TABLE DES MATIERES ..... **VII**

LISTE DES FIGURES ..... **IX**

LISTE DES TABLES ..... **X**

LISTE DES ACRONYMES ..... **XI**

INTRODUCTION GENERALE ..... **XII**

CHAPITRE 1 : RESEAX AD HOC (ETAT DE L'ART) **1**

1.1. INTRODUCTION 2
1.2. DEFINITION 2
1.3.TYPE DES RESEAUX SANS FIL 2
1.3.1. Les réseaux sans fil personnels WPAN *2*
1.3.2. Les réseaux sans fil locaux WLAN *3*
1.3.3. Les réseaux sans fil mitropolitain WMAN *3*
1.3.4. Les réseaux sans fil locaux WWAN *3*
1.4. LA NORME 802.11 4
1.4.1. Définition *4*
1.4.2. Différentes normes 802.11 ..... *4*
1.4.3. Topologie de réseaux 802.11 ..... *6*
1.4.4. Services réseaux *6*
1.5. LES ENVIRONEMENTS MOBILE 7
1.5.1. Les réseaux avec infrastructure *8*
1.5.2. Les réseaux sans infrastructure *8*
1.6. LES RESEAUX AD HOC 9
1.6.1. Définition *9*
1.6.2. Caratctéristiques des réseaux Ad hoc *10*
1.6.3. Avantages et inconvénients des réseaux Ad hoc *12*
1.6.4. Les appliactions des réseaux Ad hoc *14*
1.6.5. Routage dans les réseaux Ad hoc *14*
1.7.SECURITE DES RESEAUX AD HOC 16
1.7.1. Le WEP *17*
1.7.2. WPA *17*
1.8.CONCLUSION 18

CHAPITRE 2 : PRESENTATION DU PROBLEME DU NŒUD CACHE **19**

2.1. INTRODUCTION ET PROBLEMATIQUE 20
2.2. COUCHE MAC ET RESEAU AD HOC 21
2.3. CLASSIFICATION DES PROTOCOLES MAC 22
2.4. LA COUCHE LIAISION DE DONNEE DU 802.11 22
2.4.1. Logical link control LLC *23*
2.4.2. les trames du 802.11 ..... *24*
2.4.2.1. Les format générale de la trame *24*
2.4.3. MAC 802.11 ..... *25*
2.4.3.1. Protocole ALOHA *26*
2.4.3.2. Protocole MACA *26*
2.4.3.3. Protocole MACAW *27*
2.4.3.4. Protocole CSMA/CA *28*
2.4.3.5. Régulation du débit de transmission *30*

2.4.3.6. La detection passive *31*
2.4.3.7. La detection active *33*
2.5.CONCLUSION 34

CHAPITRE 3 : MODELISATION ET SIMULATION ET ETUDE DE PERFORMANCES 35

3.1. INTRODUCTION 36
3.2. DEFINITION UML 36
3.3. ENVIRONNEMENT DU TRAVAIL 38
3.4. PRESENTATION DU SIMULATEUR NS-2 38
3.4.1. Architecture *38*
3.4.2. le fonctionnement de NS-2 ..... *40*
3.4.3. La création de fichier de paramétrage *41*
3.4.4. Fichier trace *41*
3.4.5. L'analyse du fichier trace *41*
3.4.6. Le programme AWK *42*
3.5. INSTALLATION ET CONFIGURATION 42
3.5.1.Procédure d'installation de NS2 ..... *43*
3.6. NOTRE PROPOSITION 43
3.7. LECHOIX DU PROTOCOLE DE ROUTAGE 44
3.8. SIMULATION 45
3.8.1. Topologie d'étude *45*
3.8.2. Paramètres de la simulation *46*
3.8.3. Scénario 1 (5 Nœuds) *47*
3.8.4. Scénario 2 (7 Nœuds) *49*
3.8.5. Scénario 3 (10 Nœuds) *51*
3.8.6. Discussion des résultats *53*
3.9. CONCLUSION 55

Résumé :

Dans le réseau ad hoc sans fil, le protocole MAC synchronise l'accès de nœuds au canal. L'accès au canal s'affronte au problème classique qui est le problème de nœud caché. La détection active et la détection passive permettent de localiser les nœuds cachés. Dans la détection passive le mécanisme RTS / CTS est utilisé. Nous nous sommes basé sur ce mécanisme avec adjonction du mécanisme sleep/wakeup pour recenser les voisins des nœuds cachés dans le souci de réduire la consommation d'énergie.

Mots clés : nœud caché, énergie, sleep, wakeup

Abstract :

In the Wireless Ad hoc network, the MAC protocol synchronize nodes access to the channel. The channel access confronts with a classic problem wish is the hidden nodes problem. The passive and active detection can be used to detect the hidden nodes. In the passive detection two packets RTS and CTS are used. We based our approach on that mechanism to detect hidden nodes, also we added the sleep and wakeup mechanism to reduce energy consumption.

Keys: hidden node, energy, sleep, wakeup.

De nos jours, l'utilisation de la technologie sans fil a envahi le marché des réseaux detélécommunication. Il existe plusieurs standards tels que : WIFI (IEEE 802.11), Bluetooth(IEEE 802.15.1), Zigbee (IEEE 802.15.4), etc. Ce progrès technologique a ouvert plusieursaxes de recherches dans ce domaine.On distingue deux catégories de réseaux sans fil : les réseaux avec infrastructure et lesréseaux sans infrastructure ou les réseaux ad hoc. Dans les réseaux avec infrastructure, lescommunications s'effectuent via une station fixe. Cette approche est utilisée dans les réseauxsans fil traditionnel et les réseaux locaux sans fil. Cependant les communications dans unréseau mobile ad hoc s'effectuent en absence de toute station fixe.

Notre travail entre dans le cadre de l'étude du mécanisme de détection des nœuds caché dans les réseauxmobiles Ad hoc. Notre étude repose principalement sur les travaux de recherche qui ont étéfait, et qui sont en cours de recherche, dont le but de comprendre le principe et les contraintesd'acheminement des données entre les hôtes mobiles du réseau ad hoc.En effet, nous essayerons d'améliorer une des stratégies de détection des terminaux caché en intégrant leconcept de consommation d'énergie.Pourcela nous donnerons un aperçu sur les réseaux Ad Hoc, leurs caractéristiques, leurs applications,les différentsprotocoles de routage et leur qualité de service dans le premier chapitre.

Dans le second chapitre, nous aborderons la norme 802.11, la sous couche MAC, ainsi nous présenterons lesprotocoles d'évitement de collision et les mécanismes de détection des nœuds cachés.

Dans le dernier chapitre, nous présenterons l'implémentation de la détectionpassive avec le mécanisme RTS/CTS en prenant en considération le critère d'énergie dans lesréseaux ad hoc. Ensuitenous présenterons l'environnent du travail NS (*Network Simulator)* et l'intégration du mécanisme dans ce simulateur.

Finalement, afin de mesurer les performances , nous réaliserons dessimulations à l'aide de NS dans sa version NS-2.35.

1.1 Catégories des réseaux sans fil ……..… 4

1.2 Réseau sans fil avec infrastructure ……..……. 8

1.3 Réseau sans fil sans infrastructure...…….. 9

1.4 Le changement de la topologie des réseaux Ad hoc …..……. 11

1.5 Différents protocoles de routage Ad hoc ……...……..15

2.1 Phénomène du nœud caché ……. 20

2.2 La sous couche mac du 802.11 (Modèle OSI) …… 22

2.3 Déroulement du protocole MACA ……. 27

2.4 Processus de transmission des trames …...…….. 29

2.5 Algorithme CSMA/CA ..…….. 30

2.6 Détection passive avec RTS/CTS ..…….. 32

2.7 Détection passive sans RTS/CTS ...…….. 32

2.8 Détection active ...…… 33

3.1 Séquence d'envoi/réception sans les fonctions sleep() et wakeup()……..37

3.2 Séquence d'envoi/réception avec les fonctions sleep() et wakeup()……..37

3.3 Organisation des classes en NS……...39

3.4 Les principales étapes de simulation sous NS ……..40

3.5 Fichier NAM ……42

3.6 Les différentes étapes de modification sous NS2……...44

3.7 Séquence d'exécution d'un scénario ……...……..45

3.8Topologie d'étude (5 Nœuds) ……..47

3.9 Topologie d'étude (7 Nœuds) ……..……49

3.10 Topologie d'étude (10 Nœuds)……..…….51

3.11 Taux de consommation de l'énergie……...……..53

1.1 Différents normes physiques du 802.11 ……. 5

1.2 Autre révision de la norme 802.11 ……. 5

3.1 Paramètres de la topologie d'étude…….46

3.2 Caractéristique du pc de simulation……...…….46

Chapitre 1

Réseaux Ad Hoc (Etat de l'art)

1.1. Introduction :

Les réseaux sans fil (*Wireless LAN ou WLAN ou IEEE 802.11*), offrent aujourd'hui de nouvelles perspectives dans le domaine des télécommunications. C'est un système de transmission des données, conçu pour assurer une liaison indépendante de l'emplacement des périphériques informatiques qui compose le réseau. Les réseaux sans fil sont principalement employés lorsqu'il s'agit d'interconnecter des utilisateurs entre eux.

Ce système ne pose aucune restriction sur la localisation des usagers. Il utilise des ondes radio plutôt qu'une infrastructure câblée pour communiquer. Ce nouveau mode de communication engendre de nouvelles caractéristiques, propres à l'environnement mobile : de fréquentes déconnexions, un débit de communication et des ressources modestes, et des sources d'énergie limitées.

Dans ce chapitre, nous allons présenter les réseaux sans fil ainsi que la norme 802.11 ensuite nous allons parler des caractéristiques et applications des réseaux Ad hoc mobile.

1.2. Définition :

Un réseau sans fil (Wireless Network) est un réseau dans lequel les machines participantes ne sont pas raccordées entre elles par un médium physique. Ce type deréseau permet aux utilisateurs de se déplacer dans un certain périmètre de couverture sans perdre le signal et sans avoir besoin de câble de raccordement au réseau.

La transmission des données entre les nœuds constitutifs du réseau ne se fait pas via un support physique mais sur la base d'ondes hertziennes (radio, infrarouge). Cetype de réseau permet de relier divers équipements distants et cela dans un périmètre allant de quelques mètres à plusieurs dizaines de mètres selon les fréquences etles puissances utilisées.

1.3. Type des réseaux sans fil : [1]

1.3.1. Les réseaux sans fil personnels WPAN :

Ces réseaux concernent les réseaux sans fil à très faible portée d'une dizaine de mètres au maximum. Ils sont généralement utilisés pour établir une liaison sans fil tel que les

imprimantes, claviers, souris, téléphones portables. Les principales technologies pour ce type de réseau sont :

- **Bluetooth** : lancée par Ericsson en 1994, le Bluetooth ou IEEE 802.15.1 est la principale technologie utilisée pour les WPAN. Elle permet des débits allant jusqu'à 1 Mbps sur une portée maximale d'une trentaine de mètres tout en étant économique en consommation d'énergie.
- **Zigbee** : basée sur la norme IEEE 802.15.4, elle offre des débits moins important que ceux du Bluetooth puisqu'elle peut atteindre 250 Kbps au maximum, toute fois cette technologie est moins consommatrice que le Bluetooth.
- **Les liaisons infrarouges** : les liaisons infrarouges sont très utilisées pour des communications à courte distance, cependant leur sensibilité aux perturbations empêche le développement de cette technologie dans les réseaux sans fil supérieurs à une distance d'une dizaine de mètre.

Néanmoins, la portée d'interception peut-être très supérieure.

1.3.2. Les réseaux sans fil locaux WLAN :

Ces réseaux permettent de couvrir des zones d'une centaine de mètres environ dont la principale norme est l'IEEE 802.11 qui permet des débits allant jusqu'à 540 Mbps théoriquement.

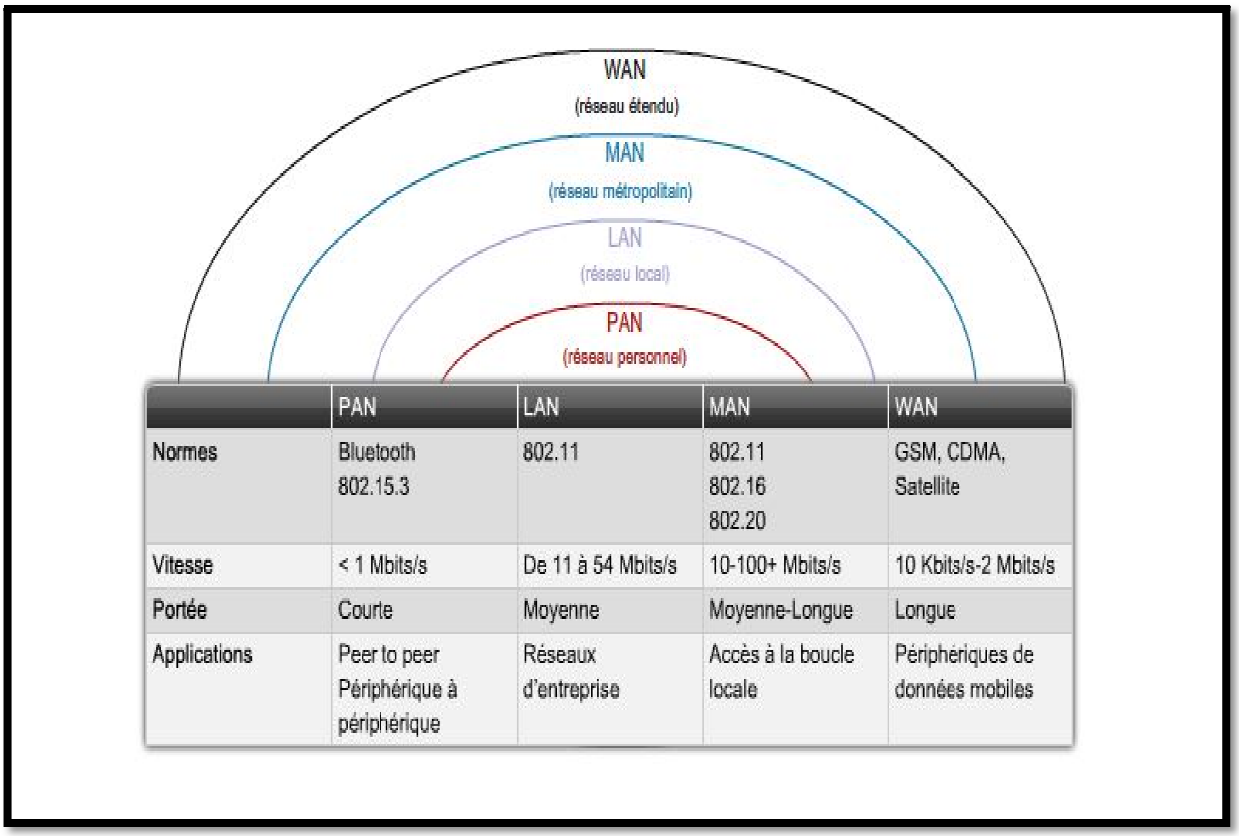
Une autre norme pour les WLAN est l'ESTI Hiperlan qui permet d'atteindre des débits de 54 Mbps en utilisant la bande de fréquences comprise entre 5150 et 5300 MHz.

1.3.3. Les réseaux sans fil métropolitains WMAN :

Plus connus sous le nom de boucle local Radio (BLR), basés sur la norme IEEE 802.16, ils permettent des débits allant jusqu'à 70 Mbps sur une portée de plusieurs kilomètres.

1.3.4. Les réseaux sans fil étendus WWAN :

Ils concernent principalement les réseaux cellulaire utilises par les opérateurs de télécommunications. Les principales technologies utilisées dans ces réseaux sont le GSM,le GPRS, l'UMTS



	PAN	LAN	MAN	WAN
Normes	Bluetooth 802.15.3	802.11	802.11 802.16 802.20	GSM, CDMA, Satellite
Vitesse	< 1 Mbits/s	De 11 à 54 Mbits/s	10-100+ Mbits/s	10 Kbits/s-2 Mbits/s
Portée	Courte	Moyenne	Moyenne-Longue	Longue
Applications	Peer to peer Périphérique à périphérique	Réseaux d'entreprise	Accès à la boucle locale	Périphériques de données mobiles

Figure 1.1: *catégorie des réseaux sans fils.*

1.4. La norme 802.11 :

1.4.1. Définition :

Le 802.11 est la norme décrivant les caractéristique d'un réseau local sans fil .le Wi-Fi par contre est la certification délivrée par le Wi-Fi alliance anciennement appelé WECA pour Wireless Ethernet Compatibility Alliance, l'organisme charge de maintenir l'interopérabilité du matériel 802.11. Pour des raisons de marketing, le Wi-Fi désigne le nom commercial 802.11.

