nous avons étudié les problèmes de perte de paquets dans les protocoles de routage des réseaux mobiles Ad hoc d'un point de vue théorique. Cette étude a révélé que la taille de la fenêtre de contention dans le protocole AODV influence sur la perte des paquets.

Notre travail nous a permis d'acquérir des connaissances sur l'utilisation de simulateur NS2 ; de simuler le protocole de routage AODV à l'utilisation des paramètres suivants : la perte des paquets et le débit. Les résultats obtenus nous permettrons de conclure qu'une perte de données dues aux retransmissions excessives et à l'encombrement du réseau indiquant une relation proportionnelle entre la taille de la fenêtre de contention, le débit et la perte de paquets.

Conclusion générale

L'objectif de ce mémoire, était d'étudier l'impact de la taille de la fenêtre de contention dans des environnements sans fil. Par ailleurs, les réseaux Ad hoc mobiles « MANET » ont une bande passante limitée et susceptible d'avoir des erreurs.
IEEE 802.11 est la norme des réseaux locaux sans fil la plus déployée.

La sécurisation du routage dans les réseaux Ad hoc reste un problème majeur. Elle se heurte souvent à la difficulté de proposer des mécanismes relativement robustes face aux différentes attaques possibles, causées par les intrusions externes et les nœuds compromis sans pour autant affecter les performances globales du réseau Ad hoc et des protocoles de routage de manière trop prononcée.

Notre travail nous a permis d'acquérir des connaissances sur l'utilisation de simulateur NS2 ; de simuler le protocole de routage AODV à l'utilisation des paramètres suivants : le débit et la perte des paquets. Les résultats obtenus nous permettrons de conclure que le protocole de routage AODV s'intéresse à trouver le plus court chemin en termes de nombres de sauts ainsi que débit s'est illustrée une situation de contention déséquilibrée et en cas de perte de paquets dues aux retransmissions excessives ainsi l'encombrement du réseau.

Notre objectif est d'améliorer la performance d'un réseau mobile Ad hoc à multi-sauts en essayant d'avoir une meilleure qualité de service en contrôlant le débit de bout en bout, et de réduire les pertes lors de la transmission des données selon des tailles différentes de fenêtre de contention.

La simulation a été utilisée pour analyser le réseau MANET sous les conditions requérant la perte de paquets et le débit, nous avons utilisé le simulateur NS-2 et pour mesurer notre approche. Nous comparerons les résultats obtenus des différents scénarios simulés sous le logiciel Gnuplot et Nam du réseau MANET, La comparaison va se faire en variant, chaque fois, un paramètre tel que la perte des paquets ou le débit, et en ajoutant une taille de fenêtre de contention de différents niveaux.

Il est important de noter que dans tous nos scénarios, nous avons procédé à la comparaison de nos résultats, nous pouvons remarquer clairement cette conclusion dans tous nos graphes de pertes de paquets où donne toujours une quantité de pertes assez faible devant une petite taille de fenêtre de contention. Les résultats des simulations montrent une grande amélioration dans le réseau au niveau des débits de bout en bout avec de grande taille de contention.

Nous conclurons que le choix d'un protocole de routage ne dépend pas seulement des paramètres cités et qu'il est intéressant de considérer et de combiner le maximum d'entre elles pour tirer les meilleurs profits et qu'il n'y a pas de solutions pour améliorer la qualité de performance des paramètres du réseau et qu'il n'y aura pas de problèmes lors du l'envoie de paquets.

La simulation est une première étape de vérification et de validation et elle est proche du modèle naturel. D'après les résultats de simulation les recherches restent en cours pour trouver l'approche la plus optimale pour la résolution de ces problèmes, d'abord pour la meilleure qualité de débit de transmission et ensuite pour la réduite de perte de paquets.