1.4.2. Différentes normes 802.11 : [2]

La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps.

Des révisions ont été apportées à la norme originale afin d'optimiser le débit (c'est le cas des normes 802.11 a ,802.11 b et 802.11g ,802.11 n appelées normes 802.11 physiques) ou bien préciser des éléments afin d'assurer une meilleure sécurité ou une meilleure interopérabilité. Le tableau 1 présente les différentes normes physiques du 802.11 et leur signification et le tableau 2 les autre révisions du 802.11 :

NORME	DESCRIPTION	Année de finalisation
802.11	Normalisation de la couche MAC (Medium Access Control) commune à tous les WLAN et de trois couches physiques : couches physique infrarouge 1 et 2 Mbit/s, couche physique FHSS 2,4 GHz à 1 et 2 Mbit/s et la couche physique DSSS 2,4 GHz à 1 et 2 Mbit.	1997
802.11a	Baptisée Wi-Fi 5 Cette norme définie une couche physique OFDM permettant des débits jusqu'à 54 Mbps.	1999
802.11b	C'est la norme la plus répandue actuellement elle utilise une couche physique DSSS sur la bande de fréquence des 2,4 GHz et 5 GHz pour atteindre des débits de 5,5 Mbps et 11 Mbps.	1999
802.11g	Cette norme définit une couche physique permettant d'atteindre les 54 Mbps.	2003
802.11n	Cette norme permet d'atteindre les 540 Mbps théoriquement en pratique, 100 Mbps.	2006

Tableau 1 :*différentes normes physiques du 802.11.*

Norme	Description
802.11c	Pontage au niveau MAC 802.11
802.11d	La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11
802.11e	La norme 802.11e vise à donnes des possibilités en matière de qualité de service au niveau de la couche liaison de données.
802.11f	La norme 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits.
802.11h	La norme 802.11h vise à rapprocher la norme 802.11 au standard européen (HiperLAN 2, d'où le h de 802.11h).
802.11i	Couche MAC qui améliore les mécanismes de sécurité de l'authentification.
802.11IR	La norme 802.11j est à la réglementation japonaise ce qui le 802.11h est à la réglementation européenne.
802.11k	Amélioration et matière de mesure des ressources radio pour les couches supérieures.

802.11m	Maintenance de la norme IEEE 802.11 avec des corrections techniques éditoriales.

Tableau 2 :*autre révision de la norme 802.11*

1.4.3. Topologie de réseaux 802.11 : [2]

Les réseaux 802.11 sont constitués de quatre composants physiques principaux :

- **Station** : Ceux sont des composant disposant d'une interface réseau sans fil permettent de se connecter au réseau. Ça peut être des ordinateurs portables, ordinateurs de poche, ordinateurs de bureau ou tout autre appareil électronique disposant de l'interface 802.11.
- **Points d'accès** : ceux sont généralement des périphériques qui servent de pont entre le réseau sans fil et les réseaux filaires mais ils effectuent également d'autres fonctions comme l'acheminement des trames aux stations concernées.
- **Medium sans fil** : En général le médium utilisé est la fréquence radio. A la base, deux couches physiques par fréquence radio et une par infrarouge ont été normalisées. Mais seules celles utilisant les fréquences radio ont été acceptées.
- **Systèmes de distribution** : pour garantir une large zone de couverture plusieurs points d'accès doivent communiquer pour suivre le déplacement des stations mobiles. Le système de distribution est donc le système permettant d'acheminer les trames vers les stations de destination.

Un réseau 802.11 est constitué d'un ensemble de stations qui communiquent entre elles. Cet ensemble est nommé « ensemble de services de base »(BBS-basic service set).Il existe deux types de BBS ou de réseaux 802.11,les réseaux sans infrastructure et les réseaux avec infrastructure.

1.4.4. Services réseaux : [3]

Le 802. 11 fournit neuf services : trois services pour la transmission de données et six services de gestion.

- **Distribution** : c'est le service utilisé pour la livraison de la trame à destination. Toute communication qui passe par un point d'accès utilise le service de distribution. Lorsque le point d'accès reçoit une trame, il utilise le service de distribution pour livrer à destination

que ce soit en passant d'abord par un autre point d'accès ou directement à la station de destination.

- **Intégration** : ce service permet de connecter le réseau 802.11 à un réseau externe à travers le système de distribution.
- **Association** : utilisé pour définir le point d'accès servant de passerelle a une station mobile. Quand une station accède au réseau pour la première fois elle utilise ce service pour s'associer à un point d'accès.
- **Réassociation** : lorsqu'une station passe d'un BSS a un autre au sein du même ESS, elle utilise ce service afin de s'associer au nouveau point d'accès.
- **Dissociation** : c'est un service de politesse qu'utilise - pas obligatoirement - une station pour se relier du réseau.
- **Authentification** : Etablit l'identité de la station avant d'effectuer l'association. Elle assure un minimum de sécurité.
- **Dés authentification** : utilise pour clore l'authentification. Elle également pour effet de clore l'association.
- **Confidentialité** : initialement assure par le protocole WEP – Wired Equivalent Privacy, ce service a été étendu par le 802.11 en apportant une authentification de l'utilisateur, la gestion de clés de chiffrement, deux problème non assurés par le WEP.
  Livraison MSDU- MAC Service Data Unit : Service responsable de l'envoi des données au destinataire.
  Contrôle de la puissance d'émission : le TCP –Transite Power Control – Réduit les interférences en diminuant la puissance d'émission des stations. Ce service a été défini par la norme 802.11h pour éviter les interférences avec les utilisateurs de la norme 5GHz en Europe.
  Sélection dynamique de la fréquence : certains systèmes radars fonctionnent dans la bande des 5GHz. C'est pourquoi le DFS – dynamique Frequencyselection – a été définit pour éviter les interférences avec ces radars.

1.5. Les environnements mobiles :

Un environnement mobile est un système composé de sites mobiles, qui permet à sesutilisateurs d'accéder à l'information indépendamment de leurs positions géographiques.Les réseaux mobiles ou sans fil peuvent être classés en deux :

1.5.1. Les réseaux avec infrastructure :

Egalement appelés le mode BSS (Basic Service Set), Il s'agit du type classique deréseau sans fil, ils sont constitués d'un groupe de sites fixes (point d'accès) auxquels seconnectent des terminaux mobiles (voir figure 1.2), leur fonctionnement s'appuie sur laprésence d'unités fixes communiquant avec un ensemble de nœuds mobiles via des ondesélectromagnétiques, mais également entre eux par un réseau filaire.

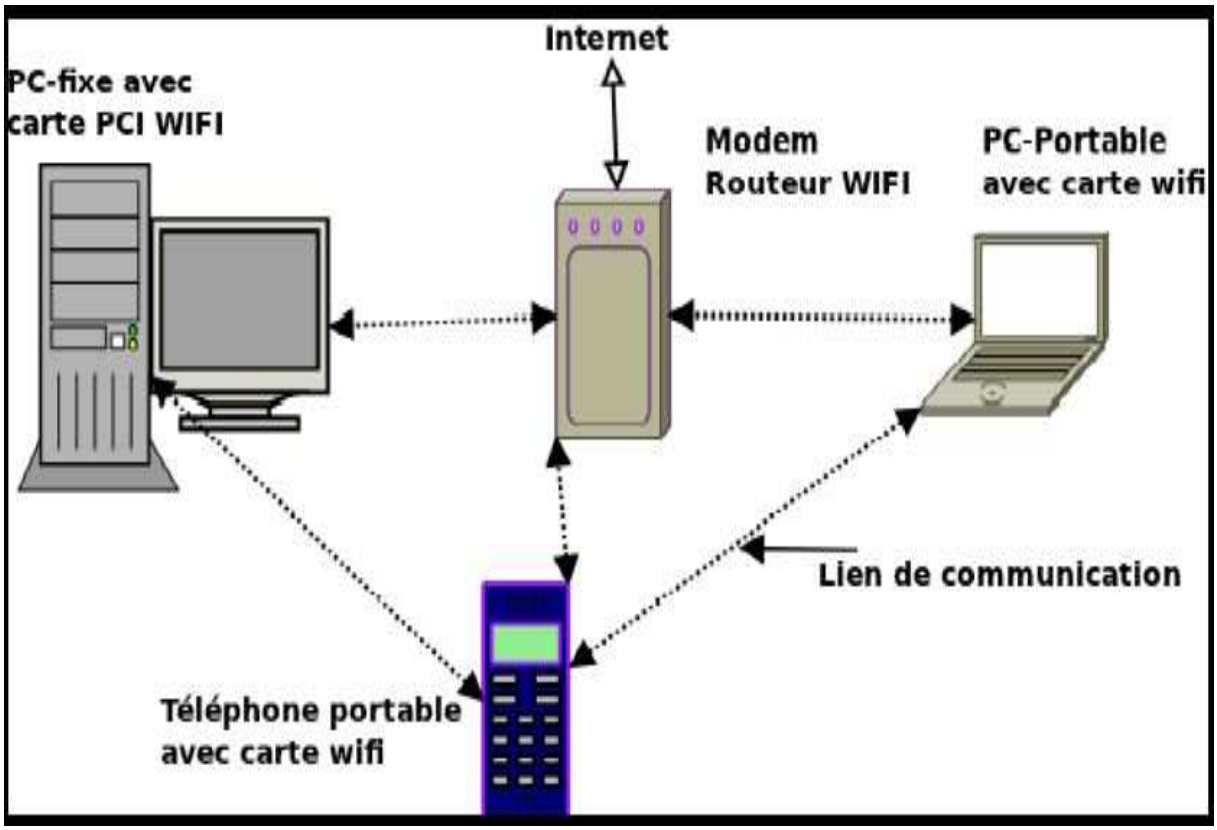


Figure 1.2: *réseau sans fil avec infrastructure.*

.

1.5.2. Les réseaux sans infrastructure :

Également appelés réseaux mobiles Ad hoc ne comportant pas l'entité « site fixe », tous les sites du réseau sont mobiles et communiquent d'une manière directe en utilisant leursinterfaces de communication sans fil.Chaque unité mobile se comporte à la foiscomme un émetteur, un récepteur et un routeur de l'information.

Les réseaux ad hoc auxquels nous nous sommes intéressés sont ceux décrits et étudiés par legroupe de travail MANET. Un réseau mobile ad hoc est défini comme unecollectiond'entités mobiles interconnectées par une technologie sans fil, formant un réseau temporaire,sans l'aide d'une infrastructure préexistante (voir figure 1.3).

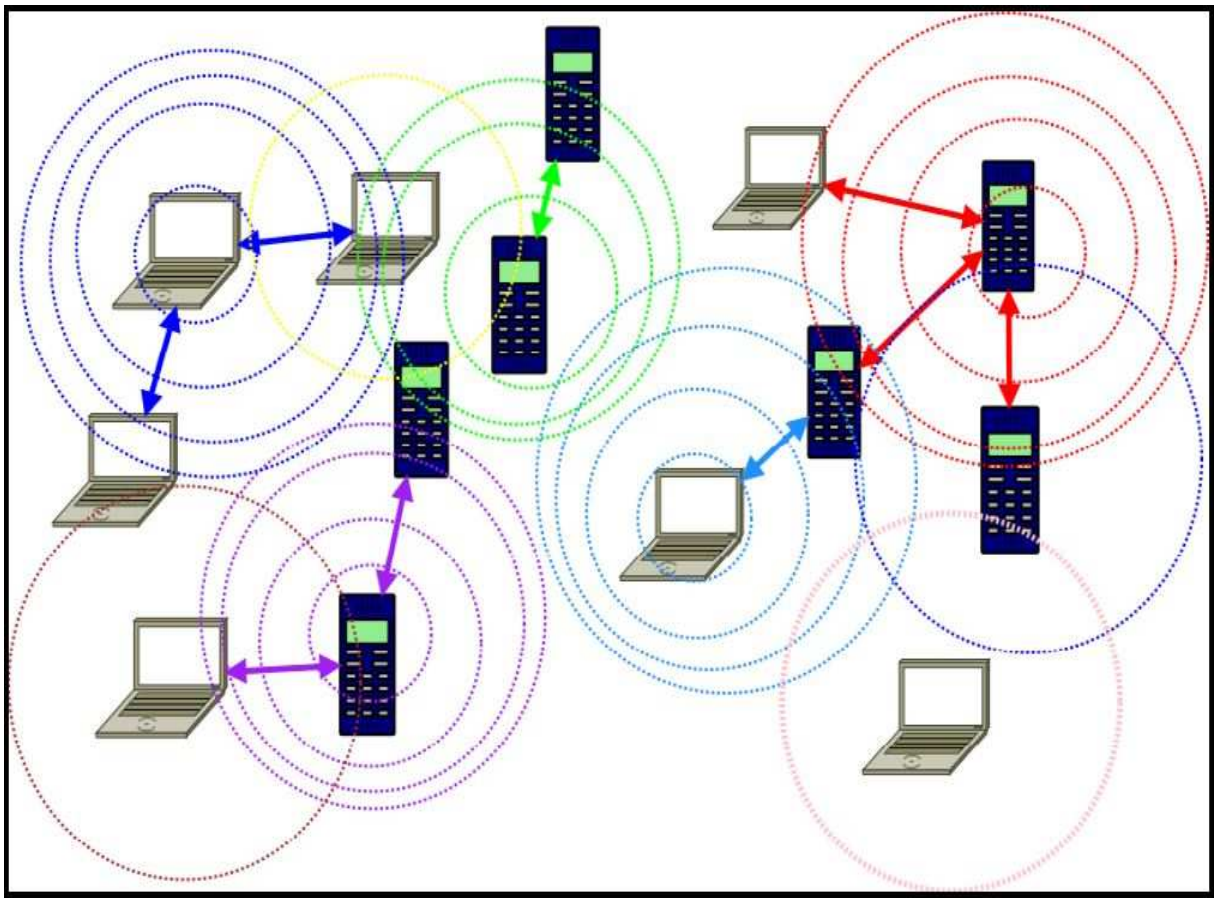


Figure 1.3: *réseau sans fil sans infrastructure.*

1.6. Les réseaux Ad hoc :

1.6.1. Définition :

Les réseaux Ad hoc appelé également MANET pour Mobile Ad hoc Network (issu du groupe de travail **[5]**) peut être définit comme un réseau formé dynamiquement par une collection de nœuds mobiles placés arbitrairement et ceci sans l'utilisation d'une quelconque infrastructure existante et sans infrastructure centralisée.

1.6.2. Caractéristiques des réseaux Ad Hoc : [6]

Parmi les caractéristiques des réseaux ad hoc :

- **Présence des interférences :**

Il est reconnu que le taux d'erreur de transmission dans les réseaux radio est nettement plus élevé que dans les réseaux filaires. Cela est dû, généralement, aux problèmes d'interférences qui peuvent être de natures diverses :

1. Le nombre limité de canaux disponibles.
2. Les fréquences d'émissions sont proches, ainsi, les émetteurs travaillant à des fréquences trop proches peuvent interférer entre eux.
3. Les bruits produits par l'environnement (certains équipements électriques, certain moteur)
4. Phénomènes d'atténuation, de réflexion et des chemins multiples qui rendent le signal incompréhensible en le déformant.

- **Topologies dynamiques :**

Une particularité très importante qui distingue les réseaux mobiles Ad Hoc des réseaux filaires est la mobilité de ses nœuds. Ces nœuds se déplacent librement dans le réseau, et à tout moment des nœuds actifs peuvent quitter le réseau ou de nouveaux nœuds peuvent le rejoindre. Cette caractéristique rend la topologie de ce type de réseaux sans fil très dynamique.

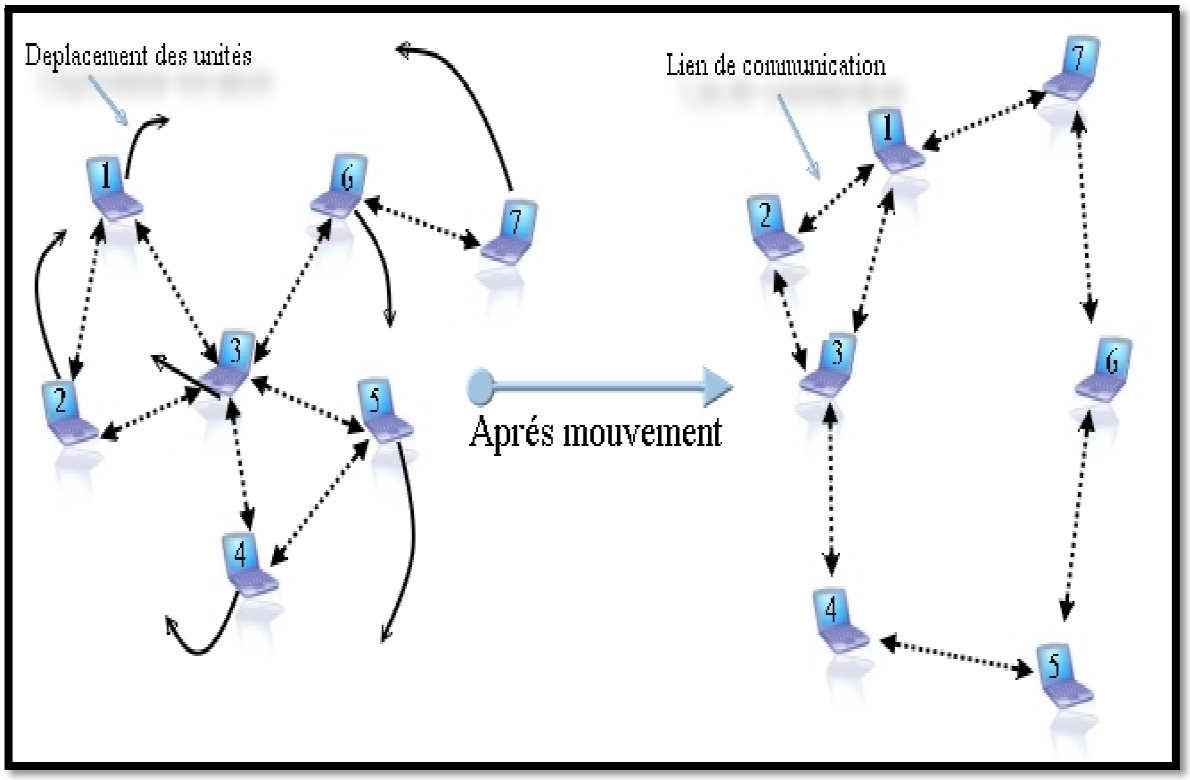


Figure 1.4 : *Le changement de la topologie des réseaux Ad Hoc*

- **Liaison à débits variables et bande passante limitée :**

Les liaisons radio présentent des débits variables et ont généralement une bande passante limitée, toujours inférieure à celle des liaisons filaires. La demande sur les applications distribuées dépasse souvent la capacité du réseau. Comme le réseau mobile est souvent une simple extension d'un réseau fixe, les utilisateurs mobiles Ad Hoc demandent les mêmes services. Cette demande ne cessera de croître avec l'augmentation des traitements multimédias et des applications basées sur les réseaux.

- **Utilisation limitée de l'énergie :**

Les nœuds d'un réseau mobile Ad Hoc sont généralement des ordinateurs portables, des téléphones portables,... Pour un bon fonctionnement du réseau, ces nœuds doiventêtre les plus autonomes que possible et ce en minimisant leur consommation en énergie. Il faut, donc de réduire autant que possible les transmissions inutiles.

- **MultiHoping « Relais » :**

C'est le fait que le chemin de l'émetteur vers le récepteur dans le réseau traverse plusieurs nœuds intermédiaires, chaque nœud agissant comme routeur. Les réseaux Ad Hoc utilisent souvent dans les communications, des chemins à relais pour cause des nœuds cachés (obstacles), de la réutilisation spatiale du médium et la conservation de l'énergie des nœuds mobiles.

1.6.3. Avantage et inconvénients des réseaux Ad hoc :

Les majeurs avantages et inconvénients sont : **[6]**

1.6.3.1. Avantage :

- **Pas de câblage :**

l'une des caractéristiques des réseaux Ad Hoc est l'absence d'uncâblage, et ce en éliminant toutes les connexions filaires qui sont remplacées par desconnexionsradio.

- **Déploiement facile :**

l'absence du câblage donne plus de souplesse, et permet dedéployer un réseau Ad Hoc facilement et rapidement. Cette facilité peut être justifiéepar l'absence d'une infrastructure préexistante permettant, ainsi, d'économiser tout letemps dedéploiement et d'installation du matériel nécessaire.

- **Permet la mobilité :**

comme l'indique leur nom, et à l'image des réseaux sans fil avec infrastructure, les réseaux mobiles Ad Hoc permettent une certaine mobilité à leurs nœuds. De ce fait, ces derniers peuvent se déplacer librement à condition de ne pas s'éloigner trop les uns des autres pour garder leur connectivité.

- **Extensible :**

l'une des propriétés les plus importantes d'un réseau Ad Hoc est la possibilité de l'étendre, et d'augmenter sa taille trés facilement et sans nécessiter trop de moyens.

❖ **Coût :**

le déploiement d'un réseau Ad Hoc ne nécessite pas d'installer des stations de base, les mobiles sont les seules entités physiques nécessaires pour déployer un tel réseau. Ce qui conduit à la réduction de son coût d'une manière significative.

1.6.3.2. Inconvénients :

❖ **Topologie dynamique:**

l'activité permanente et les déplacements fréquents des nœuds d'un réseau Ad Hoc rendent son étude trés difficile.le changement rapide de sa topologie dû aux déplacements des nœuds.

❖ **Capacités limitées (puissance de calcul, mémoire, énergie) :**

dans un tel réseau, la configuration de la portée de communication des nœuds (ce qui revient à paramétrer la puissance d'émission) est importante. En effet, il faut qu'elle soit suffisante pour assurer la connectivité du réseau. Mais plus on accroît la portée des mobiles, plus les communications demandent de l'énergie. Il faut donc trouver un compromis entre la connectivité du réseau et la consommation énergétique.

❖ **Taux d'erreur important :**

les risques de collisions augmentent avec le nombre de nœuds qui partagent le même médium. Par conséquent, plus la portée augmente, plus le risque de collisions n'est important.

❖ **Sécurité :**

un autre dilemme des réseaux Ad Hoc, et qui attire la curiosité des chercheurs et des spécialistes de ce domaine est la notion de sécurité. Un réseau Ad Hoc tel que définit précédemment ne permet pas d'assurer la confidentialité de l'information échangée entre les nœuds. Contrairement aux réseaux filaires, les réseaux sans fil sans infrastructure ne peuvent utiliser un matériel spécifique (firewall par exemple) pour empêcher les accès non autorisés au réseau.

1.6.4. Les applications des réseaux mobiles Ad Hoc :

Les applications ayant recours aux réseaux ad hoc couvrent un très large spectre, incluant les applications militaires et de tactique, l'enseignement à distance, les opérations de secours…etc. D'une façon générale, les réseaux ad hoc sont utilisés dans toutes applications où le déploiement d'une infrastructure réseau filaire est trop contraignant.

La particularité du réseau ad hoc est qu'il n'a besoin d'aucune installation fixe, ceci lui permettant d'être rapide et facile à déployer. Les opérations tactiques comme les opérations de secours, militaires ou d'explorations trouvent en ad Hoc, le réseau idéal. La technologie ad hoc intéresse également la recherche des applications civiles. On distingue entre autre:

- Les services d'urgence : opération de recherche et de secours des personnes, tremblement de terre, feux, inondation, dans le but de remplacer l'infrastructure filaire.
- Le travail collaboratif et les communications dans des entreprises ou bâtiments: dans le cadre d'une réunion ou d'une conférence par exemple.
- Les bases de données parallèles.
- Applications commerciales : pour un paiement électronique distant (taxi) ou pour l'accès mobile à l'Internet, où service de guide en fonction de la position de l'utilisateur.

1.6.5.Routage dans les réseaux ad hoc : [7]

Les protocoles de routage destinés aux réseaux mobiles Ad Hoc peuvent être classés de différentes manièresselon plusieurs critères. Ils peuvent être classés selon le type de vision qu'ils ont du réseau et les rôles attribués à ses nœuds (plat ou hiérarchique), ou encore selon l'information utilisée pour calculer les routes (vecteur de distance ou état de liens). un troisième critère peut être utilisé pour différencier entre les protocoles de routage, il s'agit de la méthode utilisée pour construire une route entre un nœud source et un nœud de destination (réactive ou proactive).La (Figure 1.5)donne une classification des principauxprotocoles proactifs, réactifs et hybrides développés ces dernières années.

1.6.5.1. LesprotocolesderoutageProactifs :

Les protocoles de routage proactifs essaient de maintenir les meilleurs chemins existants vers toutes les destinations possibles (qui peuvent représenter l'ensemble de tous les nœuds du réseau) au niveau de chaque nœud du réseau. Les routes sont sauvegardées mêmes si elles ne sont pas utilisées. La sauvegarde permanente des chemins de routage, est assuré par un échange continu des messages de mise à jour des chemins, ce qui induit un contrôle excessif surtout dans le cas des réseaux de grande taille. L'avantage de ce type de protocole est d'avoir les routes immédiatement disponibles quand les nœuds en ont besoin, mais cela se fait au coût d'échanges réguliers de messages (consommation de bande passante) qui ne sontcertainement pas tous nécessaires (seules certaines routes seront utilisées par les nœuds en général).

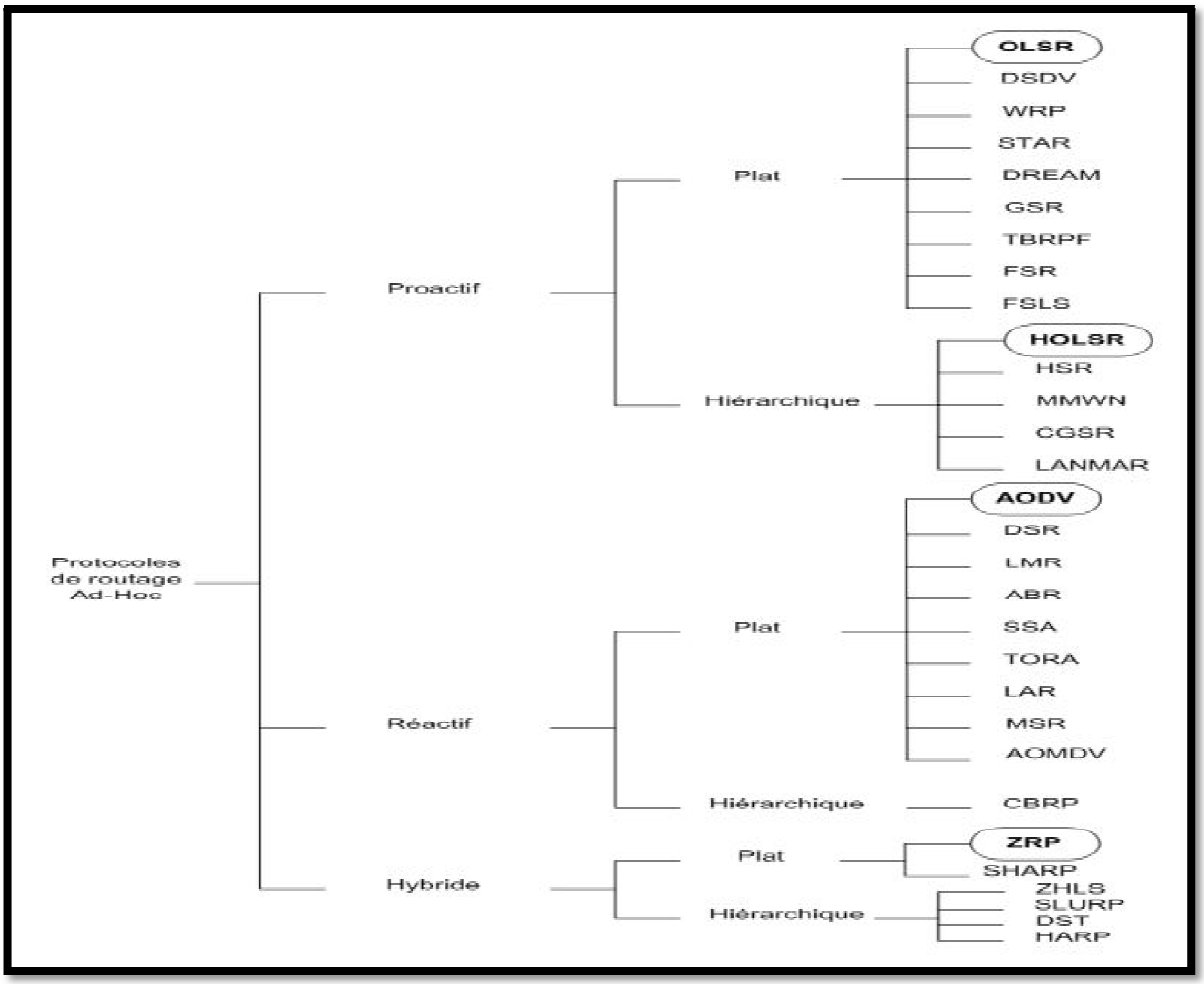


Figure 1.5: *Différents protocoles de routage Ad hoc.*

1.6.5.2. LesprotocolesderoutageRéactifs :

Les protocoles réactifs, quant à eux, ne gardent que les routes en cours d'utilisation pour leroutage. A la demande, le protocole va chercher à travers le réseau une route pour atteindreune nouvelle destination. Ce protocole est basé sur le principe de l'ouverture de route à lademande, ainsi lorsqu'un nœud veut communiquer avec une station distante, il est obligé dedéterminer une route dynamiquement. Cettetechnique permet de ne pas inonder le réseau parde paquets de contrôle et de ne conserver que les routes utilisées.

1.6.5.3. Les protocoles de routage Hybride :

Les protocoles hybrides combinent les deux approches. Ils utilisent un protocole proactif,pour apprendre le proche voisinage (voisinage à deux ou trois sauts); ainsi ils disposent desroutes immédiates dans le voisinage. Au-delà de cette zone prédéfinie, le

protocole hybridefait appel aux techniques des protocoles réactifs pour chercher des routes. Avec ce découpage,le réseau est partagé en plusieurs zones, et la recherche de route en mode réactif peut êtreaméliorée. A la réception d'une requête de recherche réactive, un nœud peut indiquerimmédiatement si ladestination est dans le voisinage ou non, et par conséquent savoir s'il fautaiguiller ladite requête vers les autres zones sans déranger le reste de sa zone. Ce type deprotocole s'adapte bien aux grands réseaux, cependant, il accumule aussi les inconvénientsdes protocoles réactifs et proactifs : messages de contrôle périodique, le coût d'ouvertured'une nouvelle route.

1.7. Sécurité des réseaux sans fil : [1]

A cause de la nature du medium utilisé, il est très facile d'intercepter les trames ,il est donc nécessaire de disposer d'un protocole de sécurité . Pour ce faire, le protocole WEP a été mis en place permettant ainsi des mécanismes de chiffrage de données et l'authentification des stations.

Ce pendant ce protocole a été largement controversé puisqu'il n'est pas tres difficile de caser les clés de chiffrement .un autre protocole a été mis en place par le Wifi alliance pour Palier a ce problème, le WPA – Wifi Protected Access -. L'IEEE aussi s'est penché sur ce déficit en créant un groupe de normalisation pour la sécurité des réseaux sans fil, le 802.11i.

1.7.1. Le WEP :

Une clé secrète est partagée entre le terminal et le réseau. La clé de chiffrement est obtenue en concaténant cette clé avec un vecteur dernière clé et décryptée par le récepteur en utilisant cette même clé.

Le chiffrement est base sur l'algorithme RC4 – Ron's Code 4 -.cet algorithme utilise la clé obtenue et un générateur de nombre pseudo-aléatoires PRNG – Pseudo – Random Number Generator- pour obtenir une séquence d'octets pseudo-aléatoires « Ksi ». Cette séquence combinée avec le message a envoyé pour trouver la séquence a envoyer. Le récepteur utilise la méthode inverse pour déchiffrer le message.

Le WEP fournit également deux méthodes d'authentification. La première est explicite et donne la possibilité à chaque station de s'associer à n'importe quel point d'accès visible. La deuxième plus sure est basée sur le partage de clé secrète .

1.7.2. WPA :

Le WPA et une recommandation de la Wifi alliance basées sur la norme 802.11i. Cette norme comble les lacunes du WEP en introduisant le choix entre divers protocoles de sécurité est une nouvelle méthode de distribution des clés. Les réseaux 802.11 i sont appelés RSN – Robust Security Network – et ils utilisent le 802.1 x pour les services d'authentification et gestion des clés. L'architecture de ces réseaux est basée sur trois élément de communication : la station qui veut être authentifiées, l'authentificateur qui est le point d'accès et un serveur d'authentification généralement RADIUS –Remote Authentification Dial – In User Server - . Les RSN interagissent avec le 802.1x en utilisant deux protocoles normalisés par le 802.11 i : TKIP – Temporel Key Integrity Protocole – et CCMP-CounterwithChipper Block Chaining Message Authentification Code Protocol -.