Références bibliographique

- A.Berrabah, H.Saidi, Balancement de charges dans les Réseaux Ad hoc, mémoire de fin d'études, Faculté des Sciences, université Abou Bakr Belkaid- Tlemcen, 2012-2013.
- Daniel MABELE MONDONGA,étude sur les protocole de routage d'un réseau ad hoc et leur impacts,mémoire, Institut supérieur d'informatique, programmation et analyse de Kinshasa - Ingénieur informaticien, 2010.
- Ghada zaibi, sécurisation par dynamiques chaotiques des réseaux locaux sans fil au niveau de la couche mac, école nationale d'ingénieurs de Sfax-Tunisie, 6/12/2012
- Males D., Pujolle G., « Wi-Fi par la pratique », Eyrolles, 2004.
- Mirar Youcef, Djettou Brahim Khalil, étude des réseaux ad hoc par la théorie des jeux, univ akliMouhand Oulhadj-Bouira, 2018/2019
- Ratsimbazafimanana Manoela, étude des performances des réseaux wifi avec des simulations sur Opnet, univ d'Antananarivo école supérieure polytechnique,2015/2016.
- Tahar Abbes Mounir, proposition d'un protocole à économie d'énergie dans un réseau hybride GSM et ad hoc, univ Oran,2011/2012
- Younes Nadim, Qualité de service des services multimédia sur les réseaux ad hoc sans fil à multi-saut, école supérieure de technologie univ Quebec,2009
- https://sourceforge.net/projects/gnuplot/

Résumé

Au cours des dernières années, les réseaux MANETs {Mobile Ad hoc NETworks) ont été le sujet de nombreux travaux de recherche. Ces recherches ont couvert plusieurs aspects tels que la qualité de service, les problèmes de routage et le problème d'accès au niveau de la couche MAC, mais bien d'autres ont essayé de développer de nombreuses approches afin de résoudre ces problématiques avec une approche plus globale.

La mise en œuvre des algorithmes de routage des réseaux véhiculaires sans fil est un problème complexe puisque l'environnement est dynamique et évolue au cours du temps ce qui implique un changement de critères des performances de réseau.

Afin de trouver une solution à ces problèmes, nous avons étudié dans un premier temps quelques protocoles de routage dédiés aux réseaux véhiculaires sans fil pour sélectionner un protocole de routage d'informations qui garantit la transmission des paquets. Nous choisissant le protocole AODV pour l'analyse du débit et de la taille de la fenêtre de contention dans les réseaux ad hoc.

En se basant sur les résultats de simulation sous le simulateur NS2 de l'algorithme de routage AODV, on a remarqué que c'est un protocole performant, mais comme les réseaux ad hoc sont un moyen de communication ouverts, cela peut construire une cible idéale pour les attaques qui pourraient intercepter les messages avant d'arriver à leurs destinations.

À la fin de notre travail, nous avons remarqué qu'en cas du débit s'est illustrée une situation de contention déséquilibrée et en cas de perte de paquets dues aux retransmissions excessives indiquant de fortes pertes de paquets à des grandes tailles de fenêtre de contention utilisée.

Cette étude nous permet de résumer qu'il n'y a pas de solution optimale qui peut s'adapter à la nature des réseaux ad hoc afin d'améliorer ses performances globales.

Mot clés: Algorithme de routage, attaque, sécurité, performances, réseau Ad hoc, sans fil, routage, protocole de routage, simulateur, AODV, NS2.

Abstract

In recent years, MANETs networks (Mobile Ad hoc NETworks) have been the subject of much research. This research has covered several aspects such as QoS, routing issues and MAC layer level access issue, but many others have tried to develop many approaches in order to solve these issues with one approach. more global.

The implementation of routing algorithms for vehicular wireless networks is a complex problem since the environment is dynamic and evolves over time, which implies a change in network performance criteria.

In order to find a solution to these problems, we first studied some routing protocols dedicated to vehicular wireless networks to select an information routing protocol that guarantees the transmission of packets. We choose the AODV protocol for throughput and contention window size analysis in ad hoc networks. Based on the simulation results under the NS2 simulator of the AODV routing algorithm, it was noticed that it is a powerful protocol, but since ad hoc networks are an open means of communication, it can build an ideal target. for attacks that could intercept messages before they reach their destinations.

At the end of our work, we noticed that in case of throughput an unbalanced contention situation arose and in case of packet loss due to excessive retransmissions indicating high packet loss at large contention window sizes used.

This study allows us to summarize that there is no optimal solution that can adapt to the nature of ad hoc networks in order to improve its overall performance.

Keywords: Routing algorithm, attack, security, performance, Ad hoc network, wireless, routing, routing protocol, simulator, AODV, NS2