1.8. Conclusion :

Dans ce chapitre nous avons présenté les concepts de base, les environnementsmobiles, les caractéristiques et les applications des réseaux ad hoc. Ces environnements sont caractérisés par de fréquentes déconnexions des nœuds et des restrictions sur les ressources utilisées, surtout si tous les usagers du système sont mobiles ce qui est le cas pour les réseaux ad hoc. Ces limitations transforment certains problèmes, ayant des solutions évidentes dans l'environnement classique, en des problèmes complexes et difficiles à résoudre.

Bien que ces réseaux présentent des avantages énormes, mais malheureusement beaucoup de problèmes restent à résoudre, notamment le problème du nœud caché que nous verrons dans le chapitre suivant.

Chapitre 2

Présentation du problème du nœud caché

2.1. Introduction et problématique :

Le problème du nœud caché dans les réseaux Ad Hoc a été souvent sujet à des recherches et différentes solution ont étés proposées à différents niveaux de la couche MAC du 802.11.

Dans les réseaux 802.11, les frontières du réseau sont assez floues vu la nature du médium de transmission. Il est tout à fait possible que deux stations A et B soit accessible pour une station C mais qu'elles ne soient pas accessible mutuellement. Dans ce cas le risque de collision augmente sensiblement (Figure 2.1), Ce problème est dit : problème du nœud caché. Pour pallier à ce problème, différentes solution ont été proposées à différents niveaux de la couche MAC du 802.11.

Dans ce chapitre nous allons décrire en détail la couche MAC et la couche liaison de donnée du 802.11 ainsi que nous verrons les différentes solutions qui ont été proposé pour fixer le problème de la collision et du nœud caché.

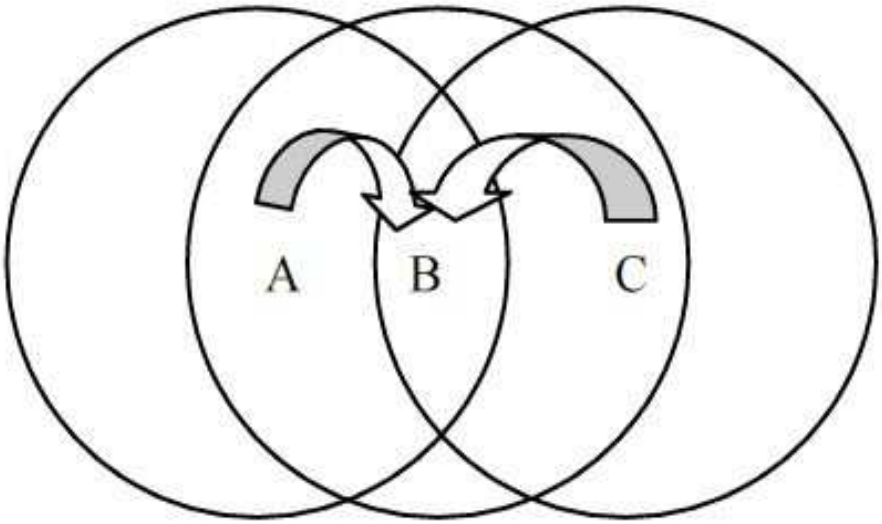


Figure 2.1: Phénomène du *Nœud caché*

2.2 Couche MAC et réseaux Ad hoc : [3]

Les protocoles MAC sont des algorithmes de gestion d'accès à un medium partagé en définissant des règles pour permettre la communication entre différents nœuds dans un ordre spécifique assurant l'efficacité des communications.

Différents protocoles MAC ont été proposé, chacun avec ces propres caractéristique et ayant des avantages et des inconvénients. Ces protocoles peuvent être comparés se basant sur les critères suivants :

- **Délai** : c'est le temps nécessaire à un paquet pour atteindre sa destination en prenant en considération le temps d'attente dans les files d'attente et les délais de retransmission.
- **Débit** : les protocoles MAC sont généralement comparés en utilisant leurs efficacités d'utilisation du medium. Ce qui correspond à la capacité du medium divisée par les données transmises. Cette valeur augmente tant que le nombre de collision et retransmission se réduit.
- **Equité** : ce qui correspond à la capacité de distribuer le medium de façons équitable entre les terminaux communicants.

  Consommation d'énergie : C'est un point critique de tous les périphériques mobiles ce qui doit être pris en compte dans les protocoles MAC.

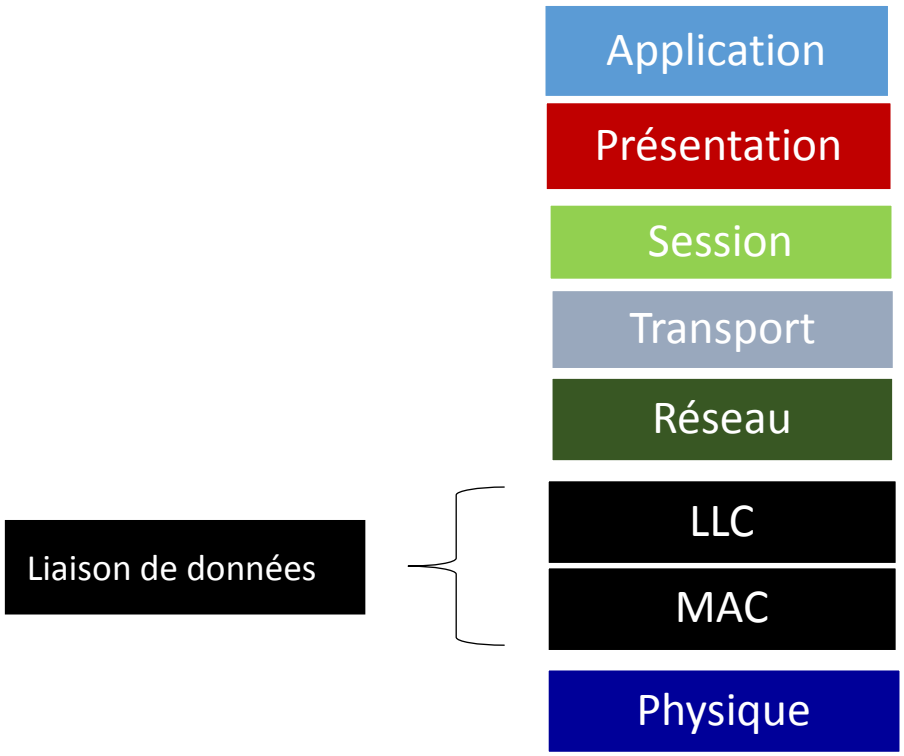


Figure 2.2: La sous couche MAC du 802.11 (Modèle OSI)

2.3. Classification des protocoles MAC : [3]

Les protocoles MAC sont classifies dans deux grandes catégories : les protocoles distribué qui peuvent être utilisés dans n'importe quelle architecture réseau (réseaux Ad hoc inclus) et les protocoles centralisés qui peuvent être mis en place que dans les réseaux centralisés. Les protocoles distribués utilisent des techniques aléatoires d'accès au medium.

2.4. La couche liaison de données du 802.11 : [4]

Le 802.11 définit seulement une partie de cette couche qui est le MAC 802.11 encapsulé par partie-Logical Link control(LLC)- définit par la norme 802.2.

2.4.1 Logical Link Control LLC : [4]

La norme 802.2 définit une couche de services de niveau liaison commune à tous les réseaux 802. Elle fournit deux types de services :

- Contrôle de flux.
- Reprise sur erreur.

Il existe trois type de LLC définit :

- LLC 1 : correspond à un service en mode sans connexion sans acquittement de données.
- LLC 2 : correspond à un service en mode avec connexion avec acquittement de données.
- LLC 3 : correspond à un service en mode sans connexion avec acquittement de données.

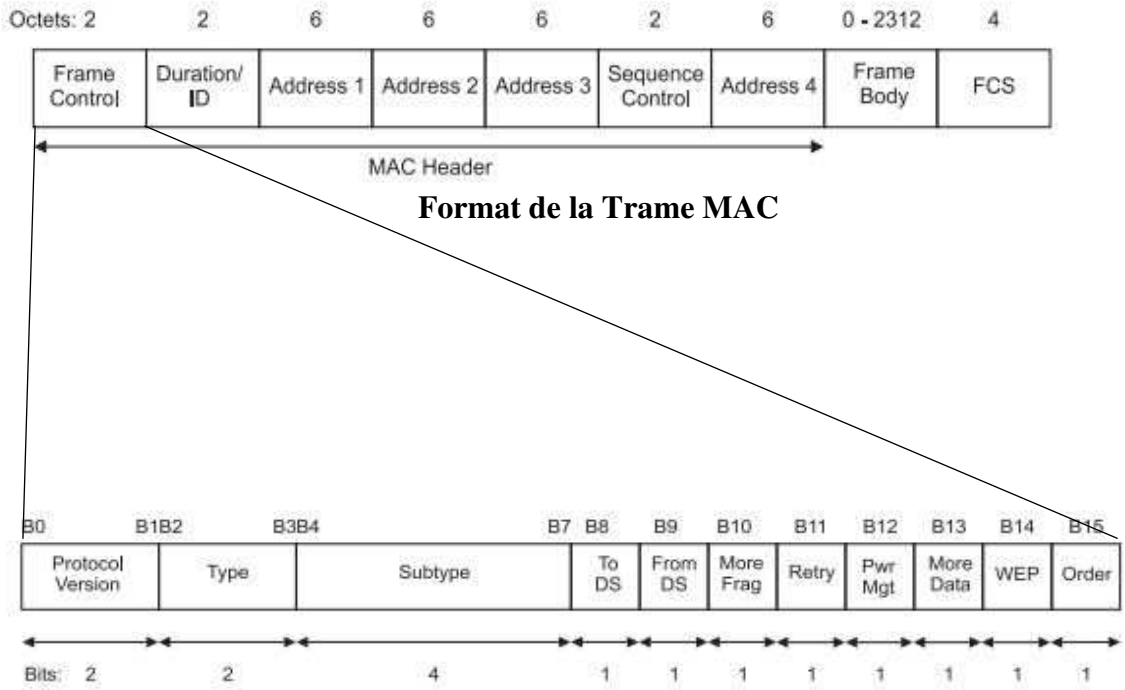
Le 802.11 utilise le LLC pour garantir une fiabilité des transmissions. Les données du niveau LLC sont structurées sous la forme d'un LPDU (LLC Protocol Data Unit).Une trame LLC est encapsulée dans la trame de niveau inférieur (MAC).le LPDU correspond donc au champ de données de la trame MAC.

DSAP	SSAP	Contrôle	Données

Trame LLC

2.4.2 Les trame du 802.11 :

2.4.2.1. Format général de la trame :



Format de la Trame MAC

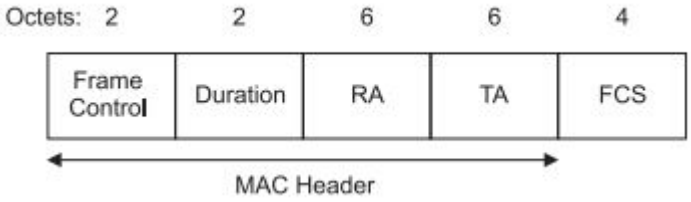
Durée/ID : utiliser généralement pour calculer le NAV mais peut avoir d'autres significations.

Champs d'adresses :La trame contient 4 champs d'adresses qui peuvent avoir plusieurs utilisations selon le type de la trame. En général l'adresse 1 correspond à l'adresse du récepteur et l'adresse 2 celle de l'émetteur.

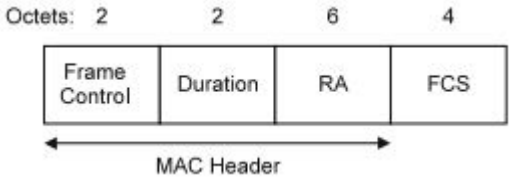
Le corps de la trame CRC sur 4 octets. **CRC- Cyclique Redundancy Check.**

Il existe trois types de trame **[2]** :

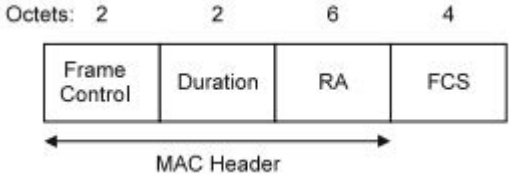
- Les trames de **données**.
- Les trames de **gestion**, transmises de la même façon que les trames de données pour l'échange d'information de gestion.
- Les trames de **contrôle**, pour contrôler l'accès au support **(RTS, CTS, ACK).**



Trame RTS



Trame CTS



Trame ACK

2.4.3 MAC 802.11 : [3]

Le 802.11 ne s'écarte pas de manière radicale des normes IEEE puisqu'il adapte les réseaux Ethernet filaire aux liaisons sans fil. Il est appelé parfois par abus de langage Ethernet sans fil. En effet, le MAC 802.11 fournit les services suivants : la délivrance des données de façon fiable, le contrôle d'accès au médium, le contrôle des erreurs, la gestion de la fragmentation, le réassemblage, la mobilité et l'énergie. Il définit deux méthodes d'accès différentes : DCF et PCF.

DCF- Distributed Coordination Function : c'est une méthode d'accès qui donne la même priorité aux stations pour accéder au support .Elle est utilisée pour la transmission des trames asynchrones.

PCF – Point Coordination Function : c'est une méthode d'accès qui donne la priorité aux trames temps réel nécessitant une bonne qualité de service. Elle est basée sur l'interrogation des stations par le point d'accès.

2.4.3.1. Protocole ALOHA : [8]

En 1970, Norman Abramson a proposé le protocole ALOHA. Dans ce protocole un nœud désirant émettre des données le fait immédiatement. Le problème de ce protocole est qu'une station ne se préoccupe pas de l'état du réseau avant d'émettre quand elle a une donnée à transmettre, elle le fait peu importe si elle va entrer en collision avec une émission déjà en cours.

2.4.3.2. Protocole MACA : [9]

Un raffinement de l'accès ALOHA a été développé sous le nom de protocole d'accès multiple à évitement de collisions,MACA : Multiple Access withCollision Avoidance.
Suivant ce protocole, l'émetteur, avant de transmettre, envoie une courte trame au récepteur, dite trame RTS (RequestTo Send). A la réception de la trame RTS, le récepteur envoie une trame CTS (Clear To Send) à l'émetteur. Cettetrame CTScomporte l'adresse de l'émetteur, l'adresse du destinataire et la taille totale de la trame (recopiée à partir de la trameRTS). Lorsque l'émetteur reçoit la trame CTS il commence à émettre la trame complète.Tout émetteur proche de l'émetteur qui détecte la trame RTS reste silencieux jusqu'à l'apparition de la trame CTS.Une fois la trame CTS envoyée, tous les émetteurs qui la reçoivent, qu'ils soient proches de l'émetteur ou du récepteur,restent silencieux durant le temps nécessaire à la transmission de la trame complète. On rappelle que la taille de cettetrame est indiquée dans la trame CTS.
Avec ce protocole les seules collisions qui peuvent survenir concernent les trames RTS. Si une collision survient surune trame RTS, le destinataire n'enverra jamais de trame CTS à l'émetteur et ce dernier, après un temps aléatoireréémettra une trame RTS.

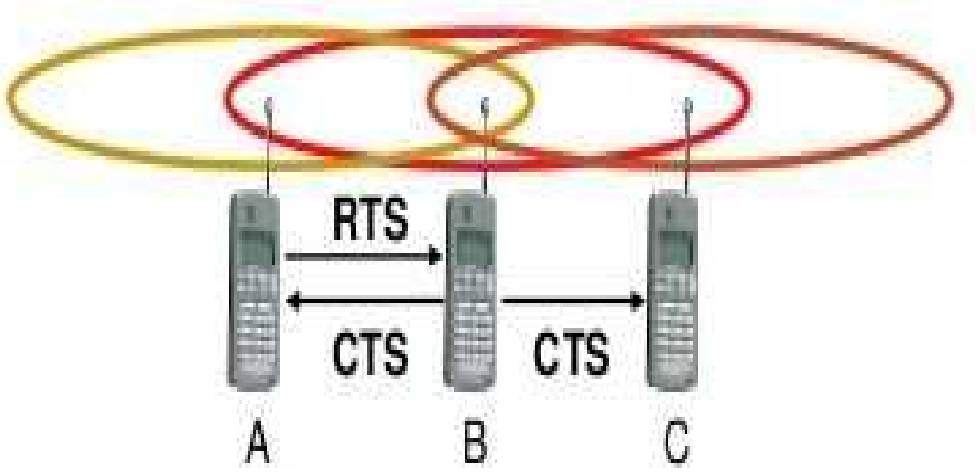


Figure 2.3: Déroulement du protocole MACA.

2.4.3.3. Protocole MACAW : [8]

C'est une amélioration du protocole MACA et c'est le protocole de base du 802.11 basé sur CSMA/CA. C'est un protocole à 4 étapes RTS – CTS – Données – Accusé de réception (ACK).

L'accès au medium se fait comme suit : quand un nœud veut émettre, il attend que le medium devienne libre pendant une période DIFS. Puis il choisit un temps aléatoire « backoff ». Ce temps est décrémenté tant que le medium reste libre et il est bloqué quand le medium devient occupé. Quand le backoff expire, le nœud envoie un RTS à la destination. Si cette dernière est prête à recevoir des données après un SIFS. Dès que le nœud émetteur recroit le CTS, il envoi la donnée âpres un SIFS et attend un ACK depuis la destination. Si l'émetteur ne recroit pas d'ACK, il retransmet le paquet. S'il ne recroit pas de CTS, l'émetteur présume que la charge sur le medium est grande et double son backoff pour les prochaines transmissions afin de réduire le risque de collision. Le durée de la transmission en cours est inclut dans le header au paquet de RTS et CTS, quand les autre nœuds reçoivent l'un

de ces paquets ils mettent à jour leur NAV et attendent son expiration avant de pouvoir transmettre à leur tour.

MACA	RTS	CTS	Données		
MACAW	RTS	CTS	DS	Données	ACK

Comparaison entre MACA et MACAW

2.4.3.4.Protocole CSMA/CA : [2]

En effet, tout comme Ethernet, le 802.11 utilise un accès multiple avec écoute de la porteuse (CSMA – carrier sense multiple access) pour contrôler l'accès au médium. Cependant, il utilise l'évitement de collision (CSMA/CA – Collision Avoidance) au lieu de la détection de la collision (CSMA/CD – Collision Detection) utilisé par les réseaux Ethernet et ceci en important un accusé de réception pour chaque paquet (ACK – acknowledgment).le temps d'accès au support est divisé en intervalles de temps.

- **Notion d'opération atomique (dialogue) :**

Une opération atomique regroupe toutes les trames envoyés par la station source vers une destination jusqu'à s'assurer de la bonne transmission d'une seule trame de données. Dans le cas général, opération atomique = trame de données + trame ACK.

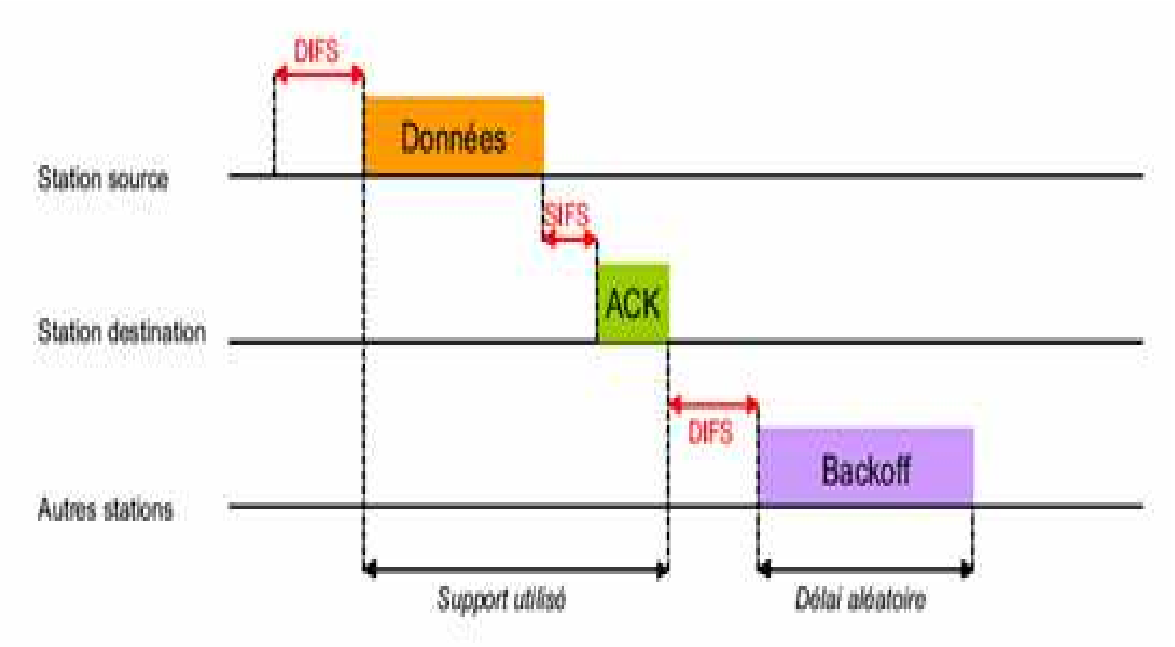


Figure 2.4 : *Processus de transmission des trames.*

SIFS – Short Inter-Frame Spacing : C'est l'intervalle de temps utilisé entre deux transmissions de la même opération atomique.

PIFS-PCF Short Inter-Frame Spacing : C'est l'intervalle de temps utilisé par le point d'accès.il lui permet d'accéder en priorité au support.

DIFS-DCF Short Inter-Frame Spacing : C'est l'intervalle de temps utilisé par les stations entre deux opérations atomiques différentes pour tenter d'accéder au support.

NAV : C'est un temps calculé selon la trame en cours d'émission pour permettre aux stations de différer leur transmission.

Le délai aléatoire : C'est un délai d'attente aléatoire attribué par l'algorithme du back-off a chaque station en attente d'émission lorsque le support devient libre. Cet algorithme permet d'éviter les collisions dans le cas ou plusieurs stations tentent d'émettre en même temps.

- **Déroulement de l'algorithme CSMA/CA : [1]**

Lorsqu'une station veut transmettre une trame de données, elle écoutera le canal avant d'émettre

- ✓ Si aucune activité n'est détectée pendant une période de temps correspondant à un DIFS, transmettre la trame immédiatement.
- ✓ Si le support est occupé, continuer de l'écouter jusqu'à ce qu'il soit libre. Quand le support devient disponible, retarder encore sa transmission en utilisant l'algorithme de Back-off avant de transmettre ses données.
- ✓ T_back-off = $[2^{2+I} * rand()]* T\_slot$
  - ➢ i: nombre de tentatives consécutives d'une station pour l'envoi d'une trame.
  - ➢ rand(): une variable aléatoire uniforme comprise entre [0, 1]

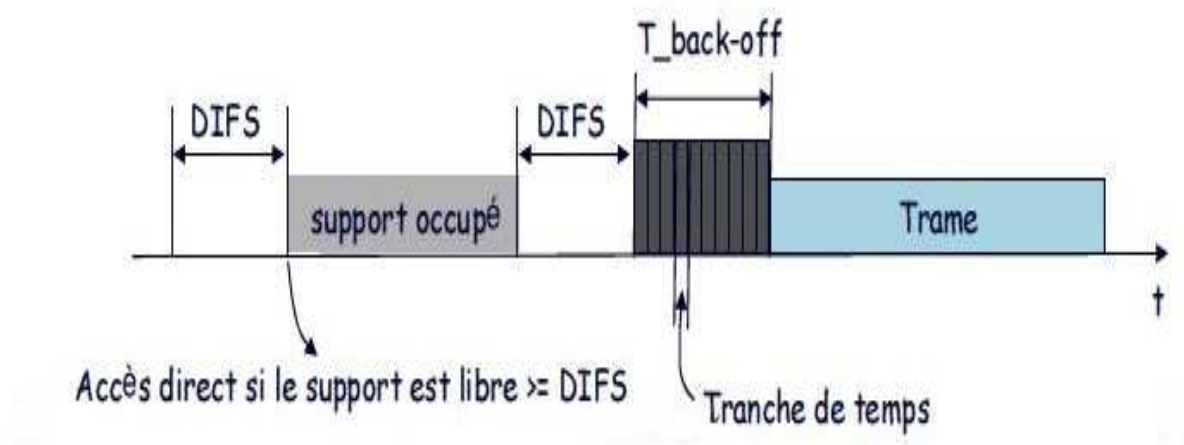


Figure 2.5: *Algorithme CSMA/CA*

2.4.3.5. Régulation du débit de transmission : [10]

Pour pallier au problème du nœud caché, les chercheurs se sont posés la question de la fiabilité du MAC 802.11 et ainsi au lieu d'éviter le problème, ils ont pensé à optimiser les performances du réseau grâce à différents algorithme se basant sur la régulation des flux de sorties qui ont étés mis en place :

ARF – Auto Rate Fallback - : est largement implémenté dans les produits commerciaux 802.11. ARF choisit d'augmenter ou de réduire le débit de transmission selon le taux de sucées ou d'échec des transmissions successives.

RBAR –ReceiverBased Auto Rate - : le récepteur sélectionne un débit de transmission adéquat a la qualité de canal mesuré à partir du paquet RTS reçu et ceci en utilisant le champ STR (Signal to Noise Ratio) prévu à cet effet.

2.4.3.6. La détection passive : [10]

Cette technique de détection de nœuds cachés est possible lorsqu'un nœud voisin au nœud effectuant la détection est en communication avec un nœud caché à ce dernier. L'avantage de cette technique est qu'elle peut être implémentée sans flux de contrôle : supplémentaire sur le réseau et ceci deux cas :

Avec RTS/CTS : un nœud « 0 » recevant un RTS de la part d'un nœud « 1 » mais destiné en réalité au nœud « 2 » conclut que le nœud « 2 » lui est probablement caché s'il ne reçoit pas de CTS de la part de ce dernier après la période se repense nécessaire.et ce nœud « 2 » est confirmé comme cache si cette opération de répéter un certain nombre de fois et ceci afin d'être sûr de la raison de la non réception du paquet. Le contraire est également possible, c'est-à-dire qu'un nœud « 0 » recevant un CTS de la part du nœud « 1 » mais qui est destinés au nœud « 2 » est ceci sans avoir reçu au préalable. Le RTS correspondant du nœud « 2 », met ce dernier dans les listes des nœuds cachés probables. Si l'opération se répète un certain nombre de fois, le nœud « 2 » est confirmé alors comme nœud caché par rapport au nœud « 0 ».

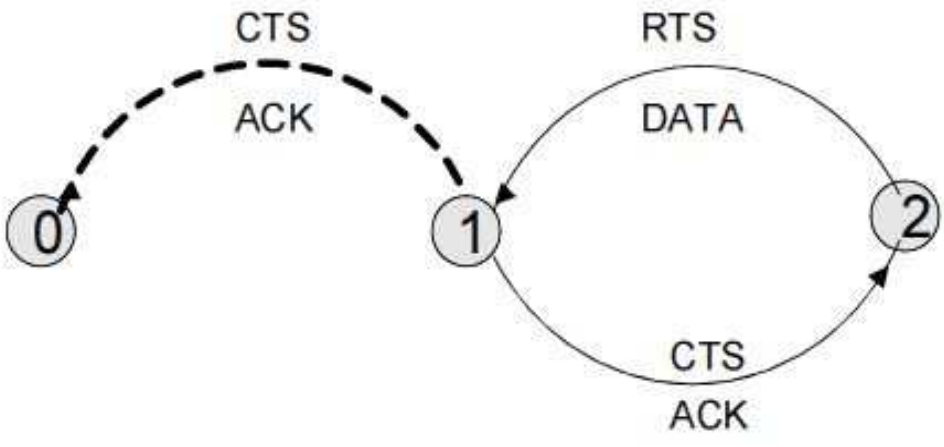


Figure 2.6 : *Détection passive avec RTS/CTS*

Sans RTS/CTS : un nœud « 0 » recevant un paquet de donnée de la part d'un nœud « 1 » mais destiné en réalité au nœud « 2 » s'attend à recevoir un ACK de « 2 » vers « 1 » après une certaine période.Il pourra conclure que le nœud « 2 » lui est caché s'il ne reçoit pas l'ACK.Et ce nœud est confirmé comme caché après un certain nombre d'ACK non reçu. Comme le premier cas, le contraire est envisageable également, c'est-à-dire que la réception d'un ACK sans avoir reçu le paquet de données correspondant nous permet de détecter un probable nœud caché.

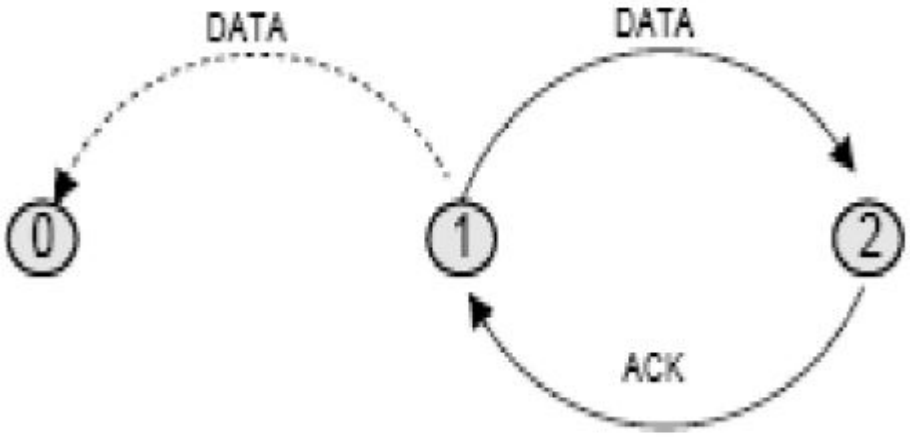


Figure 2.7 : *Détection passive sans RTS/CTS*

2.4.3.7. La détection active : [10]

La détection active est une autre technique initiée par l'émetteur. Un nœud « 0 » qui veut connaitre ses nœuds cachés envoie un paquet ARequest (Active détection Request) à tous ces voisins. Le nœud « 1 » recevant ce paquet envoi un autre type de paquet AProb a ces voisins qui lui répondent par un ACK. Si le nœud « 0 » entend l'ACK émis par le nœud « 2 » - voisin du nœud « 1 » -, il conclut que ce dernier n'est pas un nœud caché par contre s'il n'entend pas l'ACK après le délai nécessaire à la réception du paquet AProb et de la réception de l'ACK, il conclut que le nœud « 2 » est potentiellement un nœud caché, si cette opération se répète un certain nombre de fois, le nœud « 2 » est ajouté à la table des nœud cachés du nœud « 0 ».

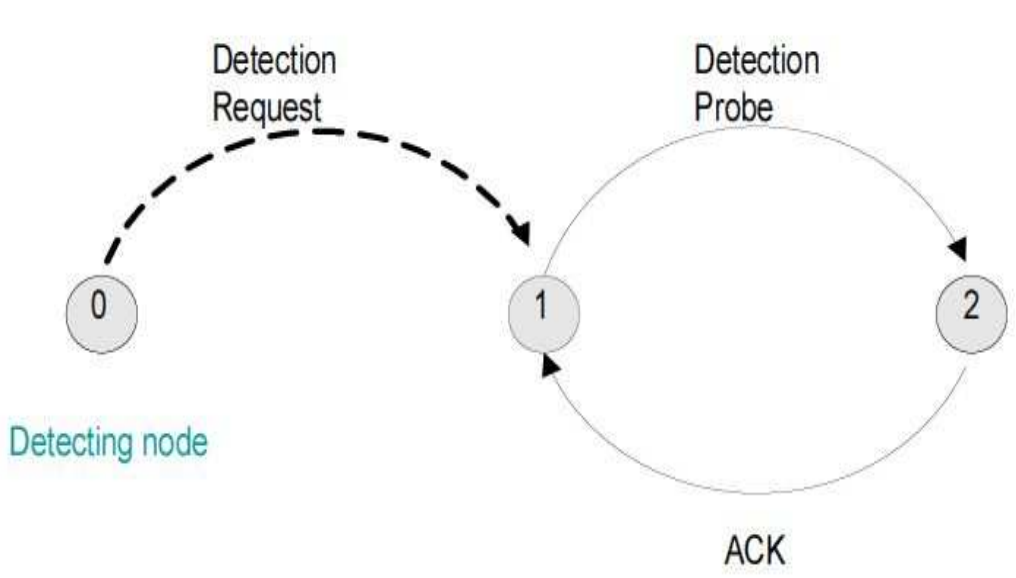


Figure 2.8: *Détection active*

2.5. Conclusion :

Ce chapitre a étais consacrer à la présentation du problème du nœud caché ainsi que la couche MAC et la couche liaison de données et leurs fonctionnalités.

Les différents mécanismes d'évitement de collision et de détection de nœud caché étaient présentés.

Nous allons détailler le mécanisme de détection passive avec RTS/CTS dans le chapitre suivant.

Chapitre 3

Modélisation et Simulation et étude de performances

3.1. Introduction :

Dans le cadre de notre travail et après étude des différentes techniques de détections des nœuds cachés, nous avons opté pour la détection passive.A cet effet nous proposons la démarche suivante :

1- Lancer la détection passive.
2- Recenser les voisins des nœuds cachés.
3- Appliquez le mécanisme sleep/wakeup sur l'ensemble des voisins.
4- Réveiller les voisins après fin de communication du nœud caché.

A cette étape nous analyserons les résultats de simulation.

Partie Modélisationde notre approche:

Nous avons opté sur la modélisation UML pour modéliser notre approche en utilisant le diagramme de séquence.

3.2. Définition UML [17].:

UML (Unified Modeling Language) est une méthode de modélisation orientée objetdéveloppée en réponse à l'appel à propositions lancé par l'OMG (Object Management Group)

dont le but de définir la notation standard pour la modélisation des applications construites àl'aide d'objets. Elle est héritée de plusieurs autres méthodes telles que OMT (Object ModelingTechnique) et OOSE (Object Oriented Software Engineering) et Booch.

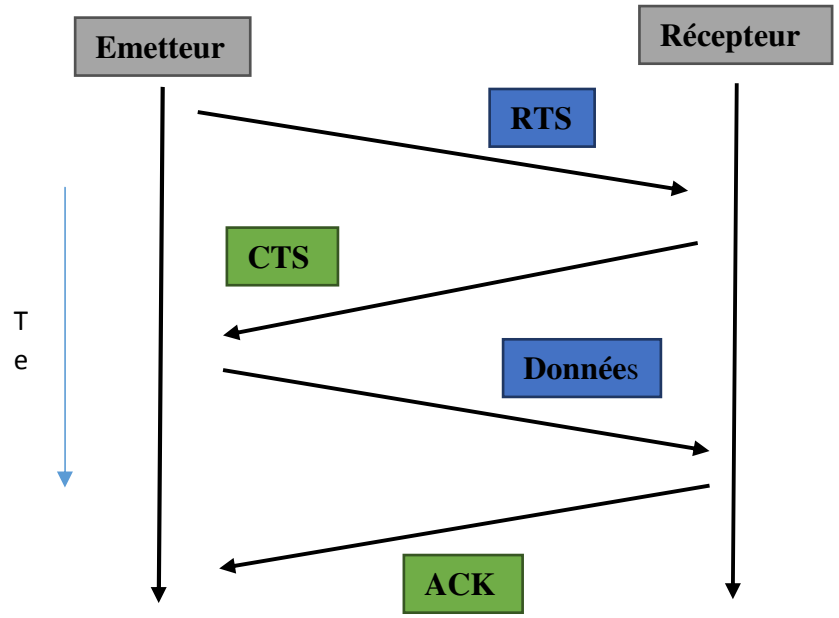


Figure 3.1: diagramme de *Séquence d'envoi/réception sans les fonctions sleep() et wakeup().*

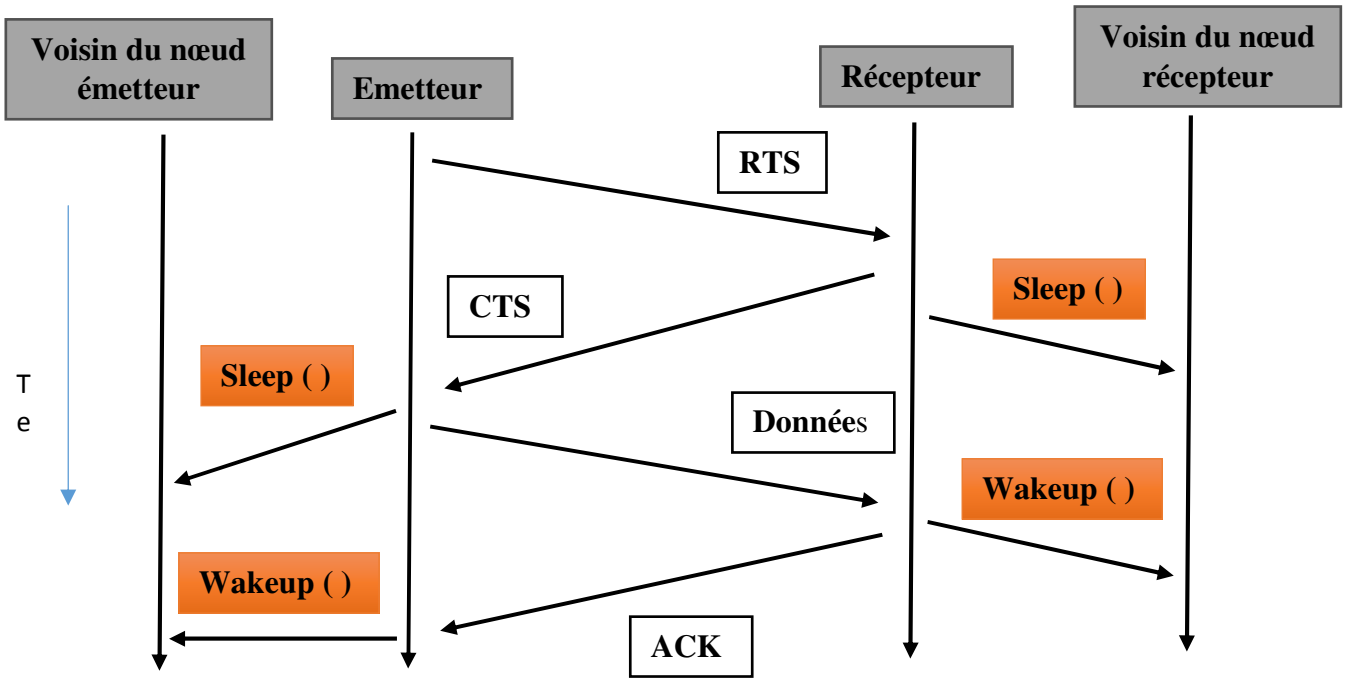


Figure 3.2: diagramme de *Séquence d'envoi/réception avec sleep() et wakeup().*

Partie simulation de notre approche

3.3. Environnement du travail :

Le simulateur réseau NS (Network Simulator) est un simulateur à événement discrets orienté objet **[11]**, basée sur le simulateur réseau REAL **[12]**. Au départ, la version 1.0 de NS a été développée au Laboratoire National de Lawrence Berkeley (LBNL) par le groupe de recherche réseau. Son développement fait maintenant partie du projet VINT (Virtual Inter Network Testbed) sous lequel la version 2.0 est sortie. Il permet à l'utilisateur de définir un réseau et de simuler des communications entre les nœuds de ce réseau. NS-2 utilise le langage OTCL (Object Tools Command Language), dérivé objet de TCL (Tools Command Language). A travers ce langage, l'utilisateur décrit les conditions de la simulation : Topologie de réseau, caractéristiques des liens physiques, protocoles utilisés, communications…etc.

Nous allons à présent détailler les outils logiciels ainsi que les outils complémentaires installés afin de réaliser notre projet.

3.4. Présentation du simulateur NS-2

NS est un outil logiciel de simulation de réseaux informatiques. Il est principalementbâti avec les idées de la conception objet **[13]**. Il est devenu un standard de référence en ce domaine. L'avantage de ce logiciel, c'est qu'il est disponible sur Internet, son utilisation est gratuite et il est compatible avec les systèmes Windows et Unix.

3.4.1. Architecture

L'architecture de ns est trés complexe et nous ne présenterons que les parties surlesquelles nous ont permis de mener à bien notre projet.Une grande partie du travail a été

de se documenter, de chercher et d'analyser le logiciel afinde mieux comprendre son fonctionnement, D'abord le principe général et l'interaction entreles langages C++ et TCL, puis plus en profondeur, l'organisation en classes C++ et finalementles structures de données. NS est un simulateur écrit sur la base du langage C++, avec au devant un interpréteur OTcl.

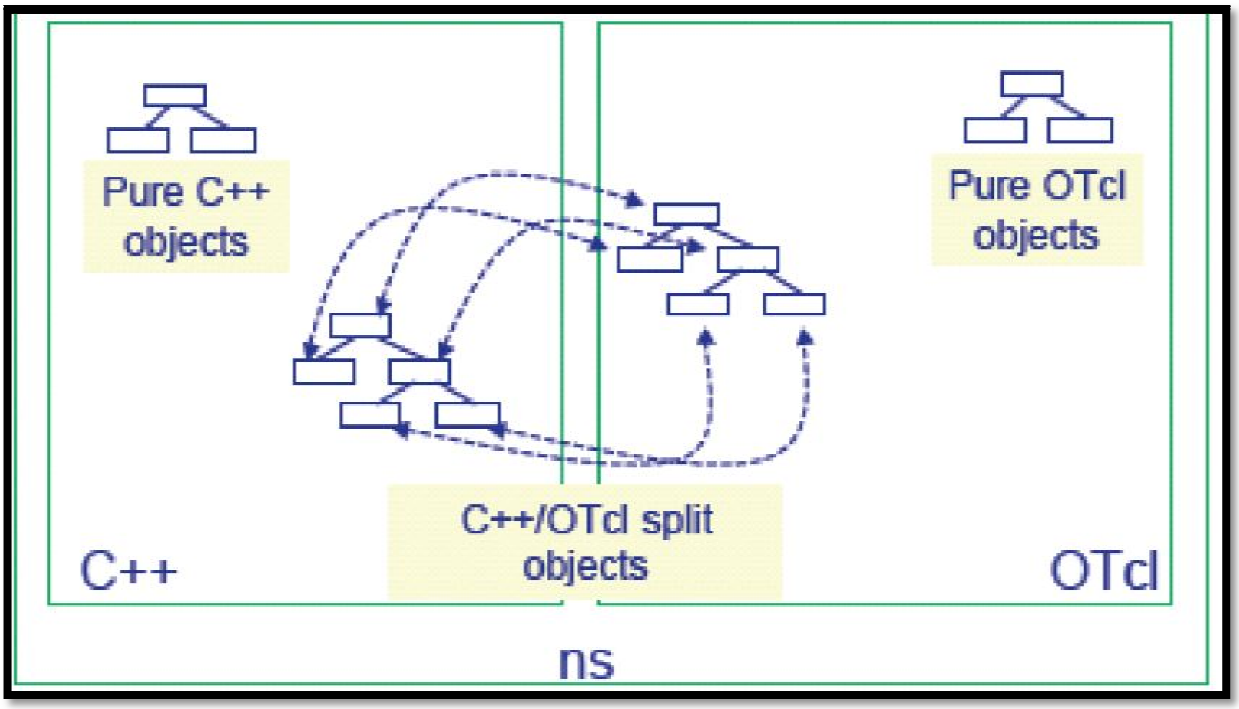


Figure 3.3: *Organisation des classes en NS*

Le coeur du logiciel est un ensemble de classes C++ qu'il est nécessaire de compiler pourconstruire l'exécutable. C'est grâce à ces classes que sont créés les objets qui sont aprèsutilisés pour simuler le fonctionnement d'une application réseau.Par exemple, les composants d'un réseau, un noeud, une couche du modèle OSI ou méme unpaquet sont en fait des objets C++ qui sont définis par des classes.Il contient les fonctionnalités nécessaires à l'étude des algorithmes de routage , des protocolesde transport, de réservation, des services intègres, des transmission, d'ordonnancement et depolitiques de gestion de files d'attente pour

effectuer des études de contrôle de congestion. La liste des catégories des principaux composants actuellement disponibles dans NSest :

- Application Web, ftp, telnet, générateur de trafic (CBR,…),
- Transport TCP, UDP, RTP, SRM,
- Routage statique ou dynamique (vecteur de distance),
- Routage Multicast
- Gestion de file d'attente : RED, DropTail, Token buket, etc
- Discipline de service : CBQ, SFQ, DRR, Fair Queueing,
- Système de transmission : CSMA/CD, CSMA/CA, lien point à point.

3.4.2. Le fonctionnement de NS-2 :

L'utilisation de NS-2 pour un scénario donné nécessite schématiquement lesétapes suivantes *(voir figure 3.4):*

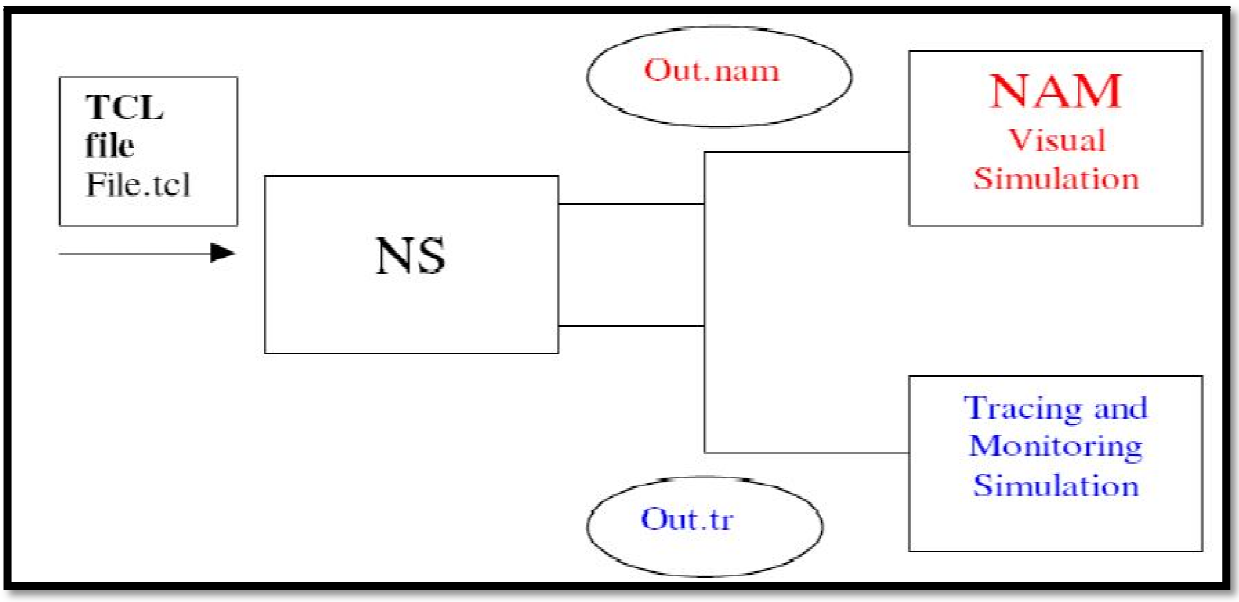


Figure 3.4: *Les principales étapes de simulation sous NS.*

3.4.3. La création de fichier de paramétrage :

Ce fichier se présente sous la forme d'un script écrit dans le Langage interprété TCL. Il décrit les différents aspects du scénario :

- Le nombre et le déplacement des unités mobile
- Le choix des différents protocoles pour chaque couche de chaque noeud
- Le nombre, le type et la durée de divers transferts de données entre ces noeuds
- Etc,…

3.4.4. Fichier traces :

Elle reproduit en interne le fonctionnement du scénario décrit précédemment etgénère un fichier de traces. Ce dernier contient l'information jugée utile, écrite dans un formatstandardisé. Le contenu du fichier de trace consiste en une liste d'évènements qui se déroulèspendant la simulation.

3.4.5. L'analyse du fichier de trace :

Cette analyse peut être effectuée au moyen d'analyseurs syntaxiques ou d'outil devisualisation comme Nam (Nerwork Animator). Le Nam est un outil d'animation basésurTcl/TK, son modèle théorique a été non seulement crée pour lire une large ensemble de données d'animation, mais suffisamment extensible pour être utilisé quelques soit le type de réseau simulé (fixe, mobile ou mixte). Ce qui permet de visualiser tout type de situation possible. A chaque création de la topologie réseau c'est à dire les nœuds et les liens, NS écrit ces informations dans un autre type de fichier trace généré a la fin de la simulation nommé « name_trace». Ce dernier, enregistre tout ce qui a une relation avec le graphisme : forme des nœuds, leur taille, leur couleur … etc.

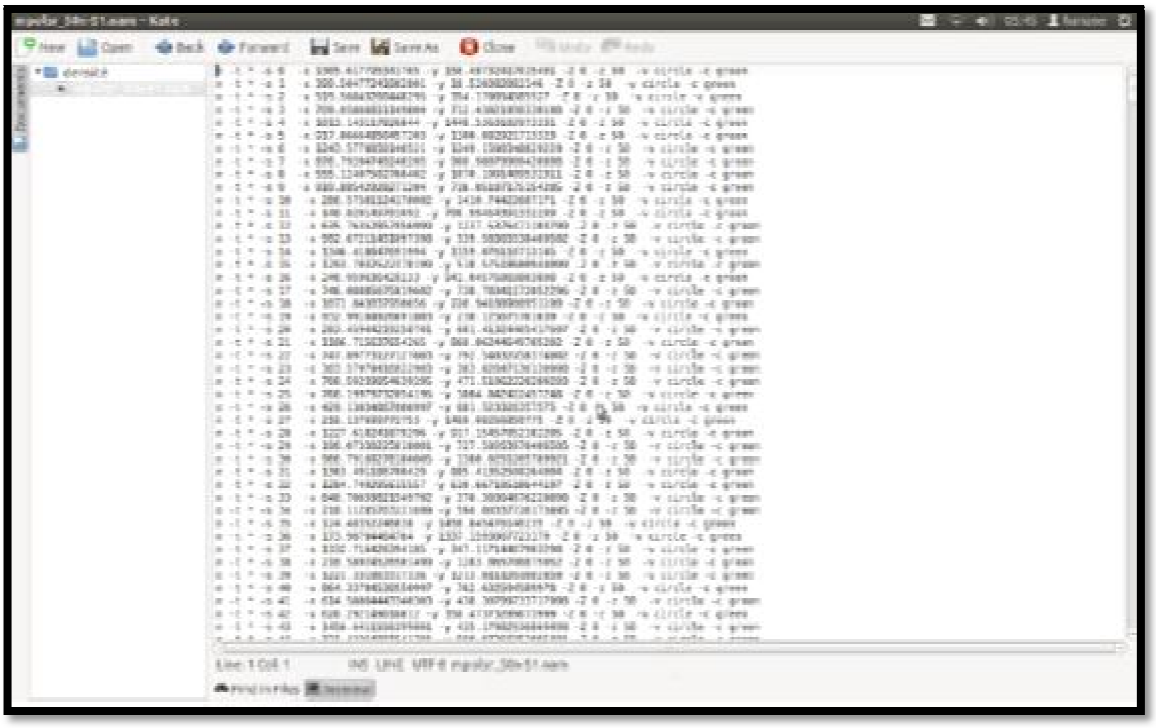


Figure 3.5: *Fichier NAM.*

3.4.6. Le programme AWK :

Cet outil est utilisé dans la simulation comme filtre du fichier trace. C'est un langage demanipulation de chaîne de caractère, disponible sur la plupart des systèmes Unix. AWK lit lefichier trace (fichier d'entré ligne par ligne) puis sélectione les lignes à traiter en lesdécoupant en champs $1 $2 $3 pour faciliter l'affichage du graphe.

3.5. Installation et configuration :

Pour étudier les performances dumécanisme de détection passive avec RTS/CTS, nous avons passé par deuxétapes : l'installation du simulateur réseau NS et l'intégration du

mécanisme dans cesimulateur, Il est important de noter que nous avons travaillé sous l'environnement Linux :Ubuntu 12.04.

3.5.1 Procédure d'installation de ns2 : paquet ns-allinone-2.35 :

1-Télécharger l'archive de la version ns-allinone-2.3 **[14]**

2- Extraction dans le répertoire home

3- Lancer la commande «./install »

4- Une fois l'Install terminé, il faut compiler ns– Commande « make » (le makefilecontient la suite d'opérations, les dépendanceset les librairies nécessaires à la compilation)

5- L'installation est alors terminée, pour la vérifier, lancer la commande« ./validate », un scripte qui permet de tester l'installation est lancé et validera ounon l'installation.

6- Pour une utilisation plus commode, nous avons exporté les variablesd'environnement pour lancer les commandes nécessaires par exemple lacommande ns.

3.6. Notre Proposition :

Nous avons proposé de mettre en place le mécanisme de détection passive avec RTS/CTS cela en ajoutant la fonction Hidden_detect() qui a pour rôle d'ajouter les nœuds cachés dans une table et les afficher après la fin de chaque simulation. Ainsi, nous avons proposé d'ajouter deux fonction sleep() et wakeup() la première met tous les nœuds voisins en mode inactive sauf l'émetteur et le récepteur. La deuxième fonction intervient lorsque l'opération d'envoi/réception des données s'achève.

Cela se fait essentiellement dans la couche MAC 802.11 (mac/mac 802_11.h et mac/mac802_11.cc).

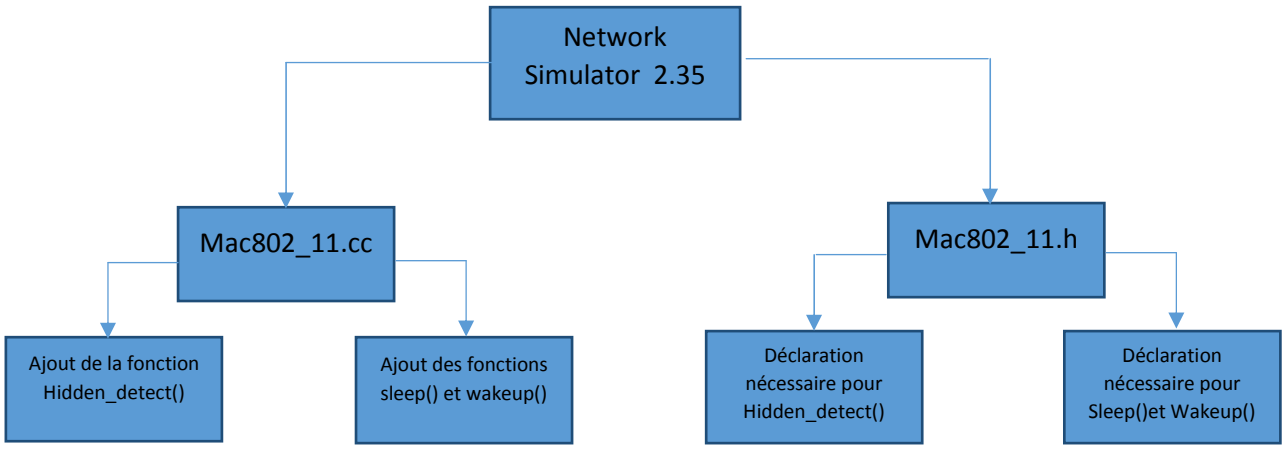


Figure 3.6: *les différentes étapes de modification sous NS2.*

3.7. Le choix du Protocole de routage

Différents protocoles pourraient être installés/utilisés afin de tester leurfonctionnement dans un réseau ad hoc. La plupart des laboratoires développant des protocolesréseaux, fournissant les fichiers et la documentation nécessaire pour installer leur protocole etles tester sous NS-2.

Il convient cependant de trouver un protocole où la source du transfert possèdesuffisammentd'informations sur le réseau et sa topologie.

Nous avons choisid'utiliser le protocole AODV **[15] [16]**.

Une modification est apporter au code source de ce protocole en ajoutant une fonction appeler Un_saut( ) qui a pour rôle de limiter le fonctionnement de sleep et wakeup sur les nœuds voisin uniquement. (Voir Annexe A).

3.8. Simulation :

Dans cette partie, nous présentons les scénarios de simulations que nous avons réalisé avec le simulateur NS-2.

Nous schématisons les résultats obtenus à l'aide de graphes et tables que nous exposons etinterprétons. Par la suite, Nous comparons taux d'énergie consommer avec les deux fonctionsleep() et wakeup() et sans leurs présence.

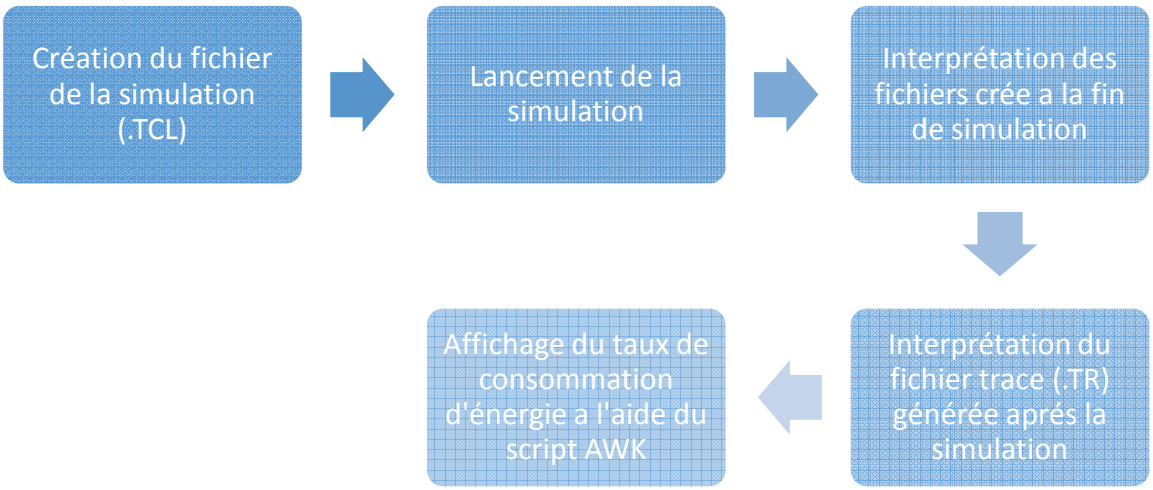


Figure 3.7: *Séquences d'exécution d'un scénario.*

3.8.1. Topologie d'étude :

Le réseau considéré est composé de 5 noeuds*(ce paramètre sera varié)* déployés sur une surface de 2000mx2000m. Nousferons des simulations d'une durée de 10 secondes *(Voir Table 1).* Il est important de noterque nous avons choisi ces paramètres à cause des limitations matérielles. En effet, les tests ontété réalisés sur un ordinateur portable personnel *(voir les caractéristiques dans le Table 2),*pour un plus grand scenario en termes de nombre de nœudset de temps de simulation, nousavons besoin d'une machine beaucoup plus puissante.

Nombre de nœuds	5, 7, 10
Durée de la simulation	10 seconds
Protocole	AODV
Surface de simulation	2000x2000 mètres

Tableau 1 :*paramètres de la topologie d'étude.*

Processeur	2.13 GHZ
Mémoire	2 Go
Système d'exploitation	Ubuntu 12.04

Tableau 2 :*caractéristiques du pc de la simulation.*

3.8.2. Paramètres de la simulation :

Avant de lancer la simulation de scénario, nous devons ajuster et fixer certainsparamètresqui vont constituer le contexte de notre simulation.Nous avons supposé que tous les nœuds du réseau sont équipés par des interfaces decommunication IEEE 802.11, et que chaque nœud possède une zone de transmission de 250m. En effet, c'est la configuration de la majorité des carte réseau WIFI actuels. Commemodèle de propagation d'ondes, nous avons utilisé le "*Two Ray Ground model* " qui prédisentla puissance reçue comme une fonction déterministe de la distance. Il représente la portée dela communication comme un cercle parfait autour de l'émetteur *(le script qui décrit laconfiguration du réseau et qui analyse les résultats de la simulation est fourni en annexe).*

Nous avons choisi de modéliser la communication entre les nœuds en utilisant le trafic CBR *(constant Bit Rate)* sur UDP, où chaque source génère des paquets de 512 octets avec untaux de 4 paquets par seconde Un total de 8 connexions a été *généré (le script correspondantest fourni en annexe)*

3.8.3. Scénario 1 (5 Nœuds) :

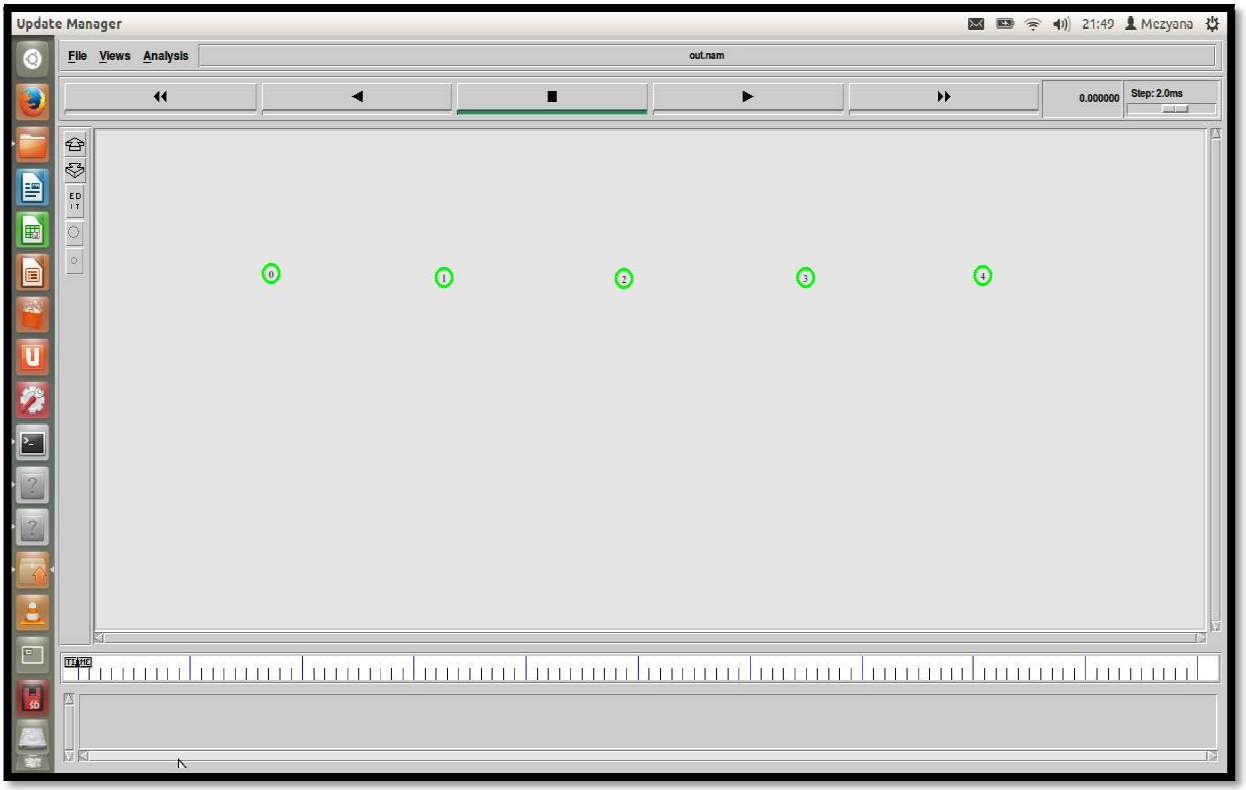


Figure 3.8: *Topologie d'étude (5 nœuds).*

C'est le scénario classique de la chaine de nœuds. Les nœuds sont disposés en chaine séparés par 200 mètres dans un réseau ou la portée de transmission est de 250 mètres, ce qui veut dire que chaque deux nœud séparé par au moins un autre nœud sont caché l'un par rapport à l'autre. La communication se fait comme suit :

Le nœud 0 envoi des paquets au nœud 1 et le nœud 3 envoi des paquets au nœud 4. La communication entre les nœuds 0 et 1 débute à l'instant 0,5 seconde et se termine à l'instant

3,4 seconds et entre 6 et 1 la communication démarre à l'instant 3,8 secondes et s'achève a l'instant 9,0 seconds.

- **Détection des nœuds cachés :**

Nœud	Action
2	Ajout le nœud caché 0
2	Ajout le nœud caché 4

Tableau 3 :*Détection des nœuds caché (Scénario 1).*

- **Consommation d'énergie :**

Le fichier trace contient le taux d'énergie de chaque nœud dans différents durée de la simulation, pour extraire l'énergie totale consommer à la fin de la simulation, nous utiliseront un script AWK (voir Annexe).

Partie 1 : (Simulation sans sleep( ) et wakeup( ))

Au lancement de la simulation, les nœuds de la topologie commencent à établir des connexions cela passe par l'exécution de plusieurs mécanismesd'échange de paquets notamment le mécanisme RTS/CTS.

⇨ **l'énergie consommé = 50,179413 Joules.**

Partie 2 : (Avec les fonction sleep( ) et wakeup( ))

Au lancement de la simulation la fonction sleep( ) est exécutéen mettant seulement les voisins du nœud source et destination en mode sleep, dès que la transmission s'achève, la fonction wakeup( ) est exécuté et tous les nœuds serons en mode wakeup.

⇨ **l'énergie consommé = 46,092051 Joules.**

3.8.4. Scénario 2 (7 Nœuds) :

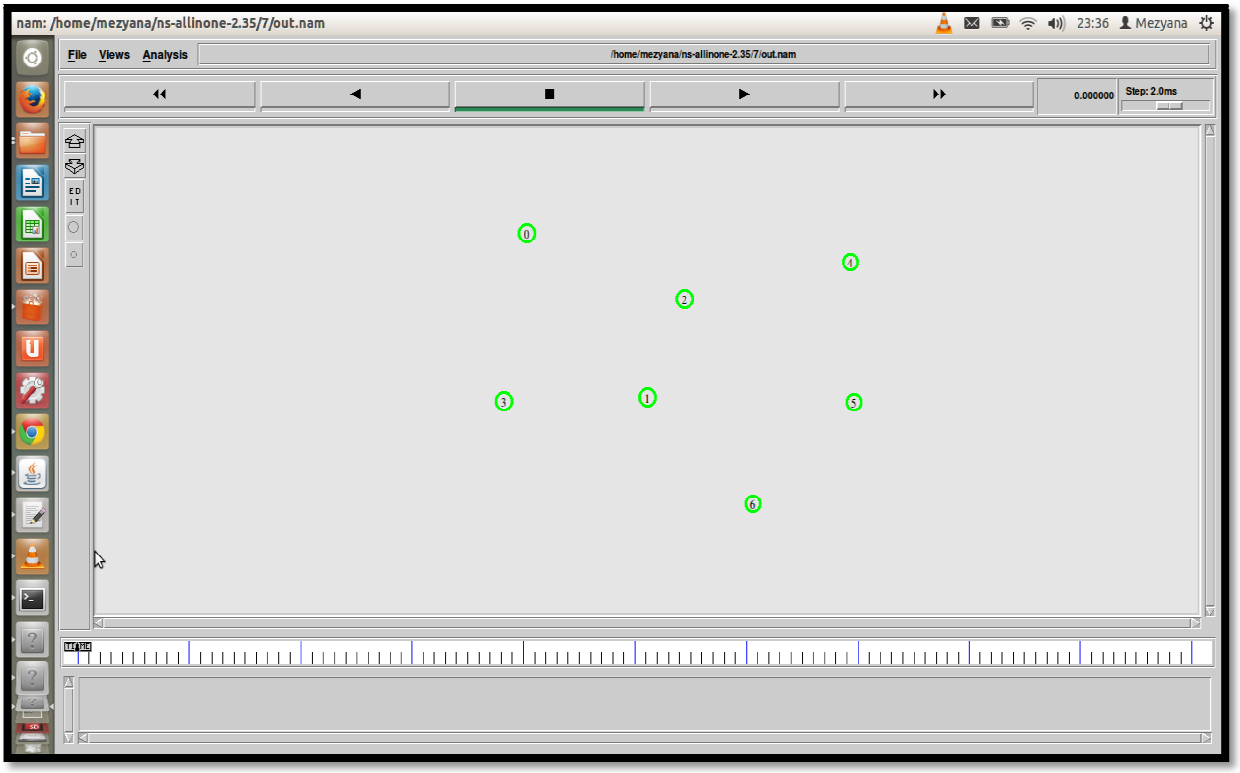


Figure 3.9: *Topologie d'étude (7 nœuds).*

La communication se fait comme suit :

Le nœud 0 envoi des paquets de donnée au nœud 2, le nœud 4 envoi des paquets de donnée au nœud 5 et le nœud 1 envoi des paquets de donnée au nœud 6. La communication entre 0 et 2 commence à l'instant 0,5 seconde et se termine à l'instant 4,7, entre 4 et 5 débute à l'instant 1,2 et se termine a l'instant 6,8 secondes et entre 1 et 6 démarre à l'instant 1,8 et s'achève à l'instant 8,7 secondes.

- **Détection des nœuds cachés :**

Nœud	Action
0	Ajout le nœud caché 1
1	Ajout le nœud caché 0
3	Ajout le nœud caché 2
2	Ajout le nœud caché 3
4	Ajout le nœud caché 0
6	Ajout le nœud caché 4
2	Ajout le nœud caché 5
6	Ajout le nœud caché 3
5	Ajout le nœud caché 1
2	Ajout le nœud caché 6
3	Ajout le nœud caché 6

Tableau 4 :*Détection des nœuds caché (Scénario 2).*

- **Consommation d'énergie :**

Partie 1 : (Simulation sans sleep( ) et wakeup( ))

⇨ **l'énergie consommé = 73,612770 Joules**

Partie 2 : (Avec les fonctionssleep( ) et wakeup( ))

⇨ **l'énergie consommé = 68,944786 Joules.**

3.8.5. Scénario 3 (10 Nœuds) :

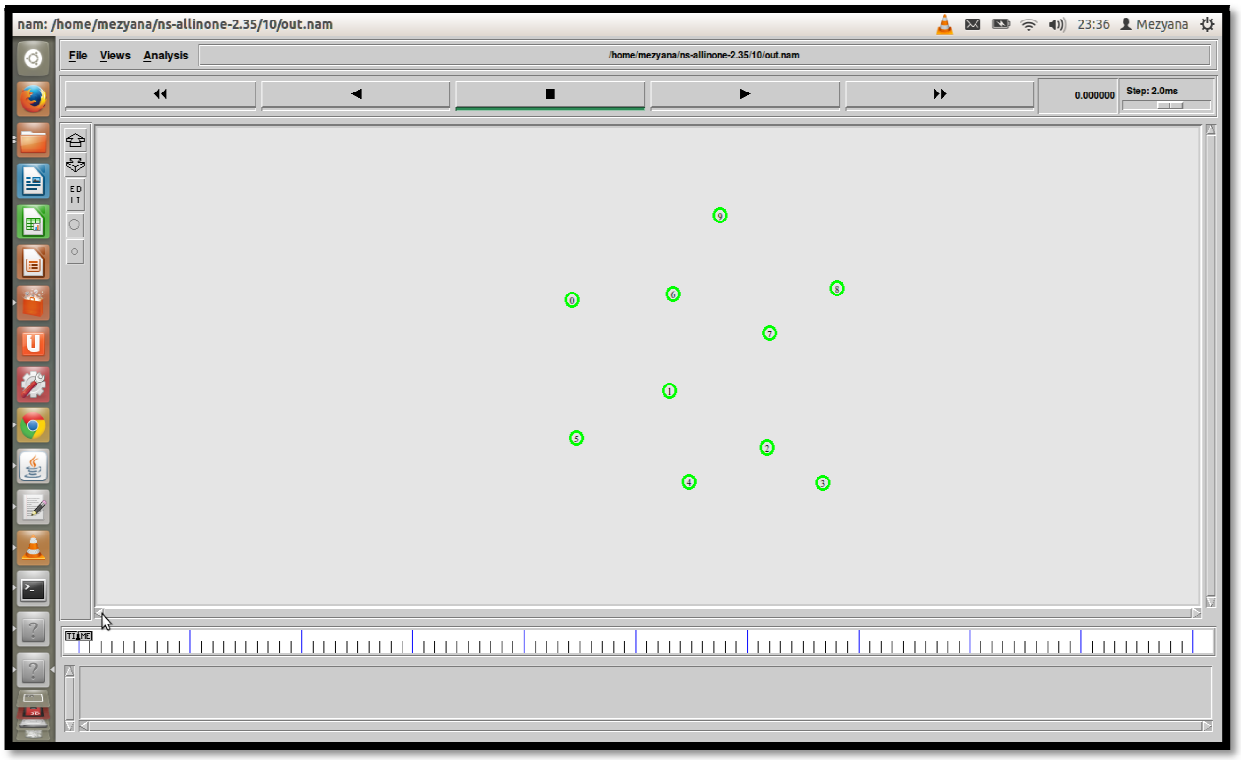


Figure 3.10: *Topologie d'étude (10 nœuds).*

La communication se fait comme suit :

Le nœud 0 envoi des paquets de donnée au nœud 6, le nœud 9 envoi des paquets de donnée au nœud 8, le nœud 2 envoi des paquets de donnée au nœud 7, et le nœud 3 envoi des paquets de donnée au nœud 4. La communication entre 0 et 6 commence a l'instant 0,5 seconde et se termine à l'instant 2,9, entre 9 et 8 débute à l'instant 1,2 et se termine a l'instant 5,5 secondes, entre 2 et 7 commence à l'instant 4,5 et se termine à l'instant 6,3 et entre 3 et 4 démarre à l'instant 7,0 et s'achève à l'instant 9,9 secondes.

- **Détection des nœuds cachés :**

Nœud	Action
9	Ajout le nœud caché 0
7	Ajout le nœud caché 0
5	Ajout le nœud caché 6
6	Ajout le nœud caché 8
6	Ajout le nœud caché 5
7	Ajout le nœud caché 5
2	Ajout le nœud caché 5
6	Ajout le nœud caché 2
8	Ajout le nœud caché 2
9	Ajout le nœud caché 2
3	Ajout le nœud caché 7
4	Ajout le nœud caché 7
1	Ajout le nœud caché 3
5	Ajout le nœud caché 3

Tableau 5:*Détection des nœuds caché (Scénario 3).*

- **Consommation d'énergie :**

Partie 1 : (Simulation sans sleep( ) et wakeup( ))

⇨ **l'énergie consommé = 102,622574 Joules**

Partie 2 : (Avec les fonctionssleep( ) et wakeup( ))

⇨ **l'énergie consommé = 88,326048 Joules.**

3.8.6. Discussion des résultats :

Dans le premier scénario le nœud 2 détecte le nœud 0 comme nœud caché ce qui indique que le nœud 2 a conclu que le nœud 0 est caché parce qu'il n'a pas entendu les ACK et CTS émis à son voisin –le nœud 1- par le nœud 0, Ensuite de la même manière, le nœud 2 détecte un deuxième nœud caché 4 et ceci grâce à la communication entre ce dernier et le nœud 3.

La consommation d'énergie dans la couche MAC 802.11 pour détecter les nœuds cachés en utilisant la détection passive (mécanisme RTS/CTS avec le mode sleep/wakeup) est inferieur par rapport à la détection passive (mécanisme RTS/CTS sans le mode sleep/wakeup)(Voir la figure 3.11).

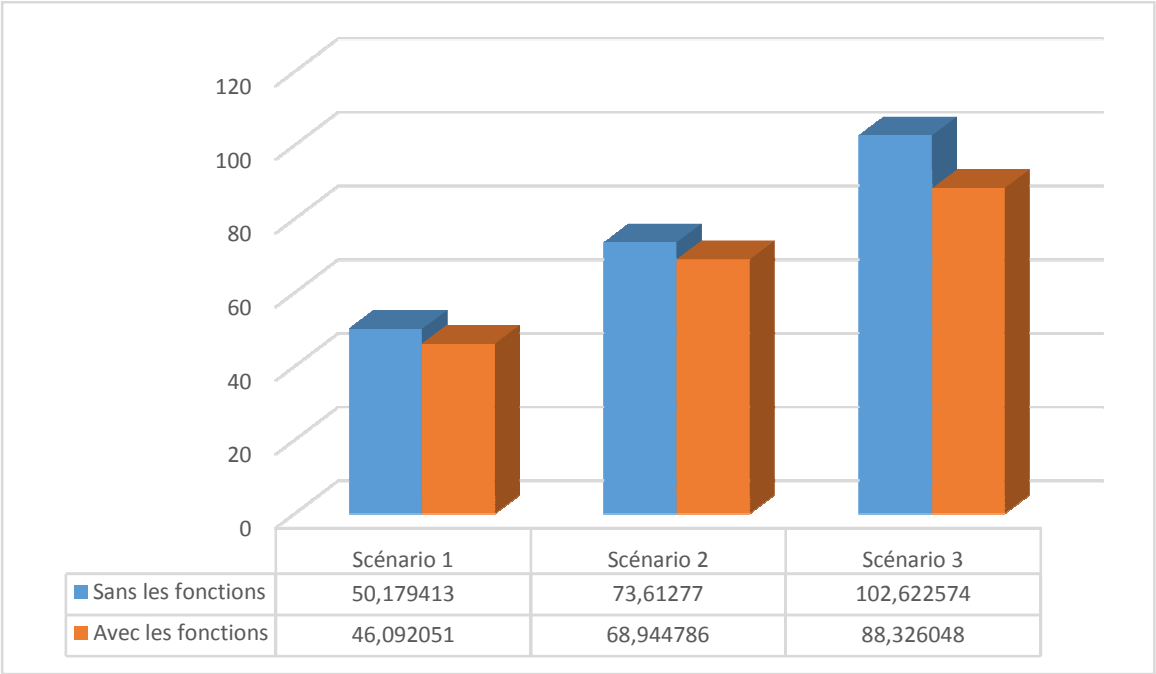


Figure 3.11: *Taux de consommation de l'énergie.*

La Figure 3.11 donne une idée globale sur l'efficacité des deux fonctions sleep et wakeup, prenons par exemple le scénario 1, en exécutant ce dernier sans l'implémentation des deux fonctions sleep et wakeup, la consommation de l'énergie étais 50,17 Joules, avec l'inclusion des deux fonctions le taux ce minimise et arrive à 46,09 Joules.

3.9. Conclusion :

Notre approche montre que l'ajout du mécanisme sleep/wakeup améliore les performances du réseau ad hoc en termes de détection des nœuds caché et de conservation d'énergie.

La détection passive consiste au recensement de l'ensemble des nœuds récepteur à l'exception du nœud récepteur. Nous avons retenu comme approche la détection passive à base de RTS/CTS que nous avons combinés avec le mécanisme sleep/wakeup emprunté du SMAC (sensor MAC).

L'implémentation de la détection passive sans les fonctions sleep/wakeup et de notre approche détection passive avec sleep/wakeup nous permet de faire une synthèse sur les performances du réseau.

Les conclusions montrent que notre approche permet la communication entre deux nœuds dans le même voisinage, la détection des nœuds caché et bien sûre minimise la consommation d'énergie toute fois un temps de calcul supplémentaire est additionné (activation des modes sleep et wakeup).

Nous prévoyons l'application future du mécanisme sleep/wakeup dans la combinaison détection active / passive.

Dans le fichier mac802.11.h et le fichier mac802.11.cc nous avons ajouté les fonctions (sleep() et wakeup()) suivantes dans le simulateur NS2.35 :

```
void Mac802_11::sleep()
state__ = 0;
radioState__ = RADIO_SLP;
Phy *p;
p=netif_;
((WirelessPhy *)p)->node_sleep();

void Mac802_11::wakeup()
state__ = 1;
if (radioState__ == RADIO_SLP)
radioState__ = RADIO_IDLE;
Phy *p;
p=netif_;
((WirelessPhy *)p)->node_wakeup(); nav_sleep = 0;
```

Dans le fichier AODV.h et le fichier AODV.cc nous avons ajouté la fonction suivante dans le simulateur NS2.35 :

```
void AODV::un_saut()
if(stat__==1)
neighbor=1;
stat__=0;
```

```
BEGIN {
total_energy_consumed = 0.000000;
}
{
state           =       $1;
time            =       $3;
node_num        =       $5;
energy_level    =       $7;
if(state == "N") {
        for(i=0;i<7;i++) {
                if(i == node_num) {
                                        energy_left[i] = energy_left[i] - (energy_left[i] -
energy_level);
                                }
                        }
                }
}
END {
printf("L'energie de chaque noeud a la fin de la simulation : \n\n")> "energyleft.txt";
for(i=0;i<7;i++) {
printf("Noeud %d : %.6f \n",i, energy_left[i]) > "energyleft.txt";
total_energy_consumed = total_energy_consumed + energy_left[i];
}
printf("\n\nL'energie total consommer : %.6f\n", (7*200)-total_energy_consumed)>
"energyleft.txt" ;
}
```

Commande d'exécution du script : awk –f **nom_du_script.awknom_du_fichier_trace.tr**

[1]Pujolle, Guy. Les réseaux. Edition Eyrolles, 2006.

[2]Gast Mathew. « 802.11 la reference». O'Reilly, 2005

[3] la norme 802.11, " http://reseau.erasme.org/IMG/resume_802.11/

resume_802.11.html " Consulté le 30 Mars 2014.

[4] 802.2: sous couche LLC « http://www.gaudry.be/_pge/r-llc.php »Consulté

le29 Mars 2014.

[5]S. Corson et J. Macker, « Mobile Ad Hoc Networking (MANET) », Technical Report RFC 2501, IETF Juin 1999.

[6]Stefano Basagni, Marco Conti, Silvia Giordano, Ivan Stojmenovic

« Mobile Ad Hoc Networking »,IEEE John Wiley & Sons publication 7 Oct. 2004

[7]MehranAbolhasan, Tadeusz Wysocki, ErykDutkiewicz«A review of routing protocols for mobile ad hoc networks », ELSEVIER,4 Juin2003

[8]N. Abramson «The ALOHA system another alternative for computer communications », NJ, vol. 37, pp. 281–285, (1970).

[9]P. Karn" MACA - A new channel access method for packet radio, In proceedings of the ARRL/CRRL Amateur Radio" 9eme computer Networking Conference (1990).

[10]Sunil Kumar, Vineet S. Raghavan, Jing Deng " Medium Access Control protocols for ad hoc wireless networks", ELSEVIER (2004).

[11]Site de simulateur réseaux NS-2 : http://www.isi.edu/ns2/ Consulté le 13 Mai 2014